State of Hawai'i
IMT

BUSINESS AND IT/IRM TRANSFORMATION PLAN

GOVERNANCE

TABLE OF CONTENTS

1.0 INTRODUCTION 10

1.1 Purpose 10

1.2 Scope 10

1.3 Document Overview 10

1.4 Associated Documents 11

2.0 GOVERNANCE 12

2.1 Enterprise Investment Life Cycle (EILC) 14

3.0 GOVERNANCE STRUCTURE 16

3.1 Executive Leadership Council (ELC) 17

3.1.1 Purpose 17

3.1.2 Membership 18

3.1.3 Roles and Responsibilities 18

3.1.3.2 Responsibilities of Voting Members 20

3.1.3.3 Responsibilities of the Chief of Staff/ELC Chair 20

3.1.3.4 Responsibilities of the CIO and OIMT Staff 20

3.1.3.5 Relationship to Other Governance Boards 20

3.1.4 Methods and Procedures 20

3.2 CIO Council (CIOC) 21

3.2.1 Purpose 21

3.2.2 Membership 21

3.2.2.1 Voting Members 21

3.2.2.2 Advisory Members 21

3.2.3 Roles and Responsibilities 21

3.2.3.1 Responsibilities of the CIOC 21

3.2.3.2 Responsibilities of Voting Members 23

3.2.3.4 Responsibilities of the CIO/CIOC Chair 23

3.2.3.5 Responsibilities of the OIMT Staff 23

3.2.3.6 Relationship to Other Governance Boards 23

3.2.4 Methods and Procedures 23

3.2.4.2 Meeting Absence 23

3.2.4.3 Meeting Ground Rules 23

3.2.4.4 Meeting Minutes 24

3.2.4.5 Communication 24

3.2.4.6 Charter Revisions 24

3.3 IT Steering Committee 24

3.3.1 Purpose 24

3.3.2 Membership 24

3.3.3 Roles and Responsibilities 24
3.3.4 Methods and Procedures 25
3.3.4.1 Meetings 25
3.3.4.2 Meeting Ground Rules 25
3.3.4.3 Meeting Minutes 25
3.3.4.4 Communication 25
3.3.4.5 Sunshine Law 25
3.4 Working Groups 25
3.4.1 Executive Group 26
3.4.3 Governance and Policy Working Groups 27
3.4.4 Technology Working Groups 28
3.4.5 Shared Services Working Groups 29

4.0 ENTERPRISE ARCHITECTURE METHODOLOGY 30
4.1 Enterprise Architecture (EA) Practice 31
4.1.1 Complete View of the IT Environment 33
4.1.2 Strategic Alignment of IT Investments to Business Needs and Priorities 33
4.1.3 Increase the Value from Investments 33
4.1.4 Transform Business Operational Effectiveness 33
4.2 Basis for the Framework, Methodology, and Delivery Process Associated with the State's EA Practice 33
4.3 Selected EA Methodology 34
4.3.1 Guiding Principles for the EA Methodology Implementation and Tailoring 34
4.3.2 Hawai'i's Tailored EA Methodology Implementation 35
4.4 Architectural Layers within the EA Framework 36
4.4.1 Enterprise Business Architecture (EBA) 36
4.4.2 Enterprise Information Architecture (EIA) 36
4.4.3 Enterprise Solution Architecture (ESA) 36
4.4.4 Enterprise Technology Architecture (ETA) 36
4.5 Technical Approach for EA Development and Continual Update 37
4.6 High-level EA Development Approach 38
4.6.1 Step One – Outline Enterprise Change Drivers 38
4.6.2 Step Two – Develop To-Be or Future-State Vision 38
4.6.3 Step Three – Outline Enterprise Architecture (EA) 39
4.6.3.1 Constructing the Conceptual Architecture 39
4.6.3.2 Outlining the Enterprise Business Architecture (EBA) 39
4.6.3.3 Outlining the Enterprise Information Architecture (EIA) 40
4.6.3.4 Outlining the Enterprise Solutions Architecture (ESA) 40
4.6.3.5 Outlining the Enterprise Technology Architecture (ETA) 40
4.6.4 Step Four – Develop Enterprise Transformation Strategy 41

4.7 Detailed Business Segment Architecture Development Approach 42
4.7.1 Step One – Develop Segment Scope and Strategic Vision 43
4.7.2 Step Two – Outline Segment Architecture 44
4.7.3 Step Three – Develop Segment Transformation (Transition and Sequencing) Plan 44
4.8 Institutionalizing and Maintaining the EA Program 46

5.0 PORTFOLIO MANAGEMENT (PFM) 47
5.1 Critical Success Factors and Performance Measures for the Portfolio 48
5.2 Roles and Responsibilities 48
5.2.2 Chief Information Officer (CIO) 48
5.2.3 Executive Leadership Council (ELC) 49
5.2.4 CIO Council (CIOC) 49
5.3 OIMT Investment Portfolio Manager (PfMgr) 49
5.4 Executive Sponsor 50
5.5 Investment/Project or Program Manager (PM) 50
5.6 State Procurement Office (SPO) 50
5.7 Department of Budget and Finance (B&F) 50
5.8 Investment Portfolio Information 51
5.9 IT Investment Management Process 52
5.10 Pre-select or Analyze/Architect Phase and Process Steps 54
5.11 Select Phase 54
5.12 Invest Phase 55
5.13 Implement, Measure, Assess, Improve, and Control Phases 55
5.14 Evaluate Phase 56
5.15 PfM and Other IT Governance and Management Activities 56
5.16 Investment Portfolio Management Tool Suite 56

6.0 PROJECT MANAGEMENT 57
6.1 Purpose 58
6.2 Scope 58
6.3 Project Management Goals and Objectives 58
6.4 Project Performance Measures 59
6.5 PMM Process 59
6.6 Other Project Management Methodologies 60
6.7 Agile Development 60
6.8 PMM Checkpoints/Approval Gates 61
6.9 Project Status Reviews 61
6.10 Proposal 62
6.11 Approved Projects 62
6.12 Completed Planning Review 62
6.13 PMM Knowledge Areas 62
6.13.1 Integration Management 62

6.13.2 Scope Management....62

6.13.3 Time Management....63

6.13.4 Cost Management....63

6.13.5 Quality Management....63

6.13.6 Human Resources Management....64

6.13.7 Communications Management....64

6.13.9 Risk Management....64

6.13.10 Procurement Management....65

6.13.12 Program and Project Organization Charts....65

6.14 Project Roles and Responsibilities....69

6.14.1 Executive Sponsor....69

6.14.2 Project Manager (PM)....69

6.14.3 Subject Matter Expert (SME)....69

6.14.4 Functional Manager....69

6.14.5 Deliverable Owner....69

6.14.6 Project Resource....69

6.14.7 Stakeholder....70

6.14.9 Project Risk Manager....70

6.14.10 Project Communications Manager....70

6.14.11 Project Issue Manager....70

6.14.12 Project Management Training....70

7.0 BUSINESS PROCESS REENGINEERING....71

7.1 Scope....72

7.2 Associated Documents....72

7.3 Selecting and Managing a Business Process Reengineering (BPR) Project....73

7.4 BPR Roles and Responsibilities....74

7.4.1 BPR Project Champions for the State....74

7.4.2 BPR Project Sponsor....74

7.4.4 Subject Matter Expert/Change Agent....74

7.4.5 Core Team....75

7.4.6 Criteria for Identification of BPR Projects....75

7.4.7 Documenting the Original and Improved Process....75

7.4.8 Identifying and Recording IT Changes or Requirements....75

7.4.9 Organizational Change Management....76

7.5 Conducting a BRP Activity Using Different Methodology....77

7.5.1 Selection of the Right BPR Methodology....77

7.6 BPR Using TOC....78

7.7 Theory of Constraint (TOC)....79

7.7.1 Constraint-based (TOC) System Architecture....79

7.7.2 System Improvement Architecture....81

7.8 Measuring Process Improvement.....82
7.8.1 Outcome Metrics.....82
7.8.2 Leading Metrics versus Lagging Metrics.....83
7.9 Notional Timeline for a BPR Using the TOC Methodology.....84
7.10 Lean.....86
7.11 Lean Principles to Practice.....86
7.11.1 Specify Value.....86
7.11.2 Define the Value Stream.....86
7.11.3 Value Flow.....86
7.11.3.1 The Concept of Kaizen (Ongoing Improvement).....87
7.11.4 End-user Pull.....87
7.11.5 Kanban.....87
7.11.6 Perfection.....87
7.11.7 Agility.....87
7.12 Six Sigma.....88
7.12.1 Define, Measure, Analyze, Implement, and Control (DMAIC).....88
7.12.2 Define.....88
7.12.3 Measure.....88
7.12.4 Analyze.....88
7.12.5 Improve.....88
7.12.6 Control.....88
7.13 Design for Six Sigma (DFSS).....88
7.13.1 Identify.....88
7.13.2 Design.....89
7.13.3 Optimize.....89
7.13.4 Validate.....89
7.14 integrated TOC, Lean, Six Sigma (iTLS).....90
7.14.1 What Are the iTLS Steps?.....90
7.14.1.1 Mobilize and Focus to Identify the Core Problem.....90
7.14.1.2 Decide How to Exploit the Constraint.....91
7.14.1.3 Eliminate Sources of Waste from the Constraint.....91
7.14.1.4 Control Process Variability and Error.....91
7.14.1.5 Control Supporting Activities.....91
7.14.1.6 Remove the Constraint and Stabilize the Process.....91
7.14.1.7 Reevaluate the System Performance and Go after the Next Constraint.....91
7.15 Conclusion
8.0 PERFORMANCE MANAGEMENT.....93
8.1 Metrics.....94
8.1.1 Outcomes (Mission and Business Results, Customer Results).....94
8.1.2 Outputs (Processes and Activities).....94
8.1.3 Inputs (Human Capital, Technology, Other Fixed Assets).....94

LIST OF FIGURES

Figure 1: Transformation Framework....11
Figure 2: Holistic Life Cycle....14
Figure 3: Governance Structure 17
Figure 4: Working Group Organization Structure....26
Figure 5: State of Hawai'i EA Practice 32
Figure 6: EA Practice Context for the State of Hawai'i....32
Figure 7: State of Hawai'i Two Level EA Methodology....35
Figure 8: Enterprise Transformation Strategy....38
Figure 9: Enterprise Transformation Strategy....41
Figure 10: Segment Transformation Plans....42
Figure 11: Business Segment Architecture Development – Business and IT Tracks 43
Figure 12: Business Segment Architecture Development Work Plan 45
Figure 13: Business Segment Architecture Development (Involvement Model) 45
Figure 14: Life Cycle and Management Perspectives and Alignment 52
Figure 15: Investment, Improvement, and Budget and Appropriation Life cycle 53
Figure 16: Supporting Methodologies to Manage Selected Investments....53
Figure 17: The Project Management Processes....59
Figure 18: PMBOK Processes Iterative Diagram....60
Figure 19: Project Processes....60
Figure 20: Basic OIMT Program Structure 65
Figure 21: Program Governance....66
Figure 22: Program Management....67
Figure 23: Project Team Organization Chart....67
Figure 24: BPR Project Screening Considerations 73
Figure 25: Managing BPR Projects 73
Figure 26: TOC's Unique Approach 68
Figure 27 - Improvement Phase Initiatives....81
Figure 28 - SDAIS Improvement Curve 84
Figure 29 - iTLS Approach....90

LIST OF TABLES

Table 1: Relationship of Architectures to Federal Reference Models 37

Table 2: PfM Information Requirements and Benefits....51

Table 3: ITIL Reviews....61

Table 4: Project Status 61

Table 5: Qualitative Risk Analysis 61

Table 6: Integration Management Processes 62

Table 7: Scope Management Processes....62

Table 8: Time Management Processes....63

Table 9: Cost Management Processes 63

Table 10: Quality Management Processes....63

Table 11: Human Resources Management Processes 64

Table 12: Communications Management Processes 64

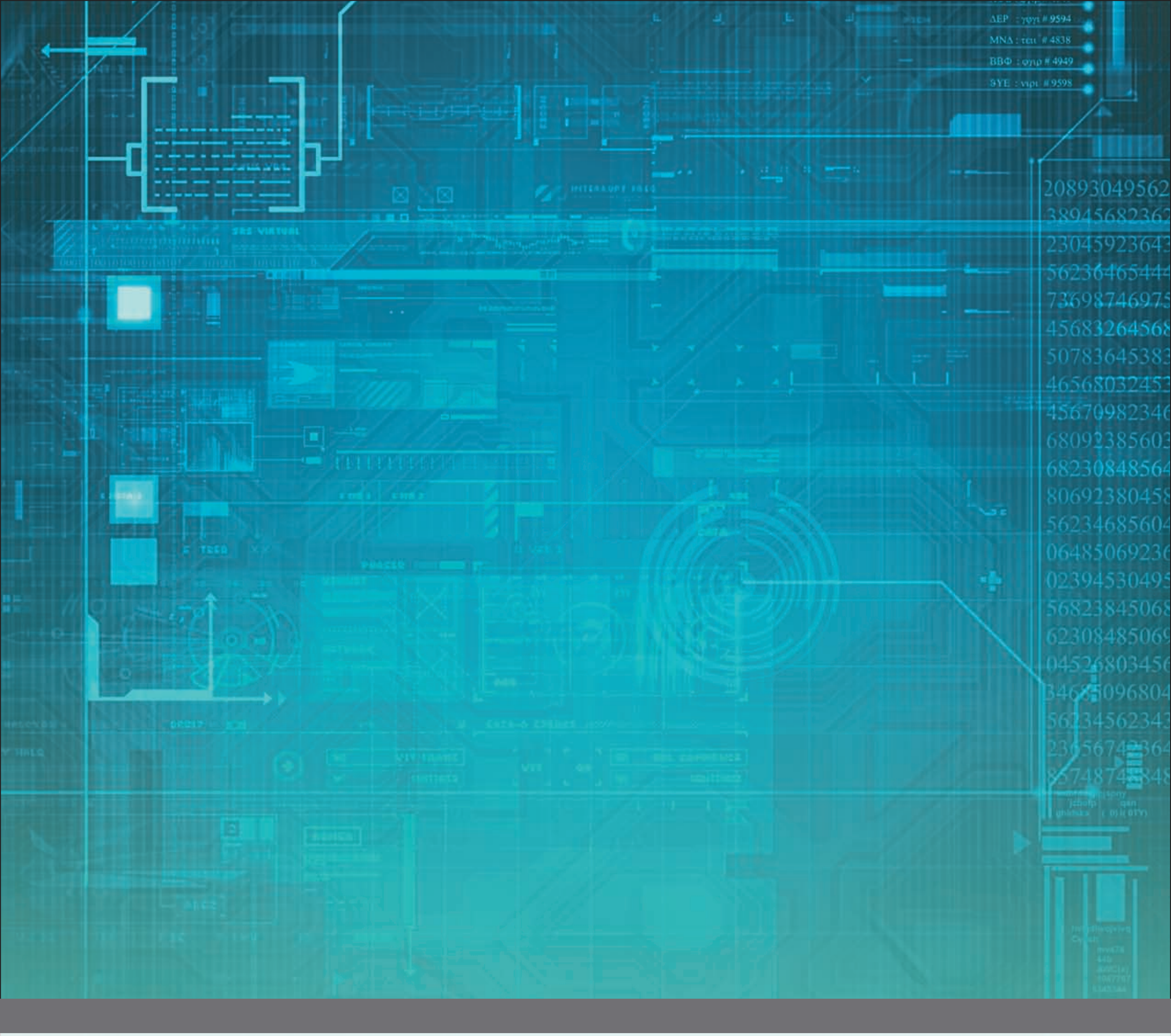
Table 13: Risk Management Processes....64

Table 14: Procurement Management Processes 65

Table 15: Project Management Process Groups and Knowledge Area Mapping 76

Table 16: Comparison of Methodologies 77

Table 17: Notional Schedule and Time Commitment for a BPR Activity Using TOC....85



1.0 INTRODUCTION

1.0 INTRODUCTION

1.1 PURPOSE

The purpose of this document is to provide a description of the structure, policies, and processes that the Office of Information Management & Technology (OIMT) will use for governing the business transformation and Information Technology/Information Resource Management (IT/IRM) of the State of Hawai'i.

1.2 SCOPE

This document establishes the governance of investments in business transformation and IT/IRM across the entire enterprise, and for the entire life cycle of the investment, from initial concept through retirement.

1.3 DOCUMENT OVERVIEW

Governance helps an enterprise ensure that it is investing its limited resources in alignment with the strategic direction desired by leadership. Management ensures that those resources are being used efficiently and effectively to produce the desired results. Governance and management of the enterprise are employed to achieve desired transformation or operational improvements fully integrated with the other elements, functions, activities, or practice areas. These related elements include:

1. The Management and Oversight function that provides a governance structure/process that oversees all related business transformation activities, IT investments, and projects to ensure they achieve desired results.

2. *The Strategic Plan* that establishes the overarching goals, strategies, objectives, and performance measures for the transformation and drives the requirements for the Enterprise Architecture (EA).

3. Projects, defined within the *Transition and Sequencing Plan (T&S Plan)*, are approved, funded, and initiated within the proposed sequence and timeframes. These include BPR projects identified to streamline current business processes, and system and technology development/implementation projects – categorized as Triage projects to address immediate needs; Pilot projects to pilot new enterprise capabilities; or Major Initiative Support projects to establish enterprise systems or technologies.

4. Portfolio Management (PfM) practice as the comprehensive inventory of all IT investments.

Figure 1 provides an overview of this integration and other functions, practice, or program areas.

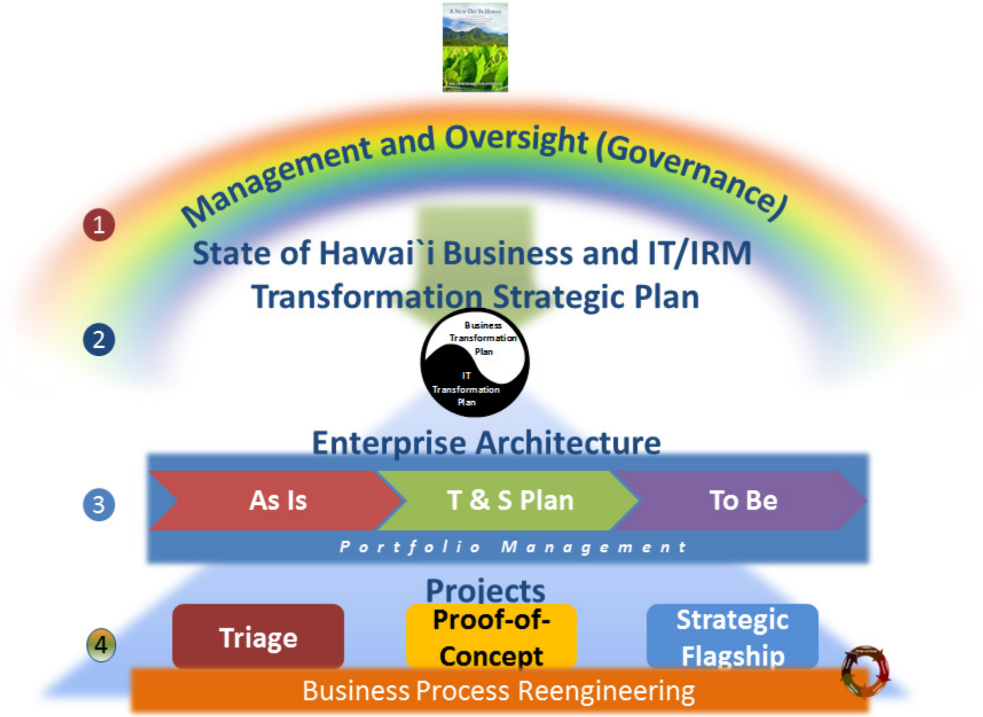

Management and Oversight (Governance)
1
State of Hawai`i Business and IT/IRM Transformation Strategic Plan
2
Business Transformation Plan
IT Transformation Plan
Enterprise Architecture
3
As Is
T & S Plan
To Be
Portfolio Management
Projects
4
Triage
Proof-of-Concept
Strategic Flagship
Business Process Reengineering

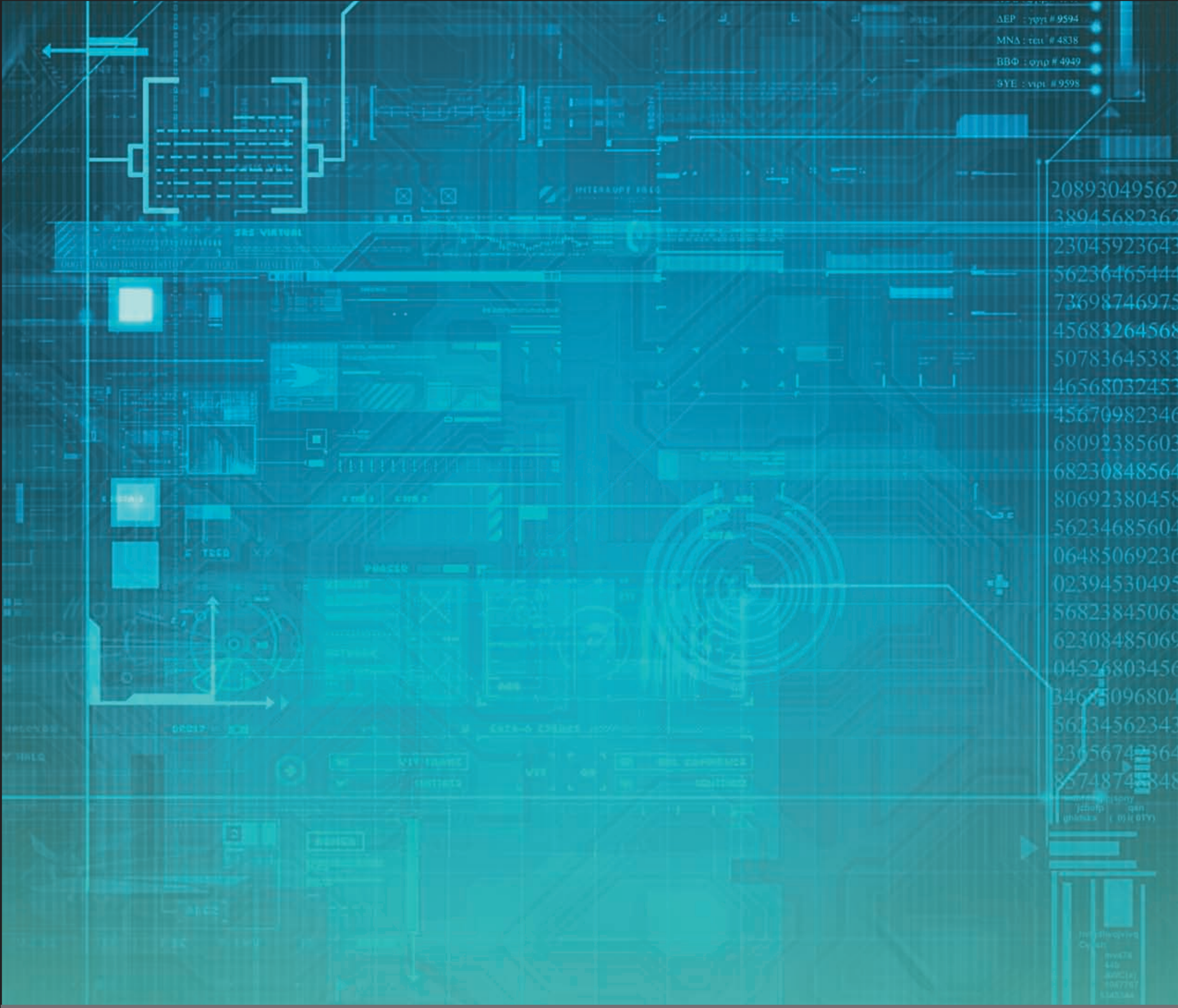
Figure 1: Transformation Framework

Finally, once specific projects are initiated, the EA future state guidance in the information, solutions and technical architectures are used as key touch points within the Systems Development Life Cycle (SDLC) for consideration and compliance within the context of EA governance and change management process.

Note: This document is a living document that will be maintained by OIMT and the Business Transformation Executive. The intended audience for this document is anyone within the State who is interested in learning about governance and the means by which investment decisions are made.

1.4 ASSOCIATED DOCUMENTS

- *State of Hawai'i Strategic Plan*
- *State of Hawai'i Business and IT/IRM Strategic Plan*
- *State of Hawai'i Enterprise Architecture*



2.0 GOVERNANCE

2.0 GOVERNANCE

Governance is the set of the organizational structure, policies, and processes by which the State selects business transformation and IT/IRM investments to ensure that strategic objectives are met efficiently and effectively, while controlling risk. ISACA, an international professional association that deals with IT Governance, defines governance as the practice that:

"…ensures that stakeholder needs, conditions and options are evaluated to determine balanced, agreed-on enterprise objectives to be achieved; setting direction through prioritization and decision making; and monitoring performance and compliance against agreed-on direction and objectives."[1]

ISACA's governance framework, the recently-published COBIT® 5, represents the current best practice in IT governance, and will serve as a model for the State of Hawai'i's governance approach.

One of the key principles of COBIT® 5 is the separation of governance and management. In short, management is about doing things right; governance is about doing the right things. Both are critical to the success of the enterprise. Sections 2-5 of this document is focused on governance; Sections 6-8 focus on management.

How, then, do we make sure we are "doing the right things"? Governance involves three main areas: the governance structure, which is the set of decision-making bodies that select the investments the enterprise will make in business transformation and IT/IRM; the policies that provide guidance on standards those investments must meet; and the process of initiating, selecting, funding, and overseeing the investments. Each of these is described in the following sections. The remainder of this section will establish some of the concepts that tie these three facets together into an integrated whole.

Before we can understand if we are doing the right things, we need to know what the right things are. What tells us what those things are? It depends on the scale and the scope we are looking at. In the broadest sense, what we do is defined by the *State of Hawai'i Strategic Plan* (currently under development). The State *Strategic Plan* establishes the mission, vision, goals, objectives, and performance metrics for the state government as a whole. It defines the outcomes that Hawai'i's taxpayers' dollars are supposed to produce in terms of health, education, transportation, social services, etc. The operations of the government—State employees, organizations, business processes, and information technology—are how these outcomes are achieved. We can go one step further and say that at the very top level why these are the desired outcomes is what the voters have demanded.

Moving down a level, we can re-establish the State government's operations as the what at the new scale. This set of goals and objectives are captured in the *State of Hawai'i Business and IT/IRM Strategic Plan*. It is that Plan that will guide the governance structure in ensuring we are "doing the right things."
The how at this level is now the individual programs that are funded and executed by the various Departments and attached agencies. Here, the why can be thought of as "because these are the things we need to do to meet the State's strategic goals."

Thus, the governance we are talking about is not about ensuring the state government as a whole is doing the right things—that is up to the Governor, the Legislature, and other elected and appointed officials in response to the desires of the people. What this governance is focused on is "are we doing the right things to support the established *Business and IT/IRM Transformation Strategic Plan?*" The "we" in this case are the CIO, the Department Directors, and the Departmental IT leads.

To make this determination, we need to establish the concept of an investment. An investment, in terms of governance, is simply a package of funding whose purpose is to improve the performance of the enterprise. We make the decision to fund an investment because we believe that it will improve the efficiency and/or effectiveness of our efforts to achieve our goals and objectives. Funding is provided to State agencies from the Legislature via programs. A program is a combination of people, processes, and technologies that are collectively designed to produce certain outcomes. For example, the objective of the Tourism program (BED 113) is "to achieve a strong and sustainable tourism industry that values and perpetuates Hawai'i's natural and cultural resources, honors Hawai'i's people and heritage, and supports a vital economy." The objective of the School Community Services program (EDN 500) is "to provide lifelong learning opportunities for adults and to meet other community needs of the general public."

Programs encompass leases, operating expenses (including personnel, equipment, other expenses), and capital improvements. An investment, for the purposes of this governance process, is that subset of a program's funding that is intended for business transformation or IT/IRM. A single program can have multiple investments, and it will also likely have spending that is not covered by an investment, as we use the term. Similarly, a given investment may actually be funded by multiple programs. The goal here is to supplement the State's program structure with a parallel structure that enables governance of business transformation and IT/IRM investments without changing the established budget process.

An investment has been established for each existing State program to capture all the information technology that program has purchased and which remains in use. These legacy investments form the foundation of the portfolio of investments established for each Line of Business (LOB) and managed by the Portfolio Executive. (For an explanation of LOB, see "ENTERPRISE ARCHITECTURE METHODOLOGY;" for a description of portfolio management, see "Portfolio Management").

Investments can be short-term pilots, or they can persist over years. They comprise hardware, software, services, and other resources (government full-time employees [FTEs], leased space, etc.). An investment typically has a business process analysis/reengineering and/or a requirements-gathering project in the early stages, and then a system development or acquisition stage.

2.1 ENTERPRISE INVESTMENT LIFE CYCLE (EILC)

Government agencies continually assess current performance, identify opportunities for performance improvement, and translate opportunities into specific actions. Key the effectiveness of governance is the concept of life cycle management. That is, establishing and maintaining visibility into an investment from its conception to its ultimate retirement. Governance that focuses only on the procurement of IT systems is less than optimal, because it would allow, for example, the automation of an obsolete process. Life cycle governance, on the other hand, looks at the entire value chain and requires business process analysis and potential reengineering before buying or building an IT system to support it. This is called the Enterprise Investment Life Cycle (EILC).

The EILC can be thought of as a superposition of several commonly-recognized life cycle models, including the IT Investment Life Cycle (Select, Control, Evaluate) and the Performance Improvement Life Cycle (Architect, Invest, Implement) used by the Federal Government, the Project Management Methodology as defined by the Project Management Institute® and adopted by OIMT, and the System Development Life Cycle (SDLC). The integration and coordination of these interrelated functions into a holistic life cycle (Figure 2) minimizes redundant efforts, stakeholder burden, cost, and complexity and ultimately favors achievement of desired mission outcomes and business results.

<table>
<tr><th>IT Investment Life Cycle</th><th>OMB Performance Improvement Cycle</th><th colspan="2">Project Management/ Methodology</th><th>System Development Life Cycle (SCLC)</th><th>Enterprise Investement Life Cycle (EILC)</th></tr>
<tr><td rowspan="4">(Pre-Select or Analyze)</td><td rowspan="4">Architect</td><td colspan="2">Initiation</td><td rowspan="5"></td><td>Need/Concept</td></tr>
<tr><td colspan="2">Planning & Design</td><td rowspan="2">Definition</td></tr>
<tr><td>Executing</td><td>Monitoring & Controlling</td></tr>
<tr><td colspan="2">Closing</td><td>Financial Planning</td></tr>
<tr><td>Select</td><td>Invest</td><td colspan="2"></td><td rowspan="2">Aquisition</td></tr>
<tr><td rowspan="9">Control</td><td rowspan="12">Implement</td><td colspan="2">Initiation</td><td>Initiation</td></tr>
<tr><td colspan="2" rowspan="4">Planning & Design</td><td>Concept</td><td rowspan="4">Detailed Requirements & Design</td></tr>
<tr><td>Planning</td></tr>
<tr><td>Requirements Analysis</td></tr>
<tr><td>Design</td></tr>
<tr><td rowspan="2">Executing</td><td rowspan="2">Monitoring & Controlling</td><td>Development</td><td>Development</td></tr>
<tr><td>Test</td><td rowspan="2">Deployment</td></tr>
<tr><td colspan="2">Closing</td><td>Implementation</td></tr>
<tr><td colspan="2" rowspan="3"></td><td rowspan="3">Operations & Management</td><td rowspan="4">Operations & Maintenance</td></tr>
<tr><td>Evaluate</td></tr>
<tr><td rowspan="2"></td></tr>
<tr><td colspan="2"></td><td>Disposition</td></tr>
</table>

At the highest level, the basic flow of EILC governance process is as follows:

NEED/CONCEPT: When a new idea or a new requirement that will require resources arises, the business lead (typically a PM) will initiate a new investment in the OIMT Portfolio Management system (This system has net been deployed. More specifics will be provided in the final publication of this document.) He or she will enter into the system a basic description of the proposed investment, which goals and objectives of the Business and IT/IRM Transformation Strategic Plan it is intended to support, the expected results, a rough order of magnitude (ROM) estimate for the resources that will be required, and identification of potential risks. At this stage, all figures are preliminary.

DEFINITION: OIMT works with the proposed investment's sponsor to understand the proposal and see if there is a potential solution already available. If not, the sponsor proceeds to build a more complete business case and alternatives analysis. Depending on the size, complexity, and risks of the proposed investment, varying levels of detail will be needed to pass the first review gate (review gates are described in Section 5 – Governance Process). In some cases, this is where the enterprise or segment architecture development effort takes place. In most cases, a more narrowly-focused conceptual solution architecture and business process reengineering occurs in the Definition phase.

FINANCIAL PLANNING: The business case is finalized and a funding strategy developed. In many cases, the program already has money available to execute the project. If not, other sources of funding may be required, including potentially a budget request for the next fiscal year.

ARCHITECT REVIEW GATE

ACQUISITION: In the Acquisition phase, high-level requirements identified in the Definition phase are turned into a Request for Proposals (or Request for Quotes, as appropriate) to solicit vendors to provide hardware, software, or services. If Commercial-off-the-Shelf (COTS) hardware or software is to be purchased, the requirements from the Definition phase must be complete enough to allow for selection.

DETAILED REQUIREMENTS & DESIGN: For investments requiring system development, a detailed requirements and system design phase occurs. This phase can be skipped when purchasing COTS products, but is vital to development of successful custom systems. The detailed requirements are a formal statement of the expected benefits, scope, assumptions and constraints, and interfaces. It includes the functional, operational, business, user, technical, performance, security, infrastructure, usability, and integration requirements for the project. Requirements must be testable and in accordance with enterprise architecture standards.

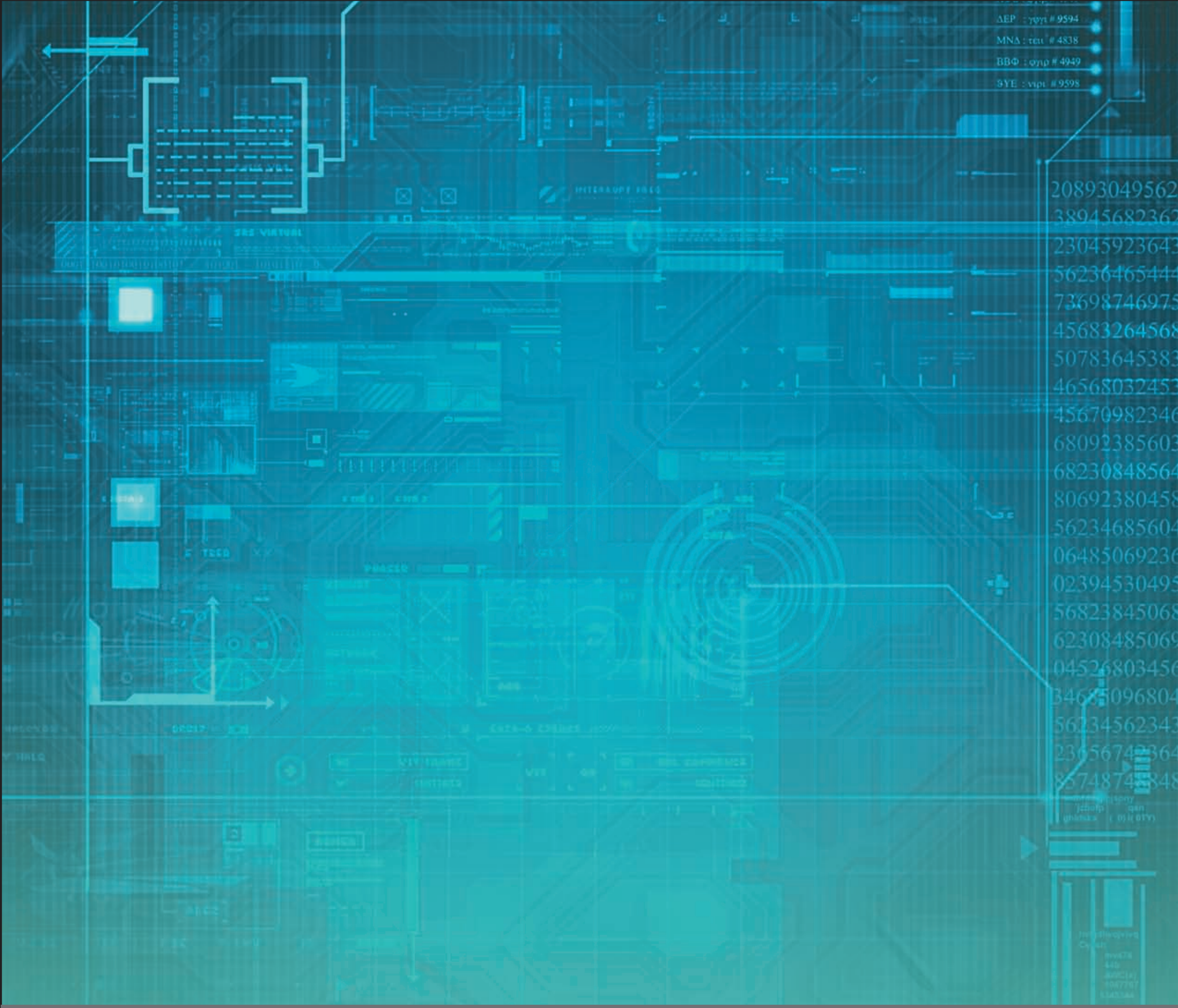
INVEST REVIEW GATE

DEVELOPMENT: System development, including testing, to create a solution that meets business requirements and architecture standards. Development can be done in-house by State resources, by contractors, or a combination.

DEPLOYMENT: Deployment includes installation, configuration, documentation, and training.

IMPLEMENT REVIEW GATE

Operations and Maintenance: Operations and Maintenance outlines the various tasks and activities being performed on an ongoing basis. It will also identify the key personnel and the tasks assigned to them necessary to effectively handle routine production processing, ongoing maintenance, and identified problems, issues, and/or change requests.



3.0 GOVERNANCE STRUCTURE

3.0 GOVERNANCE STRUCTURE

The governance structure for Business and IT/IRM Transformation in the State of Hawai'i will consist of two tiers: the top level is the Executive Leadership Council (ELC)—the 18 Department Directors and the CIOC, which consists of the Departmental IT Leads. The Legislatively established IT Steering Committee also provides advice and guidance to the CIO. To focus on specific topic areas and provide recommendations to the CIOC, various Working Groups are established under the CIOC. This structure is depicted in Figure 3.

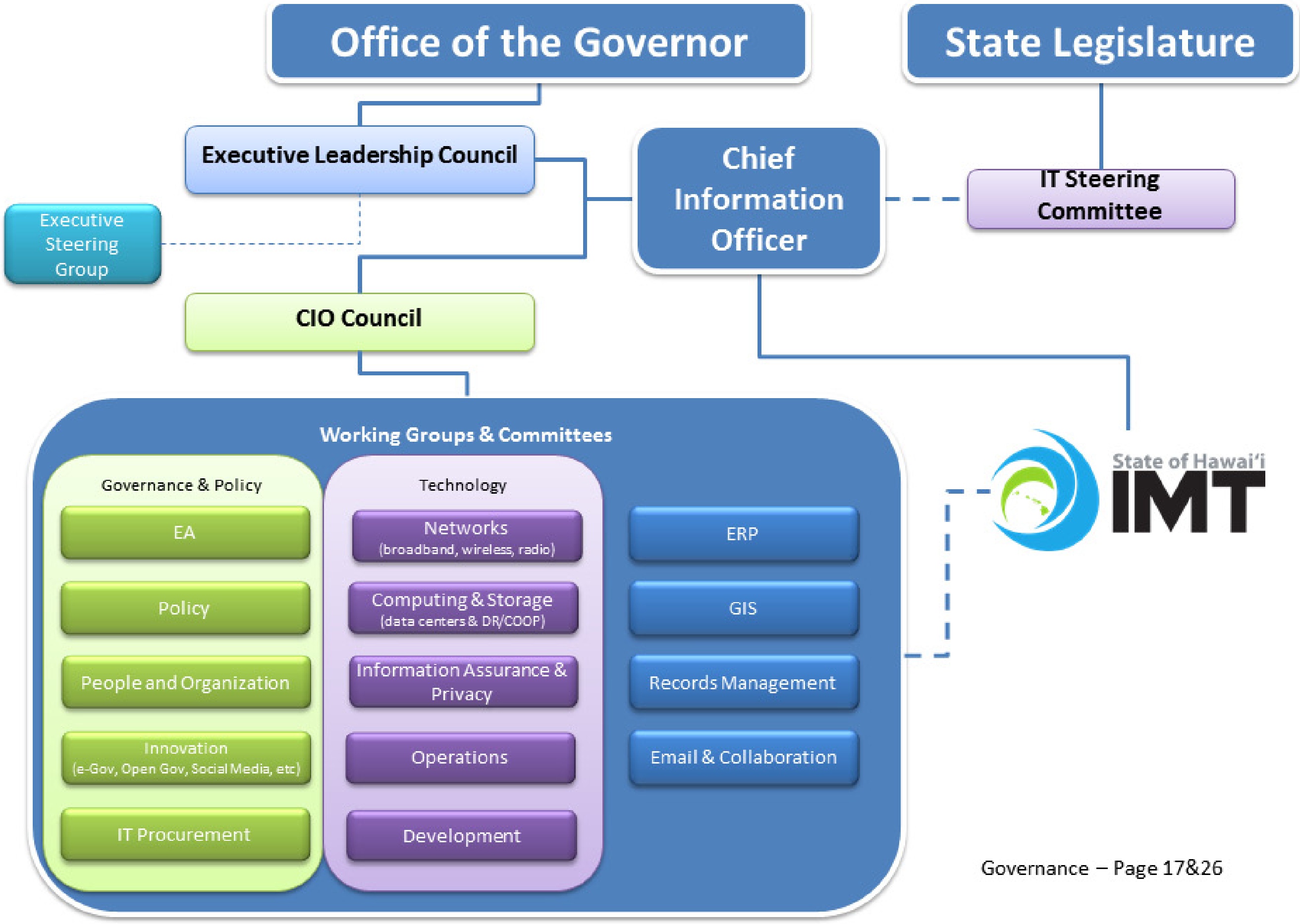


Figure 3: Governance Structure

The specific responsibilities of each governing body are described below.

3.1 EXECUTIVE LEADERSHIP COUNCIL (ELC)

3.1.1 PURPOSE

The ELC provides the State's strategic vision and direction for investments in business process improvement and Information Technology/Information Resource Management (IT/IRM). The ELC is the senior board accountable to the Governor and is responsible for setting priorities, establishing and tracking initiatives, resolving conflicts among Departments, and providing resources for transformation and IT/IRM initiatives.

The ELC is responsible for the five focused areas of IT governance:

- Strategic Alignment
- Ensuring management has put in place an effective strategic planning process
- Ratifying the aligned business and IT strategy
- Ensuring the IT organizational structure complements the business model and direction

- Value Delivery
- Sponsoring cross-cutting IRM/IT and business transformation initiatives
- Ascertaining that OIMT has put processes and practices in place that ensure IT delivers provable value to the business
- Ensuring investments represent a balance of risk and benefit and that budgets are acceptable

- IT Resource Management
- Monitoring how management determines what IT resources are needed to achieve strategic goals
- Ensuring a proper balance of IT investments for sustaining and growing the enterprise
- Allocating business resources required to ensure effective IT governance over projects and operations

- Risk Management
- Maintaining awareness about IT risk exposures and their containment
- Evaluating the effectiveness of management's monitoring of IT risks

- Performance Management
- Assessing senior management's performance on IT strategies in operation
- Working with the CIO to define and monitor high-level IT performance

3.1.2 MEMBERSHIP

ELC membership consists of the voting and advisory members described below.

3.1.2.1 VOTING MEMBERS

The members of the ELC are the Directors of the Executive Branch Departments of the government of the State of Hawai'i, listed in the *Policy Plan*, and the Chief Information Officer (CIO). The Chair of the ELC is the Governor's Chief of Staff.

3.1.2.2 ADVISORY MEMBERS

Advisory members are non-voting members who attend meetings as subject matter experts to the Council. They provide recommendations on issues related to, for example, legislative compliance, records management, security, project management, enterprise architecture, and infrastructure impacts and risks associated with specific investments. They advise the ELC on the technical feasibility of proposed projects, the project's adherence to IT architectures and standards, its relationship to other IT projects, and the reasonableness of the project cost estimates. Advisory members may be government personnel or contractors.

The Chair or any other member of the ELC may invite other advisory members as appropriate for consultation on the decisions before the ELC.

3.1.3 ROLES AND RESPONSIBILITIES

The roles and responsibilities of the ELC are described below.

3.1.3.1 RESPONSIBILITIES OF THE ELC

1. The ELC provides leadership, strategic direction, prioritization, and coordination among the Departments with respect to business transformation and IT/IRM.

2. The ELC fosters cooperation and communication, brokers disputes, enables joint action, and engenders commitment from stakeholder across the State.

3. The ELC communicates awareness and understanding of business and IT objectives and direction to appropriate stakeholders and users throughout the enterprise.

4. The ELC is responsible for reviewing, understanding, and approving or disapproving (with comments and required remedial actions):

IT Strategic Plan and Annual Operating Plan. *The IT Strategic Plan* defines the mission, vision, goals, objectives, and performance metrics for how IT contributes to the State's strategic goals, and the related costs and risks. The IT Strategic Plan will address, at a minimum, the following areas:

- Policy and Organization
- Leadership/Management
- Process/Change Management
- Information Resources Strategy and Planning
- IT Performance Assessment: Models and Methods
- IT Project/Program Management
- Capital Planning and Investment Control (CPIC)
- Acquisition
- e-Government
- Information Security/Information Assurance (IA)
- Enterprise Architecture
- Technology Management and Assessment

The *Annual Operating Plan* is a yearly addendum to the *Strategic Plan* that identifies the specific Initiatives that will be undertaken in that year to achieve the objectives defined in the *Strategic Plan*, their resource requirements, and their associated performance targets.

According to the COBIT Framework, version 4.1, the optimal state is achieved when:

> "IT strategic planning is a documented, living process; is continuously considered in business goal setting; and results in discernible business value through investments in IT. Risk and value-added considerations are continuously updated in the IT strategic planning process. Realistic long-range IT plans are developed and constantly updated to reflect changing technology and business-related developments. Benchmarking against well-understood and reliable industry norms takes place and is integrated with the strategy formulation process. The strategic plan includes how new technology developments can drive the creation of new business capabilities and improve the competitive advantage of the organization."

Enterprise Architecture. The *Enterprise Architecture (EA)* describes both the current state (as-is) and the target state (to-be) of how the State's IT aligns with and supports the business. This information is typically presented in accordance with a series of established reference models; Performance, Business, Service, Data, and Technology. The EA also includes a transition sequencing plan.

COBIT's description of an optimized architecture states:

> "The information architecture is consistently enforced at all levels. The value of the information architecture to the business is continually stressed. IT personnel have the expertise and skills necessary to develop and maintain a robust and responsive information architecture that reflects all the business requirements. The information provided by the information architecture is consistently and extensively applied. Extensive use is made of industry good practices in the development and maintenance of the information architecture, including a continuous improvement process. The strategy for leveraging information through data warehousing and data mining technologies is defined. The information architecture is continuously improving and takes into consideration non-traditional information on processes, organizations, and systems."

Biennial and Supplementary Budget Requests. Hawai'i's budget is determined on a biennial basis beginning each even-numbered fiscal year, with an opportunity for supplemental budget requests to address emergent requirements in the odd-numbered years.

Budget requests must be as specific as possible for both costs and benefits. A sound business case should accompany each request for funding to provide the Legislature. Alternative funding sources (e.g., grants and in-kind donations, Federal funds, fee-for-service) should be explored prior to requesting resources from General Funds. For each budget request cycle, the ELC will review the proposal recommended by the CIO Council (CIOC) and approve, disapprove, or reprioritize each specific request prior to submission to the Legislature. At their discretion, the ELC may also add funding requests for new initiatives. The ELC is responsible for ensuring the budget request is sufficient to maintain the IT operations of the State.

COBIT states that investment management is optimal when:

> "Industry good practices are used to benchmark costs and identify approaches to increase the effectiveness of investments. Analysis of technological developments is used in the investment selection and budgeting process. The investment management process is continuously improved based on lessons learned from the analysis of actual investment performance. Investment decisions incorporate price/performance improvement trends. Funding alternatives are formally investigated and evaluated within the context of the organization's existing capital structure, using formal evaluation methods. There is proactive identification of variances. An analysis of the long-term cost and benefits of the total life cycle is incorporated in the investment decisions."

Statewide IT Policies. The ELC reviews and approves IT/IRM and business transformation-related policies that apply across all Departments within the State. Such policies include program and project management methodologies for IT/IRM and business transformation initiatives, IT/IRM acquisition, and records management policies, among others.

The COBIT criteria for optimal IT Policy management are:

> "The information control environment is aligned with the strategic management framework and vision and is frequently reviewed, updated and continuously improved. Internal and external experts are assigned to ensure that industry good practices are being adopted with respect to control guidance and communication techniques. Monitoring, self-assessment and compliance checking are pervasive within the organization. Technology is used to maintain policy and awareness knowledge bases and to optimize communication, using office automation and computer-based training tools."

Major Initiatives. Major Initiatives are those IT/IRM and business transformation initiatives that involve multiple Departments, cost millions of dollars, or take years to implement. In the past, each Department has undertaken major initiatives independently. While when looked at as individual projects, each one of these efforts had merit, the State can no longer afford to pursue major initiatives without coordination and sharing among the Departments. The ELC evaluates and approves major initiative proposals, and has oversight responsibility for the management and execution of these initiatives.

COBIT defines optimized project management as:

> "A proven, full life cycle project and program methodology is implemented, enforced and integrated into the culture of the entire organization. An ongoing initiative to identify and institutionalize best project management practices is implemented. An IT strategy for sourcing development and operational projects is defined and implemented. An integrated project management office is responsible for projects and programs from inception to post-implementation. Organization-wide planning of programs and projects ensures that user and IT resources are best utilized to support strategic initiatives."

3.1.3.2 RESPONSIBILITIES OF VOTING MEMBERS

1. Voting members are responsible for representing their Department, taking into consideration the interests of the State as a whole, in developing and maintaining the State enterprise and segment architectures.

2. Additionally, voting members are responsible for ensuring that they, or their pre-approved designee, are in attendance for meetings where voting may be required. This will be communicated ahead of the meeting via the agenda.

3.1.3.3 RESPONSIBILITIES OF THE CHIEF OF STAFF/ELC CHAIR

1. Presides over meetings and enforces this Charter.

2. With the assistance of the CIO and OIMT Staff, coordinates, schedules, and establishes the agenda for ELC meetings.

3. Ensures that proposed changes to the Charter are approved by the ELC before implementation.

4. Maintains the list of appointed members and ensures that those voting are members or designees appointed by their respective office directors as required by this Charter.

5. Establishes the advisory members of the ELC and other advisors as requested.

6. With the assistance of the CIO and OIMT staff, keeps the ELC informed of Hawai'i's IT strategy, architecture, initiatives, and policies and any proposed changes thereto.

3.1.3.4 RESPONSIBILITIES OF THE CIO AND OIMT STAFF

1. Provides guidance and assistance to IT/IRM and business transformation project sponsor offices in preparing the information that must be submitted for ELC reviews.

2. Provides advisory members and speakers to the ELC.

3. Provides support to the ELC for meeting arrangements, correspondence, recordkeeping, publication of minutes, and other logistical requirements as needed.

4. Maintains the Enterprise Alignment Database (EAD)/ Governance Tool to be used as a reference by the ELC.

3.1.3.5 RELATIONSHIP TO OTHER GOVERNANCE BOARDS

1. The ELC is the senior governance body in the State, accountable directly to the Governor. Its decisions shall be held binding by the CIOC, the State CIO, and OIMT.

2. Every document, policy, or initiative that the ELC will be asked to review and approve will have already been approved by the CIOC.

3. The ELC will consider recommendations made by the IT Steering Committee in its deliberations, but ultimately the decisions of the ELC will be based on its members' own perception of the best interests of the State.

3.1.4 METHODS AND PROCEDURES

This section describes the ELC's methods and procedures for meetings and communications.

3.1.4.1 MEETINGS

The ELC shall meet at least once per quarter, typically in the last month of each quarter, and as often as necessary to accomplish its purpose. Agendas will be distributed electronically to the ELC membership prior to the date of the meeting, but the primary purpose of each meeting is in alignment with the State's fiscal year. In general, the meeting topics will be as follows:

- December – Supplemental Budget Submission
- March – Architecture/Portfolio Review
- June – IT Strategic Plan/Annual Operating Plan
- September – Strategic Priorities

Meetings will be scheduled for three hours.

3.1.4.2 MEETING ABSENCE

In the event that a member cannot attend a meeting, the designee may cast proxy votes during the meeting, providing the designee has been pre-approved by the CIO.

3.2.4.3 MEETING GROUND RULES

The Chair presides over the meetings. The ELC uses consistent criteria for evaluating and approving IT/IRM and/or business transformation initiatives, including changes to the EA. Decisions are made by a simple majority vote of the members present. The Council will proceed with voting with the members present and the vote will be recognized by all members as valid.

3.1.4.4 MEETING MINUTES

The OIMT Staff will prepare and distribute the draft meeting minutes to the membership electronically. Members may provide comments or corrections in the minutes for a two week period after the draft minutes have been distributed. The final minutes will be distributed to the membership again and stored as permanent records for internal viewing and possible distribution to oversight authorities upon request without further approval by the ELC.

3.1.4.5 COMMUNICATION

Meeting invitations, agendas, review documents, and other notices will be distributed by the Chair via email to each member unless other means are requested by individual members. Additionally, agendas, review documents, and final meeting minutes will be posted to the OIMT collaboration site.

3.2 CIO COUNCIL (CIOC)

3.2.1 PURPOSE

The CIOC provides the State's expertise and understanding for investments in business process improvement and IT/IRM. The CIOC is accountable to the CIO, their respective Department Directors, and the ELC. It is responsible for bringing issues related to IT/IRM to the attention of the CIO, making recommendations regarding future plans to the CIOC, tracking initiatives, resolving conflicts among Departments, and providing resources for transformation and IT/IRM initiatives. Related to the five focus areas of IT governance, the CIOC is responsible for:

- Strategic Alignment
  - Functioning as the "idea" entry point for new investment ideas and requirements
  - Agreeing to the aligned business and IT strategy
  - Ensuring the IT organizational structure complements the business model and direction
  - Representing Department needs and priorities
- Value Delivery
  - Reviewing, promoting, and supporting IT/IRM projects and investments in achieving successful outcomes
  - Ascertaining that OIMT has put processes and practices in place that ensure IT delivers provable value to the business
  - Ensuring investments represent a balance of risk and benefit and that budgets are acceptable
  - Stewards Department Solutions and Department-Specific Infrastructure in compliance with Enterprise Architectures and Standards
- IT Resource Management
  - Sponsoring agreements to establish enterprise standards for enterprise-level technology, shared data, and web services
  - Monitoring how management determines what IT resources are needed to achieve strategic goals
  - Ensuring a proper balance of IT investments for sustaining and growing the enterprise
  - Allocating business resources required to ensure effective IT governance over projects and operations
- Risk Management
  - Maintaining awareness about IT risk exposures and their containment
  - Evaluating the effectiveness of management's monitoring of IT risks
- Performance Management
  - Assessing senior management's performance on IT strategies in operation
  - Working with the CIO to define and monitor high-level IT performance

3.2.2 MEMBERSHIP

The CIOC membership consists of the voting of advisory members described below.

3.2.2.1 VOTING MEMBERS

The members of the CIOC are the IT Leads of the Departments of the government of the State of Hawai'i, as listed in the *Policy Plan.* The Chair of the CIOC is the State CIO.

3.2.2.2 ADVISORY MEMBERS

Advisory members are non-voting members who attend meetings as subject matter experts to the Council. They provide recommendations on issues related to, for example, legislative compliance, records management, security, project management, enterprise architecture, and infrastructure impacts and risks associated with specific investments. They advise the CIOC on the technical feasibility of proposed projects, the project's adherence to IT architectures and standards, its relationship to other IT projects, and the reasonableness of the project cost estimates. Advisory members may be government personnel or contractors.

The Chair or any other member of the CIOC may invite other advisory members as appropriate for consultation on the decisions before the CIOC.

3.2.3 ROLES AND RESPONSIBILITIES

This section describes the roles and responsibilities of the CIOC.

3.2.3.1 RESPONSIBILITIES OF THE CIOC

First, the CIOC provides leadership, strategic direction, prioritization, and coordination among the Departments with respect to business transformation and IT/IRM.

The CIOC fosters cooperation and communication, brokers disputes, enables joint action, and engenders commitment from stakeholder across the State.

The CIOC communicates awareness and understanding of business and IT objectives and direction to appropriate stakeholders and users throughout the enterprise.

The COBIT Framework, version 4.1, the state that the optimal state is achieved when:

> "The information control environment is aligned with the strategic management framework and vision and is frequently reviewed, updated and continuously improved. Internal and external experts are assigned to ensure that industry good practices are being adopted with respect to control guidance and communication techniques. Monitoring, self-assessment and compliance checking are pervasive within the organization. Technology is used to maintain policy and awareness knowledge bases and to optimize communication, using office automation and computer-based training tools."

Second, The CIOC is responsible for reviewing, understanding, and recommending to the ELC for approval or disapproval (with comments and required remedial actions) for the items described below.

IT Strategic Plan and Annual Operating Plan. The *IT Strategic Plan* defines the mission, vision, goals, objectives, and performance metrics for how IT contributes to the State's strategic goals, and the related costs and risks. The IT Strategic Plan will address, at a minimum, the following areas:

- Policy and Organization
- Leadership/Management
- Process/Change Management
- Information Resources Strategy and Planning
- IT Performance Assessment: Models and Methods
- IT Project/Program Management
- Capital Planning and Investment Control (CPIC)
- Acquisition
- E-Government
- Information Security/Information Assurance (IA)
- Enterprise Architecture
- Technology Management and Assessment

The *Annual Operating Plan* is a yearly addendum to the Strategic Plan that identifies the specific Initiatives that will be undertaken in that year to achieve the objectives defined in the Strategic Plan, their resource requirements, and their associated performance targets.

According to the COBIT Framework, version 4.1, the optimal state is achieved when:

> "IT strategic planning is a documented, living process; is continuously considered in business goal setting; and results in discernible business value through investments in IT. Risk and value-added considerations are continuously updated in the IT strategic planning process. Realistic long-range IT plans are developed and constantly updated to reflect changing technology and business-related developments. Benchmarking against well-understood and reliable industry norms takes place and is integrated with the strategy formulation process. The strategic plan includes how new technology developments can drive the creation of new business capabilities and improve the competitive advantage of the organization."

Enterprise Architecture (EA). The *Enterprise Architecture (EA)* describes both the current state (As-Is) and the target state (To-Be) of how the State's IT aligns with and supports the business. This information is typically presented in accordance with a series of established reference models: Performance, Business, Service, Data, and Technology. The EA also includes a transition sequencing plan.

COBIT's description of an optimized architecture states:

> "The information architecture is consistently enforced at all levels. The value of the information architecture to the business is continually stressed. IT personnel have the expertise and skills necessary to develop and maintain a robust and responsive information architecture that reflects all the business requirements. The information provided by the information architecture is consistently and extensively applied. Extensive use is made of industry good practices in the development and maintenance of the information architecture, including a continuous improvement process. The strategy for leveraging information through data warehousing and data mining technologies is defined. The information architecture is continuously improving and takes into consideration non-traditional information on processes, organizations, and systems."

Biennial and Supplementary Budget Requests. Hawai'i's budget is determined on a biennial basis beginning each even-numbered fiscal year, with an opportunity for supplemental budget requests to address emergent requirements in the odd-numbered years.

Budget requests must be as specific as possible for both costs and benefits. A sound business case should accompany each request for funding to provide the Legislature. Alternative funding sources (e.g., grants and in-kind donations, Federal funds, fee-for-service) should be explored prior to requesting resources from General Funds. For each budget request cycle, the CIOC will review the proposal recommended by the CIOC and approve, disapprove, or reprioritize each specific request prior to submission to the Legislature. The CIOC may also add funding requests for new initiatives, at their discretion. The CIOC is responsible for ensuring that the budget request is sufficient to maintain the IT operations of the State.

COBIT states that investment management is optimal when:

> "Industry good practices are used to benchmark costs and identify approaches to increase the effectiveness of investments. Analysis of technological developments is used in the investment selection and budgeting process. The investment management process is continuously improved based on lessons learned from the analysis of actual investment performance. Investment decisions incorporate price/performance improvement trends. Funding alternatives are formally investigated and evaluated within the context of the organization's existing capital structure, using formal evaluation methods. There is proactive identification of variances. An analysis of the long-term cost and benefits of the total life cycle is incorporated in the investment decisions."

The CIOC will review and make recommendations to the ELC, IT/IRM and business transformation-related policies that apply across all Departments within the State. Such policies include program and project management methodologies for IT/IRM and business transformation initiatives, IT/IRM acquisition, and records management policies, among others. Any policies that will apply to personnel outside of OIMT and ICSD will be approved by the CIOC.

COBIT criteria for optimal IT Policy management are defined as:

> "The information control environment is aligned with the strategic management framework and vision and is frequently reviewed, updated and continuously improved. Internal and external experts are assigned to ensure that industry good practices are being adopted with respect to control guidance and communication techniques. Monitoring, self-assessment and compliance checking are pervasive

> within the organization. Technology is used to maintain policy and awareness knowledge bases and to optimize communication, using office automation and computer-based training tools."

Major Initiatives. Major Initiatives are those IT/IRM and business transformation initiatives that involve multiple Departments, cost millions of dollars, or take years to implement. In the past, each Department has undertaken major initiatives independently. While when looked at as individual projects, each one of these efforts had merit, the State can no longer afford to pursue major initiatives without coordination and sharing among the Departments. The CIOC is responsible for evaluating major initiative proposals, making recommendations to the ELC, and overseeing the management and execution of these initiatives.

COBIT defines optimized project management as:

> "A proven, full life cycle project and program methodology is implemented, enforced and integrated into the culture of the entire organization. An ongoing initiative to identify and institutionalize best project management practices is implemented. An IT strategy for sourcing development and operational projects is defined and implemented. An integrated project management office is responsible for projects and programs from inception to post-implementation. Organization-wide planning of programs and projects ensures that user and IT resources are best utilized to support strategic initiatives."

3.2.3.2 RESPONSIBILITIES OF VOTING MEMBERS

1. Voting members are responsible for representing their Department, taking into consideration the interests of the State as a whole, in developing and maintaining the NRC enterprise and segment architecture.
2. Additionally, voting members are responsible for ensuring that they, or their pre-approved designee, are in attendance for meetings where voting may be required. This will be communicated ahead of the meeting via the agenda.

3.2.3.4 RESPONSIBILITIES OF THE CIO/CIOC CHAIR

1. Presides over meetings and enforces the Charter.
2. With the assistance of the OIMT Staff, coordinates, schedules, and establishes the agenda for CIOC meetings.
3. Ensures that proposed changes to the Charter are approved by the CIOC before implementation.
4. Maintains the list of appointed members and ensures that those voting are members or alternates appointed by their respective office directors as required by the Charter.
5. Establishes the advisory members of the CIOC and other advisors as requested.
6. With the assistance of the OIMT staff, keeps the CIOC informed of Hawai‘i's IT strategy, architecture, initiatives, and policies and any proposed changes thereto.

3.2.3.5 RESPONSIBILITIES OF THE OIMT STAFF

1. Provides guidance and assistance to IT/IRM and business transformation project sponsor offices in preparing the information that must be submitted for CIOC reviews.
2. Provides advisory members and speakers to the CIOC.
3. Provides support to the CIOC for meeting arrangements, correspondence, recordkeeping, publication of minutes, and other logistical requirements as needed.
4. Maintains the Enterprise Alignment Database (EAD)/ Governance Tool to be used as a reference by the CIOC.

3.2.3.6 RELATIONSHIP TO OTHER GOVERNANCE BOARDS

1. The CIOC will consider recommendations made by the IT Steering Committee in its deliberations, but ultimately the decisions of the CIOC will be based on its members' own perception of the best interests of the State.
2. The CIOC makes recommendations to ELC. In some areas (notably, those specific to IT), the ELC may delegate decision authority to the CIOC, but the ELC maintains ultimate responsibility

3.2.4 METHODS AND PROCEDURES

This section describes the CIOC's methods and procedures for meetings, communications, and charter revisions.

3.2.4.1 MEETINGS

The CIOC shall meet at least once per month and as often as necessary to accomplish its purpose. Agendas will be distributed electronically to the CIOC membership prior to the date of the meeting.

3.2.4.2 MEETING ABSENCE

In the event that a member cannot attend a meeting, the designee may cast proxy votes during the meeting, providing the designee has been pre-approved by the CIO.

3.2.4.3 MEETING GROUND RULES

The Chair presides over the meetings. The CIOC uses consistent criteria for evaluating and approving IT/IRM and/or business transformation initiatives, including changes to the EA.

Decisions are made by a simple majority vote of the members present. The Council will proceed with voting with the members present and the vote will be recognized by all members as valid.

3.2.4.4 MEETING MINUTES

The OIMT Staff will prepare and distribute the draft meeting minutes to the membership electronically. Members may provide comments or corrections in the minutes for a two week period after the draft minutes have been distributed. The final minutes will be distributed to the membership again and stored as permanent records for internal viewing and possible distribution to oversight authorities upon request without further approval by the CIOC.

3.2.4.5 COMMUNICATION

Meeting invitations, agendas, review documents, and other notices will be distributed by the Chair via email to each member unless other means are requested by individual members. Additionally, agendas, review documents, and final meeting minutes will be posted to the OIMT collaboration site.

3.2.4.6 CHARTER REVISIONS

Revisions to this Charter will be made by providing the proposed changes to the CIOC at a monthly meeting. The Council will review the proposed changes and vote for adoption at the next meeting. 3.3 IT Steering Committee

3.3.1 PURPOSE

Act 200, Session Laws of Hawaiʻi 2010, established the Information Technology Steering Committee (ITSC) to assist the CIO with executing his responsibilities. The Act, as amended by Act 84 of 2011, states:

> There is established an Information Technology Steering Committee to assist the chief information officer in developing the State's information technology standards and policies, including but not limited to:
>
> 1. Assisting the chief information officer in developing and implementing the state information technology strategic plans;
>
> 2. Assessing executive branch departments' progress in meeting the objectives defined in the state information technology strategic plans and identifying best practices for shared or consolidated services;
>
> 3. Ensuring technology projects are selected based on their potential impact and risk to the State, as well as their strategic value;
>
> 4. Ensuring that executive branch departments maintain sufficient tools to assess the value and benefits of technology initiatives;
>
> 5. Assisting the chief information officer in developing state information technology standards and policies; and
>
> 6. Clarifying the roles, responsibilities, and authority of the information and communication services division, specifically as it relates to its statewide duties.

The members of the ITSC shall be appointed in equal number by the senate president and speaker of the house of representatives, respectively, and shall include representatives from executive branch departments, including large user agencies such as the Department of Education and the University of Hawaiʻi; the judiciary; the legislature; and private individuals. The CIO shall serve as the chair of the committee and shall ensure that the committee is evaluated periodically.

3.3.2 MEMBERSHIP

As appointed by the Legislature, the voting members of the ITSC are:

- Sanjeev "Sonny" Bhagowalia, CIO
- David Lassner
- Gordon Bruce
- Liane Moriyama

3.3.3 ROLES AND RESPONSIBILITIES

The responsibilities of the ITSC are as indicated by the Hawaiʻi Revised Statues.

3.3.4 METHODS AND PROCEDURES

This section describes the ITSC's methods and procedures for meetings, communications, and applicability of the Sunshine Law.

3.3.4.1 MEETINGS

The ITSC shall meet monthly, typically in the last month of each quarter, and as often as necessary to accomplish its purpose. Agendas will be distributed electronically to the ITSC membership prior to the date of the meeting.

Meetings will be scheduled for one hour.

3.3.4.2 MEETING GROUND RULES

The Chair presides over the meetings. The ITSC is advisory in nature and may provide the CIO with advice, insight, and recommendations on any topic related to IT standards and practices.

3.3.4.3 MEETING MINUTES

The OIMT Staff will prepare and distribute the draft meeting minutes to the membership electronically. Members may provide comments or corrections in the minutes for a two-week period after the draft minutes have been distributed. The final minutes will be distributed to the membership again and stored as permanent records for internal viewing and possible distribution to oversight authorities upon request without further approval by the ITSC.

3.3.4.4 COMMUNICATION

Meeting invitations, agendas, review documents, and other notices will be distributed by the Chair via email to each member unless other means are requested by individual members. Additionally, agendas, review documents, and final meeting minutes will be posted to the OIMT collaboration site.

3.3.4.5 SUNSHINE LAW

In general, the Sunshine Law applies to all state and county boards, commissions, authorities, task forces, and committees that have supervision, control, jurisdiction, or advisory power over a specific matter and are created by the State Constitution, statute, county charter, rule, executive order, or some similar official act.

A committee or other subgroup of a board that is subject to the Sunshine Law is also considered to be a board for purposes of the Sunshine Law and must comply with the statute's requirements.

3.4 WORKING GROUPS

Working Groups are standing bodies that, with the exception of the Executive Steering Group (ESG), are accountable to the CIOC, and which are responsible for planning and oversight of a specific area of the State's IT enterprise. The ESG is accountable to the ELC. The Working Groups are not decisional or governance entities themselves, although via their recommendations to the CIOC, may have a significant influence on the decisions of the larger body. Recommendations of the working groups are presented to CIOC for approval or recommendation to the ELC.

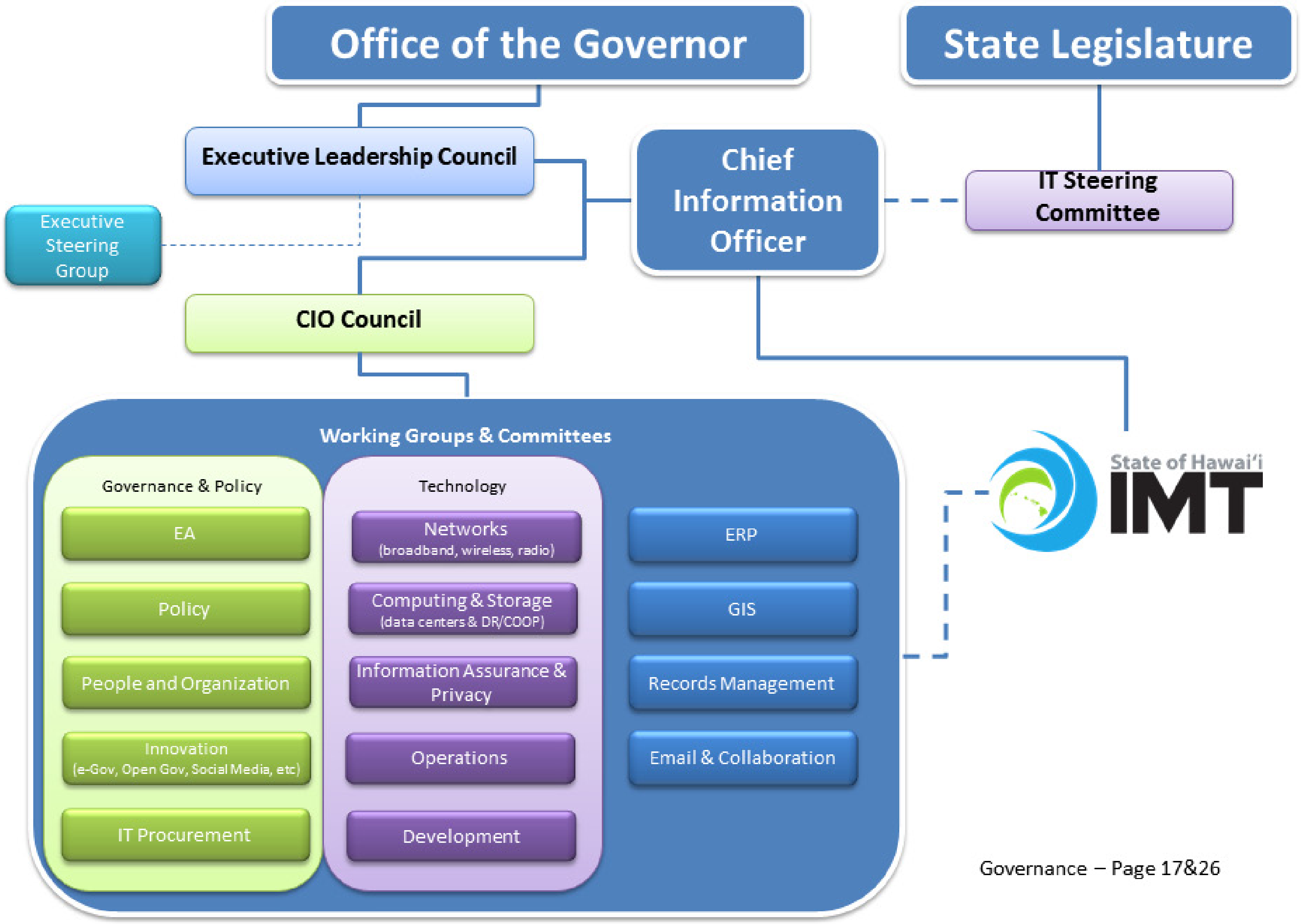
Membership of a Working Group may be composed of any IT support personnel, as designated by their respective Department CIO or DP Lead. In FY12, Working Groups will contribute to the development of the State's *Business and IT/IRM Transformation Strategic Plan*, including governance, methodologies, and enterprise architecture, but they will also continue to meet after the publication of the *Strategic Plan* to guide and oversee the implementation and operations of Hawai'i's IT enterprise.

The contributions of the Working Groups to the Strategic Plan will be critical to the success of Hawai'i's transformation in the coming years. Working Groups will develop the vision for the future state of Hawai'i's business and IT/IRM enterprise. Vision means a description, including diagrams and flowcharts, of the high-level processes and information flows of the ideal future state and the technology that will enable them. The Working Groups will also outline the projects and investments that will need to take place over the next ten years to implement the vision, including the required infrastructure, analysis and business process reengineering, requirements development, and system design, development, and deployment. These projects and investments will need to be sequenced, identifying the dependencies among them and potential risks and constraints. Finally, a rough cost estimate for each investment will be developed that includes personnel, contractors, hardware, software, training, and services.

The work product expected from each working group is a five-to-ten page document that follows a template that will be provided by OIMT. It describes the desired future state, shows the sequence of investments, and provides a cost breakdown. This product will be integrated with the inputs from other working groups and LOBs to create the overall To-Be EA and the Transition and Sequencing Plan for the next ten years. This Plan will in turn serve as the foundation for the State's IT budget requests to the Legislature. Therefore, it is important that the vision be realistic, and as accurate and complete as possible.

Working Groups are organized into three main areas, plus the ESG. These areas are: Governance and Policy, Technology, and Shared Services. In some cases, the size and complexity of a specific topic with a Working Group's domain may necessitate the formation of a sub-working group. If this need seems likely to continue, the CIOC will formally establish a new Working Group to address the specific issue.

Figure 4 depicts the organization of the Working Groups in relation to the CIO, OIMT, and the governance bodies (CIOC, ELC, and ITSC). Descriptions and current membership in each of the Working Groups follow.



Governance – Page 17&26

Figure 4: Working Group Organization Structure

3.4.1 EXECUTIVE GROUP

Group	Description
Executive Steering Group (ESG)	The ESG is composed of senior executives, nominally Department Deputy Directors or equivalents, who provide guidance and recommendations on matters outside of the scope of the CIOC, especially those that relate to business processes and business transformation. Specifically, the ESG reviews informational and decisional briefings prepared for the ELC to ensure quality and completeness when, due to their non-IT related subject matter, they have not been previously approved by the CIOC prior to their presentation to the ELC. Briefs that are not approved (informational) or endorsed (decisional) by the ESG will not be presented to the ELC.

3.4.3 GOVERNANCE AND POLICY WORKING GROUPS

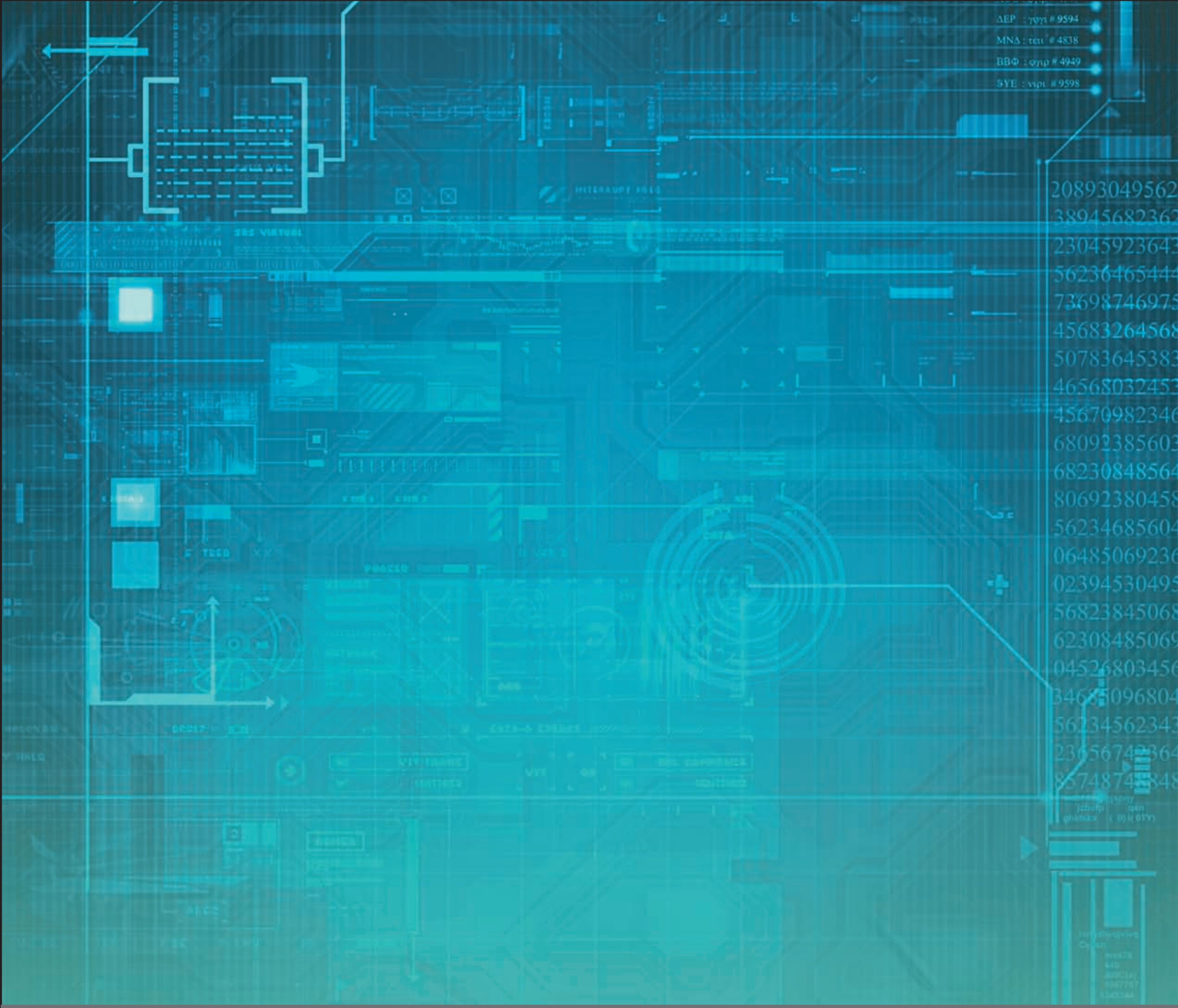
Group	Description
IT Policy Working Group	The IT Policy Working Group reviews and recommends for approval the IT Policies applicable state-wide. Each policy will be reviewed and re-approved at least annually. The Policy Working Group is also responsible for ensuring that any deficiencies in IT policies found by audits or other means are addressed promptly.
Enterprise Architecture Group	The EA Working Group reviews and evaluates the EA of the State of Hawai'i. Hawai'i's EA includes the EBA, the LOBs and business functions the State Government engages in to accomplish its mission of serving the citizens of Hawai'i; the ESA, which describes the systems and applications used throughout the state to support its business processes; the EIA, which describes the structure and content of the information and data used by the state; and the ETA, which describes the hardware and software infrastructure within and upon which the solutions and information reside. Each architecture layer consists of both an As-Is, which describes the current state, and a To-Be, which describes the future state. Once the As-Is has been captured, it will be continually updated to reflect the evolution of the state's business and IT environment. The To-Be will be updated when new ideas or technologies become available and are selected by the EA Working Group and approved by the CIOC for inclusion in the target state. The EA Working Group also reviews and recommends for approval the Transition and Sequencing Plan, the high-level timeline for migrating processes, systems, applications, data structures, and technology to the target state.
People and Organization Working Group	The People and Organization Working Group is responsible for examining and recommending an organizational structure and human resources development plan to the CIOC. This group will plan for the integration of ICSD into OIMT, as well as the longer-term structure for managing the IT support personnel throughout each of the Departments. The Working Group will address not only organizational structure, but staffing levels, reporting relationships, position descriptions, personnel evaluation standards and practices, career development, recruiting and retention strategies, and relationship with the employees' union.
Innovation Working Group	The Innovation Working Group provides a formal mechanism for new ideas to be introduced into the state's business and IT enterprise. The initial focus of the group will be on potential e-Government and Open Government initiatives and social media. The Working Group should find ways to encourage innovation throughout the State and among the citizens through challenges, outreach events, industry days, conducts conferences with thought leaders, etc. Eventually, an Innovation Lab within OIMT could be established as a test bed or incubator for new ideas, which could provide programmatic support for proof-of-concept pilots identified by the group.
IT Acquisition Working Group	The IT Acquisition Working Group will work with the SPO to identify ways to make procurement of IT products and services by the state more agile and responsive to customer needs. Potential areas to explore include supplementing SPO staff with PIMT personnel to assist with processing of IT procurements; proposing changes to acquisition regulations and legislation; negotiating enterprise license agreements, GWACS, and BPAs; and/or establishing a web-enabled product and service catalog with pre-negotiated prices.

3.4.4 TECHNOLOGY WORKING GROUPS

Group	Description
Networks Working Group	The Networks Working Group is responsible for the vision and operation of the state's information networks. This WG oversees local-, wide-, and personal-area networks, wireless data (i.e., 3G/4G wireless mobile, and wi-fi), radio and microwave, satellite, and voice and video transmission. The group is also the CIOC's interface with the Hawai'i Broadband Initiative and the Federal Communications Commission (FCC). The group will coordinate with the Computing and Storage Working Group on the topic of Disaster Recovery and Continuity of Operations (DR/COOP).
Computing and Storage Group	The Computing and Storage Working Group plans and oversees the State's computing and storage environment, including data centers, servers, mainframes, supercomputers, personal computing (i.e., desktops, laptops, tablets, and PDAs), cloud, and peripherals (printers, scanners, cameras, etc.). The group establishes and monitors the technical refresh plan for the State. The group will develop a plan for consolidating the State's data centers over the next ten years as part of the Transformation Strategic Plan. The group will coordinate with the Networks Working Group on the topic of DR/COOP.
Information Assurance and Privacy Working Group	The Information Assurance and Privacy (IA & P) Working Group plans and oversees the State's IA &P programs; the policies, technologies, and standards the state employs to protect the confidentiality, integrity, and availability of the State's information at rest, in motion, and at work via application layer and security and continuous monitoring. The IA&P group will investigate Security-as-a-Service and Privacy-as-a-Service models for potential use by the State.
Service Management and Operations Working Group	The Operations Working Group is responsible for overseeing the day-to-day operations of the State's IT enterprise. They establish the system and service management processes and set performance standards for availability, response time, trouble calls, capacity utilization, energy consumption, etc. The group reviews the previous month's measures and longer-term trends and to formulate and recommend courses of action to improve performance. The group develops and implements the state's service delivery framework, applying ITIL standards and practices to manage service delivery. They are responsible for overseeing operations of the Service Desk, maintenance, and customer service excellence.
Development Group	The Development Working Group oversees the Development, Modernization, and Enhancement projects undertaken by the State. The Development Working Group sets development standards (e.g., project management, performance metrics, SDLC methodology, etc.) and serves as the primary oversight body of development, modernization, and enhancement (DME) projects. The Development Working Group reviews project status, directs PMs to address issues and monitors their resolution, and escalates issues to the CIOC. The group manages by exception, using dashboards and business intelligence tools to pull project information in real time rather than requiring PMs to create periodic reports. The group will also explore ways to make solution development within the state cheaper, better, and faster, potentially through approaches such as code libraries like forge.mil, Agile development, open source, etc.

3.4.5 SHARED SERVICES WORKING GROUPS

Group	Description
Enterprise Resource Planning (ERP) Working Group	The ERP Working Group focuses on the business, information, and technology requirements for the shared services that will comprise the State's ERP solution, namely Finance/Accounting, Human Resources, Supply Chain Management, Project Management, and Customer Relationship Management (CRM). The group will plan and oversee the first phase of the ERP project, develop the Statement of Work (SOW) and hire the consultants to perform the analysis and formal requirements development; manage the system integrator and ERP vendor in configuring and deploying the solution; and continue to evaluate the effectiveness and evolving requirements of the system.
Geospatial Information Systems (GIS) Working Group	The Geospatial Information Systems (GIS) Working Group is charged with developing the Strategic Plan for defining and implementing the desired future state for GIS in the State of Hawai'i. GIS, for the purposes of this Working Group, includes hardware, software, data, and standards for capturing, managing, analyzing, and displaying all forms of geographically referenced information. The group will focus primarily on those GIS systems and data of the State government, but they will also identify opportunities to coordinate with Federal and local governments, non-profit, academic, and commercial organizations and make available to them the capabilities, systems, and data used by the State.
Records Management Working Group	The Records Management Working Group ensures that the State's technology supports the standards established for maintaining official state records, including how records are created, where they are stored, how they are searched and accessed, and how they are disposed. The group oversees scanning/imaging of paper records, long-term storage and archiving, indexing, and cataloging of state records.
Email and Collaboration (Unified Communications) Working Group	The Email and Collaboration Working Group coordinates common standards for email and collaboration solutions within the state. The group will also oversee deployment and operations of the Active Directory (AD) and Domain Name System (DNS). Additionally, this group will investigate potential solutions for voice, video, and messaging capabilities.



4.0 ENTERPRISE ARCHITECTURE METHODOLOGY

4.0 ENTERPRISE ARCHITECTURE METHODOLOGY

In FY2012, the State of Hawai'i embarked on a significant journey to bring about dramatic business and IT transformation to improve efficiency, streamline government processes, and enhance service delivery to constituents. Key initial actions were the hiring of a Chief Information Officer (CIO), the appointment of a Business Transformation Executive, and the establishment of the OIMT. These executives and this organization were given the mandate to lead the overall transformation. In addition, the CIO was tasked with by the Legislature to create the State's Strategic Plan. To support the implementation of the Strategic Plan, the need for an EA and the implementation of EA as a practice was required in order to give structure and direction to the transformation efforts.

4.1 ENTERPRISE ARCHITECTURE (EA) PRACTICE

To understand breadth, depth, and complexity of an EA practice, it is helpful to begin with the definitions of the terms and consider their implications.

ENTERPRISE: An abstract concept of a unit of economic organization or activity; especially a business organization, having a systematic, purposeful activity. *Merriam-Webster*

Within the definition of enterprise, there are some relevant implications:

- The significance of the term unit as it relates to overall organization and activity as a whole; to be able to define boundaries and bring clarity to what is internal to the enterprise and what is external.
- Recognition that end purposes of the "systematic, purposeful activity" do exist and can be assessed and evaluated resulting in indicators and measures of operational performance and mission success.
- The inference that the breadth of consideration contains a significant number of components and subordinate activities, all resulting in a significant level of complexity.
- The abstraction regarding the boundaries of the enterprise—recognizing that one major portion of the Executive Branch (such as a Department) can be considered an enterprise

ARCHITECTURE: The art of designing and building structures involving a complexity of components of various types and how they are organized and integrated into a unifying or coherent form. *Merriam-Webster*

Within the definition of architecture, there are also some relevant implications:

- The significance of the term art indicates that the architecture is not a science and therefore has no single formula in terms of how it is created.

With the definitions and implications of these two words, the goal of the EA practice is design enterprise components to achieve the business goals and objectives to a defined level of effectiveness. Key aspects of the EA practice are to:

- Construct and document the To-Be or future state conceptual architecture of the structure of the enterprise.
- Compare the To-Be state to the As-Is or current state.
- Analyze the gaps.
- Create a *Transition and Sequencing Plan (T&S Plan)* to define a roadmap or transition approach in order to close the gaps between the As-Is and To-Be states and achieve the desired goals, strategies, objectives, and performance measures identified in the Strategic Plan.

Due to the inherent complexity of any enterprise, and by default an EA and everything that is required to achieve the desired transformation, the practice of EA is defined within sub-categories or architectures (i.e., business, information, solutions, infrastructure) in order to create manageable components or layers. This sub-categorization offers different views or perspectives into the enterprise along with its identified challenges; and also enhances the IT stakeholders' analysis of the enterprise one segment at a time. Additional details regarding these sub-categories are described below

Figure 5 illustrates the EA practice as it is defined for the State of Hawai'i.

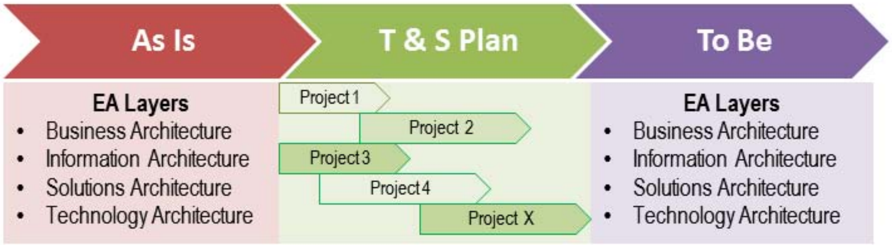


Figure 5: State of Hawai'i EA Practice

The EA helps organize, prioritize, achieve the future state for the IT environment and then manages it going forward. For the enterprise to achieve desired transformation or operational improvements, the EA must be fully integrated with the other elements, functions, activities, or practice areas. These related elements include:

1. The Management and Oversight function that provides a governance structure/process that oversees all related business transformation activities, IT investments, and projects to ensure they achieve desired results.

2. The Strategic Plan that establishes the overarching goals, strategies, objectives, and performance measures for the transformation and drives the requirements for the EA.

3. Projects, defined within the T&S Plan, are approved, funded, and initiated within the proposed sequence and timeframes. These include BPR projects identified to streamline current business processes and system and technology development/implementation projects which are categorized as Triage projects to address immediate needs; Pilot projects to pilot new enterprise capabilities; or Major Initiative Support projects to establish enterprise systems or technologies.

4. The Portfolio Management (PfM) practice as the comprehensive inventory of all IT investments.

Figure 6 provides an overview of this integration and other functions, practice, or program areas.

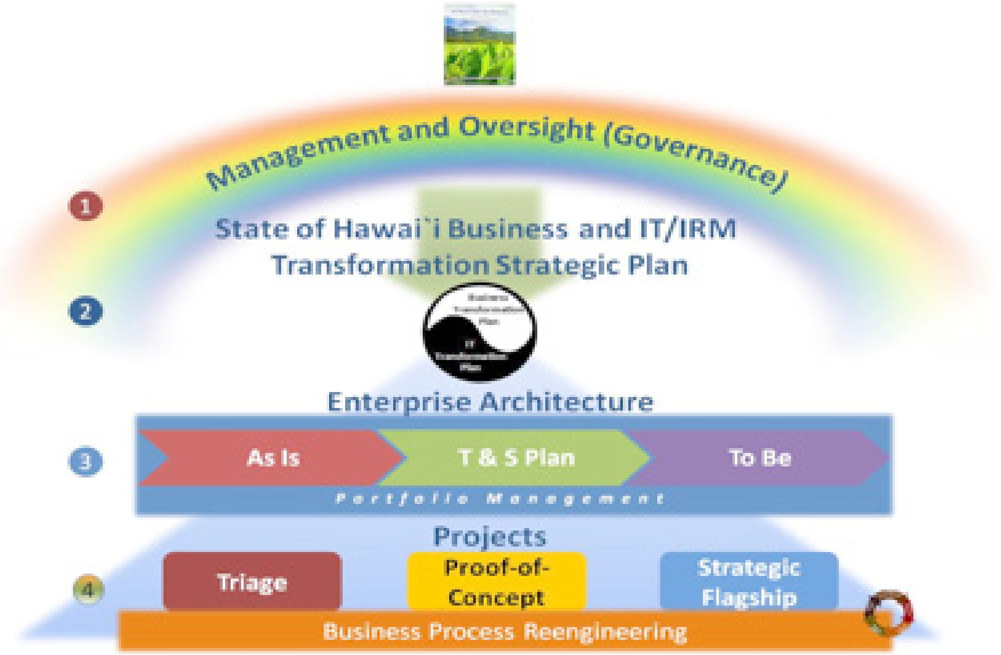

Management and Oversight (Governance)
1
State of Hawai`i Business and IT/IRM
Transformation Strategic Plan
2
Enterprise Architecture
3
As Is
T & S Plan
To Be
Portfolio Management
Projects
4
Triage
Proof-of-Concept
Strategic Flagship
Business Process Reengineering

Figure 6: EA Practice Context for the State of Hawai'i

Finally, once specific projects are initiated, the EA future state guidance in the information, solutions and technical architectures are used as key touch points within the SDLC for consideration and compliance within the context the EA governance and change management process.

The following sections highlight the primary benefits of an EA for the State.

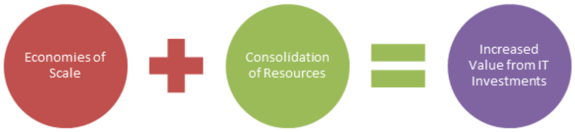
4.1.1 COMPLETE VIEW OF THE IT ENVIRONMENT

A well-defined EA framework enables the State of Hawai'i to define and model the enterprise as an entire system in all its dimensions and complexity on a continuous basis. EA provides a means for the State to collaborate on creation of the future state vision and define path forward for managing the process of change from the current state to the To-Be vision. The EA focuses on key points of integration that are needed in horizontal business services/processes (e.g., availability of critical enterprise information or Shared Services) and in vertical enterprise (or common) system and technology stacks or platforms. The dimensions (i.e., perspectives or layers) include the business and its mission and services, how the enterprise is organized and how it works, and then it is linked to the information, system, and technology investments and services.

4.1.2 STRATEGIC ALIGNMENT OF IT INVESTMENTS TO BUSINESS NEEDS AND PRIORITIES

A well-defined EA framework supports the traceability of key relationships between the business structures (e.g., services and processes) to the supporting information systems and technologies and their effectiveness in meeting business objectives. The goal of the EA process is to delineate the relationships between these elements and ensure they are aligned to produce the desired results.

4.1.3 INCREASE THE VALUE FROM INVESTMENTS


Economies of Scale
+
Consolidation of Resources
=
Increased Value from IT Investments

An EA framework promotes enterprise decisions on standards, which in turn create. Standardizing the IT environment across the enterprise creates economies of scale and provides opportunities to consolidate the environment. These actions simplify the environment and drive increased value from IT investments.

4.1.4 TRANSFORM BUSINESS OPERATIONAL EFFECTIVENESS

While the EA framework facilitates enterprise visioning, collaboration, integration, alignment, and investment decisions, the EA framework also enables greater responsiveness to the ongoing needs for improving and transforming the execution of the business mission, service performance, and operational effectiveness.

4.2 BASIS FOR THE FRAMEWORK, METHODOLOGY, AND DELIVERY PROCESS ASSOCIATED WITH THE STATE'S EA PRACTICE

In creating the EA practice for the State, numerous EA frameworks, methodologies, and delivery processes were reviewed. Careful consideration was given to the approaches that other States and the Federal government have adopted. As part of the selection process, the robustness of the framework, methodology, and delivery process was evaluated and assessed to ensure the complexities of the State's Departmental environments would be accommodated while providing features which facilitate ease of adoption and use; to provide the capability to guide investment in business and technology solutions, and to ensure appropriate alignment with organizational business needs.

The selected framework, methodology, and delivery process approach for the State of Hawai'i and guidance on its implementation are provided below.

4.3 SELECTED EA METHODOLOGY

The State of Hawai‘i EA's Methodology uses the federal government's Federal Enterprise Architecture (FEA) and Federal Segment Architecture Methodology (FSAM) as its foundational framework. The rationale for using the FEA as the foundation is that the Federal Government has a depth of experience and maturity in implementing an EA methodology as well as in development of the EA artifacts themselves in a complex government structure. In addition the FEA/FSAM approach divides the LOBs and addresses the levels (i.e., enterprise, segment, solution) of detail. The Federal government models also relate directly to State government and specifically departmental programs that receive Federal funding. (More information on the FSAM is available at http://www.fsam.gov/.)

Level of Goverment	Architecture Scope	Level Of Detail	Area Of Impact
Enterprise	Agency Department	Low	Strategic
Segment	Lines of Business	Medium	Business
Solution	Functional	High	Operational

Once selected, the State's implementation of the FSAM was tailored, making use of key aspects of other proven methodologies (e.g., defined by Gartner, NASCIO), to align with the guidance provided by the CIO for the State of Hawai‘i and to address inherent risks experienced in EA implementations. The goals of the tailoring included:

- Simplification—adjustments were made to simplify the terminology, the architecture layers and deliverables, and the steps involved in the methodology.
- Streamlining—adjustments were made to incorporate a more incremental and iterative approach to EA development to balance the speed of accomplishment and realization of the downstream benefits in investment decision making with the depth and detail in the EA models and artifacts.

The following guiding principles address the implementation and tailoring activities.

4.3.1 GUIDING PRINCIPLES FOR THE EA METHODOLOGY IMPLEMENTATION AND TAILORING

Consistent with the CIO's guidance on a pragmatic, agile program implementation a few guiding principles to the development of the methodology have been established:

1. Employ various methods to support responsiveness in achieving results and building momentum for the program as a whole.
2. Structure EA development projects consistent with small increments to facilitate making rapid progress.
3. Time-box the EA development work within an increment. Limit the time allotted to any one project to support the time demands that participants have on them, and to ensure results are achieved in a rapid fashion.
4. Use disciplined scope management in each EA project consistent with the segment technique to ensure that the scope of study can be addressed in the planned time allotment.
5. Balance the breadth of scope and level of depth that a specific project addresses consistent with the time allotment. For example, some EA develop tasks will be established as outlined tasks to focus on rapid identification and brainstorming without full details.
6. Plan for iterations to circle back and enhance detail as time allows. Begin with high-level outlines for broader scopes (enterprise or LOB), and follow with iterations to detail subordinate areas.
7. Evolve over time from principles-based guidance towards model based guidance with, as stated by Gartner, "just enough modeling, just in time."
8. Use techniques from Gartner such as the Common Requirements Vision and the Conceptual Architecture Principles to capture statements that outline needed requirements for EA changes and principles guiding decisions and standardizations within the EA. Then as time allows reflect these results in updates to the EA models. Learn to document the essence of the change or the future state vision in statements first, and then models to facilitate moving fast. Consistent with guidance from Gartner, the goal is not to model the world but to concentrate on those aspects of the business process/information system/technical infrastructure that will need to be changed to deliver the new operational performance objectives.

4.3.2 HAWAI'I'S TAILORED EA METHODOLOGY IMPLEMENTATION

Using these guiding principles, the FSAM methodology was adjusted for use in Hawai'i as depicted in Figure 7 below.

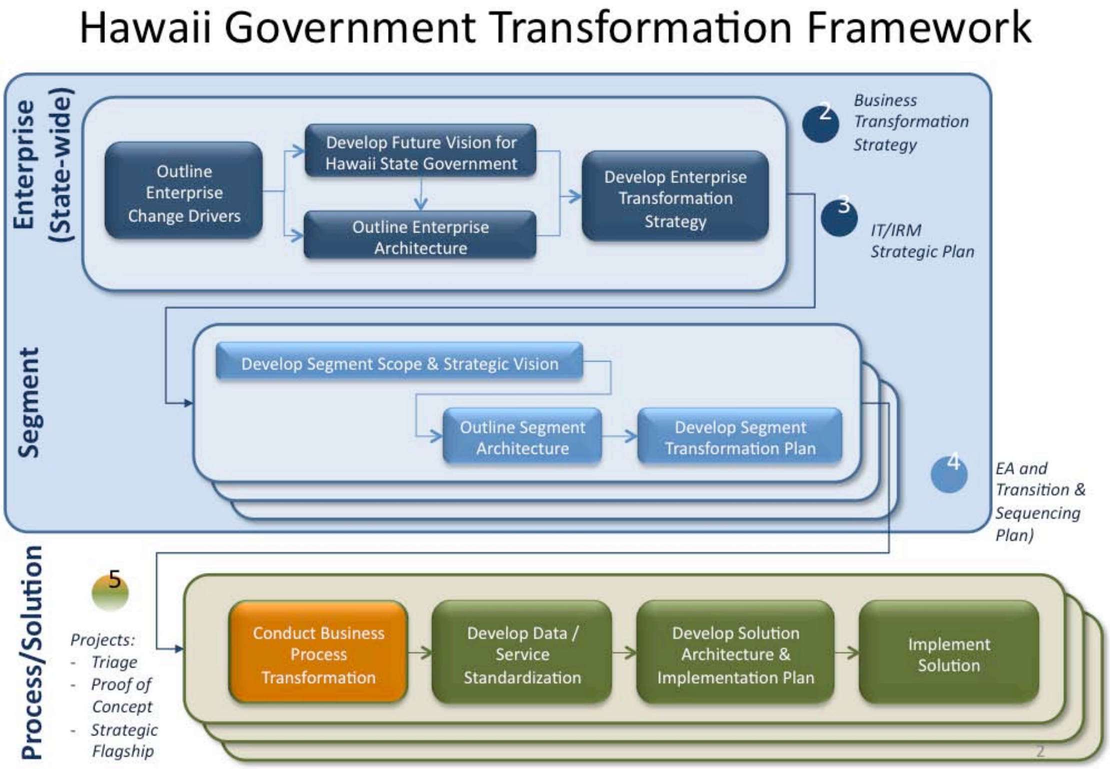

Hawaii Government Transformation Framework
Enterprise (State-wide)
Outline Enterprise Change Drivers
Develop Future Vision for Hawaii State Government
Outline Enterprise Architecture
Develop Enterprise Transformation Strategy
2
Business Transformation Strategy
3
IT/IRM Strategic Plan
Segment
Develop Segment Scope & Strategic Vision
Outline Segment Architecture
Develop Segment Transformation Plan
4
EA and Transition & Sequencing Plan)
Process/Solution
5
Projects:
- Triage
- Proof of Concept
- Strategic Flagship
Conduct Business Process Transformation
Develop Data / Service Standardization
Develop Solution Architecture & Implementation Plan
Implement Solution

Figure 7: State of Hawai'i Two Level EA Methodology

The Hawai'i methodology for EA is a framework based on two levels: 1) an enterprise level that is holistic and state-wide in its view, and 2) a segment level that is based upon the FSAM concept and enables detailed EA development in achievable components along the segment boundaries. Each level has a simplified and streamlined approach as compared to the FSAM. At each level there are two tracks: one focused on the business perspective supported by the senior executives, and the second focused on the information management and technology supported by the CIO and IT managers within each Department. The basic workflow within each level is similar and includes:

1. Identifying the strategic external and internal drivers for change and the associated transformation objectives

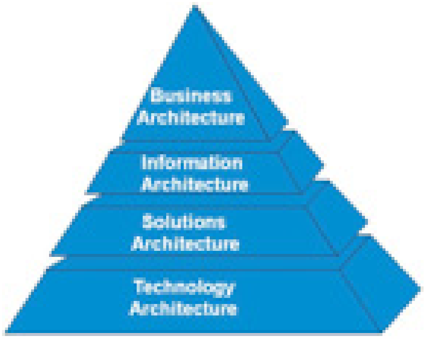
2. Developing the future state vision for business performance

3. Identifying the implications for change on the supporting IT systems and infrastructure and outlining the needed restructuring, i.e., re-architecting

4. Developing the implementation strategy/plan for achieving the objectives

The EA development establishes the overall objectives for integration, sharing, and standardization—identifying the integration touch points horizontally and vertically across the enterprise. The overall structure of the EA is established with a focus on assigning stewardship of key components and identifying stakeholder involvement influenced by the identified integration points. The EA development at the segment level drills down into further detail resulting in greater clarity on defining a full suite of integrated solutions and systems to meet the performance objectives of the segment.

4.4 ARCHITECTURAL LAYERS WITHIN THE EA FRAMEWORK



An integral aspect of the EA is the definition of the architectural layers. The layers facilitate an important objective by decomposing the enterprise into sub-categories. An important characteristic of this layered structure is the flow down of requirements from layer to layer. Within the State of Hawai'i's methodology, the subordinate architectural layers were tailored to be consistent with the traditional the four-layer model described in the Gartner approach. The four layers used within the State of Hawai'i's EA framework are defined below.

4.4.1 ENTERPRISE BUSINESS ARCHITECTURE (EBA)

The EBA layer describes a comprehensive business model within the EA. The business model includes:

- The business mission, services, and performance objectives within the Departments and State
- The associated Service Delivery value chains including support for the citizens who use the services and other government entities that work with the State to deliver services
- The detailed business processes that define how work is done including policies, business rules, and organizational alignment

The top-level component for organizing the EBA is a LOB. The LOBs are subdivided into Core Mission Areas that are citizen-facing services and Support Service Areas that are internally-focused services. The LOB is a critical entity for organizing business operations of the State from a functional perspective independent of the Departments, attached agencies, or programs that perform them in order to promote collaboration across the Departments to bring cross-cutting transformation. The LOBs are used in organizing all stewardship responsibilities for business service/process performance, information quality and availability, and information system functionality, usability, and integration. Stewards for each LOB, generally Department-based, will be identified.

4.4.2 ENTERPRISE INFORMATION ARCHITECTURE (EIA)

The EIA represents the second or information layer within the EA. The EIA begins with the:

- Conceptual information model to promote the identification of common or shared information at the enterprise level and within the LOBs
- Development of standard definitions of the structures and values of common information

The key integration point between the EBA and EIA is the identification of critical information needs within the business process definitions to facilitate information reuse, analysis, and decision-making; and the resulting information definition, structuring, classification, and storage, delivery, and exchange solutions to enable its confidentiality, integrity, and availability.

4.4.3 ENTERPRISE SOLUTION ARCHITECTURE (ESA)

The ESA represents the solution layer of the EA. The ESA focuses on solutions that involve the application of IT systems and products to automate and streamline business processes and information delivery and use. In this context, the term solution may seem analogous to an IT information system or an application. The solution concept used here is somewhat broader in that it may include IT service provision such as a service desk or data center. The key integration touch points for the ESA in relation to the EBA and EIA are associated with the most challenging enterprise issue: delivering solutions that help achieve strategic goals and meet key business process and information needs.

4.4.4 ENTERPRISE TECHNOLOGY ARCHITECTURE (ETA)

The ETA is the fourth and final layer of the EA. The ETA supports and enables delivery of the enterprise solutions through technology. The ETA identifies and organizes the breadth of technologies needed within taxonomy of technology domains, categories, product types, specifies standard protocols, and products for use in the State's technical infrastructure. The key integration point related to the ESA deals with standard solution patterns that specify a technology stack and IT platforms for hosting, managing, and supporting enterprise solutions.

Table 1 identifies each of the architectures, provides a crosswalk to the associated reference models within the FEA, and outlines key features of that layer.

Table 1: Relationship of Architectures to Federal Reference Models

Group	FEA/FSAM Reference Model	Features
Enterprise Business Architecture (EBA)	• Business Reference Model (BRM) • [Business perspective of] Services Reference Model (CRM) • Performance Reference Model (PRM)	• LOB Stewardship • Value Chain • Core Mission Areas| • Internal Support Areas • Horizontal Enterprise Services Layer
Enterprise Information Architecture (EIA)	• Data Reference Model (DRM)	• Management of Shared Data - Enterprise - LOB • Data Stewardship • Data Standardization
Enterprise Solutions Architecture (ESA)	• [IT perspective of] SRM	• IT Services Integration Layers - Enterprise - LOB
Enterprise Technology Architecture (ETA)	• Technical Reference Model (TRM)	• Solution Patterns (Reference Architectures) • Technology Architecture Taxonomy • Guiding Principles • Technology Standards and Guidelines

4.5 TECHNICAL APPROACH FOR EA DEVELOPMENT AND CONTINUAL UPDATE

This section describes the technical approach followed in executing both the enterprise-level and segment-level iterations for EA development. Types of segments that are defined for development in the FY2012 timeframe and associated variations in the detailed segment architecture development approach are also described.

Due to the nature of the biennial budget cycle for the State of Hawai'i and the scope of the enterprise, the target To Be or future state vision has been established for the next ten years. The objective of the future state vision is to portray “a day in the life” experience of key customers (citizens) and stakeholders (Federal and local government officials, contracting/supplier businesses, etc.) in terms of interacting, receiving services from, or doing business with the State.

Note that a fundamental principle regarding the approach for developing the future state vision was unrestricted by any barriers or inhibiters that might exist in the current state. Once the future state vision was established, only then was consideration given to analyzing the gaps that exist between the current state and the future state in order to develop the roadmap of initiatives to close the gap.

A related principle involves recognizing the need to continually maintain or update the current state baseline over the ten-year timeframe in order to readjust the roadmap as required to close the gaps to achieve the future-state vision.

Fundamental Principles for Developing the Future State EA Vision

- Unrestricted by any barriers or inhibitors present in the current state
- Continually maintain and update the current state baseline in order to readjust the T&S
- Business drives the direction

Finally, the most important principle applied to the EA development at both the enterprise- and segment-levels is the dual-track structure that distinguishes and interlaces business (executive) involvement and IT senior management involvement. For any EA to be successful, the business must drive the results. The methodology must be structured to represent the business.

4.6 HIGH-LEVEL EA DEVELOPMENT APPROACH

The top level of the EA methodology for the State is intended to establish the overall structure of all four of the architectural layers and to surface the enterprise-level integration points involving the horizontal or cross-cutting LOB services or value chains, and common or shared information, systems, services, and infrastructure.

Figure 8 illustrates the Business and IT tracks, noted in three principles above, and the activities and associated work products.

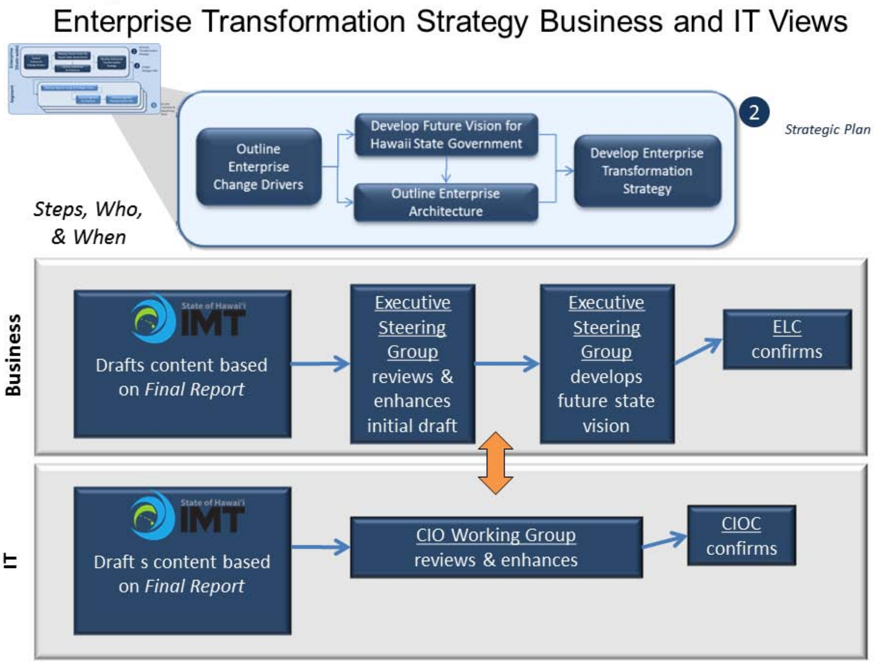

Enterprise Transformation Strategy Business and IT Views
2
Strategic Plan
Outline Enterprise Change Drivers
Develop Future Vision for Hawaii State Government
Outline Enterprise Architecture
Develop Enterprise Transformation Strategy
Steps, Who, & When
Business
IT
State of Hawai'i IMT
Drafts content based on Final Report
Executive Steering Group reviews & enhances initial draft
Executive Steering Group develops future state vision
ELC confirms
Draft s content based on Final Report
CIO Working Group reviews & enhances
CIOC confirms

Figure 8: Enterprise Transformation Strategy

The details of the four steps in the enterprise-level work process are described below.

4.6.1 STEP ONE – OUTLINE ENTERPRISE CHANGE DRIVERS

As part of the development and annual update of the *Strategic Plan,* the external and internal business environment for the State is being characterized with a focus on the forces that are considered drivers for transformation. Techniques typically used in such an evaluation consist of an analysis of internal strengths, weaknesses, external opportunities, and threats (SWOT) analysis resulting in a set of statements that communicate the opportunities for strategic improvement that provide direction for constructing and restructuring the future-state vision for government operations, organizations, and performance. This analysis is performed at the business level by the executive leadership and led by the Business Transformation Executive and then at the IT level by the IT senior leadership (or CIOC led by the CIO).

4.6.2 STEP TWO – DEVELOP TO-BE OR FUTURE-STATE VISION

The development of the future-state vision for Hawai'i is another key activity in the development of the *Strategic Plan*. The executive leadership within the State describes and characterizes the future state of government operations and performance from a business perspective (i.e., not from an IT/IRM perspective). The opportunities for strategic improvement result in constructing or restructuring the how State government should functions. The logical thought progression moves from strategic goals that must be achieved within the future state, business strategies for achieving them, lower-tier strategic objectives, and associated performance indicators or measures (measures that evolve and objectives are reached) that establish the transformation direction.

4.6.3 STEP THREE – OUTLINE ENTERPRISE ARCHITECTURE (EA)

In response to and in parallel with the development of the future state vision for government operations is the initial structuring of the high-level EA. There are two major activities within this step:

1. Capturing the requirements for change within the enterprise information, solutions, and technology infrastructure to achieve the transformation objectives

2. Outlining the key components within each of the architectural layers, their horizontal and vertical integration points, and characterizing those areas impacted by the change requirements

Matrices are typically used to document and maintain the traceability (or line of sight) from strategic transformation objective to EA change requirements, to EA components within the layers affected by the change.

In the initial iteration for the State of Hawaiʻi, the content for the future state of each architectural layer is developed at an outline level (i.e., all the components are being identified two or three levels deep in decomposition for each architecture layer but without fully characterizing the components). The As-Is or current state baseline was captured as effectively as feasible during the *Final Report.*

There are specific approaches used to outline the EA as a whole and the individual subordinate architectures. These approaches are discussed below.

4.6.3.1 CONSTRUCTING THE CONCEPTUAL ARCHITECTURE

The Gartner EA methodology popularized a technique known as conceptual architecture which is used as a foundational framework in starting the development of the EA. The conceptual architecture technique facilitates a starting point by keeping considerations for change and restructuring of the enterprise at a higher conceptual level in an initial iteration of architectural development. This technique focuses on developing statements of principle that communicate the essence of how the overall IT environment must be structured (or restructured) and provide guidance on the ongoing decision making process to achieve that structure. The conceptual architecture helps outline what the essential components need to be, identify new or changed components that must exist, and how the components must interact and integrate in order to achieve the needed requirements for transformation.

Some key concepts and features of a conceptual architecture as articulated in *The Commonwealth of Virginia's Conceptual Architecture* documentation include:

- Providing high-level guidance for aligning business drivers and architectural requirements with the underlying technological components to meet the vision of the Enterprise Architecture.
- Defining a logically consistent set of principles that will guide engineering across domain architectures. (Note: Domain architectures refer to the first-level decomposition or ETA layer.)
- Identifying applicable EA best practices as conceptual architecture principles. These principles are high-level fundamental truths, ideas, or concepts that frame and contribute to the understanding of the EA.
- Deriving conceptual architecture principles from best practices that have been assessed for appropriateness to the State's EA. The justifications and implications of each principle is identified and documented within the context of the State environment, and there is a direct linkage between each principle to one or more of the transformational change requirements.
- Enabling the enterprise to identify strengths and weaknesses in the current IT delivery methods, policies, skills, and organization based on these principles. It further provides a baseline to assess the applicability and appropriateness of the current technology products deployed by the enterprise. Finally, it provides a framework to derive, prioritize, and drill-down into necessary domain architectures.

4.6.3.2 OUTLINING THE ENTERPRISE BUSINESS ARCHITECTURE (EBA)

The following tasks are accomplished in outlining the future-state EBA:

- Establishing the LOB
- Identifying the Core Mission Areas and the Support Service Areas
- Identifying the subordinate business functions and enterprise services within each LOB
- Establishing stewardship policies and principles
- Identifying and obtaining agreement on departmental stewardship and stakeholder assignments
- Establishing a governance framework for making changes to the EBA going forward

4.6.3.3 OUTLINING THE ENTERPRISE INFORMATION ARCHITECTURE (EIA)

The following tasks are accomplished in outlining the future-state EIA:

- Constructing a Conceptual Information Architecture which identifies a decomposition of information subject areas that are consistent with the lines of business and subordinate business services.

- Identifying key subject area relationships that indicate information dependencies across lines of business.

- Augmenting stewardship policies and principles to encompass the information subject areas as associated responsibilities for information quality/integrity, availability, and security.

- Establishing requirements and principles to drive standard enterprise information integration, delivery, analysis, and collaboration solutions.

4.6.3.4 OUTLINING THE ENTERPRISE SOLUTIONS ARCHITECTURE (ESA)

The following tasks are accomplished in outlining the future-state ESA:

- Constructing a notional future state ESA which identifies an optimum set of IT solutions to automate the business and information components of the EBA and EIA.

- Identifying key crosscutting enterprise IT services (e.g., web services) that need to exist within a common services layer.

- Establishing requirements and principles to drive standard enterprise solution patterns, technical integration capabilities, and platforms.

4.6.3.5 OUTLINING THE ENTERPRISE TECHNOLOGY ARCHITECTURE (ETA)

The following tasks are accomplished in outlining the future-state ETA:

- Identifying and outlining requirements for enterprise solution patterns (or reference architectures for standard types of solutions):
    - Developing initial high-priority enterprise-wide solution patterns
    - Standardizing on strategic application platforms and technologies for future applications development, acquisition, and integration
    - Outlining standard development methods, skills development (training) and skills acquisition (contracting), and standard tools/technologies
    - Outlining a communication plan to socialize the standards and guidance within each Department
    - Potential solution patterns include:
        - Web applications
        - Mobile applications
        - Social media systems
        - Workflow services
        - Document management services
        - GIS software platform/technology
        - IT infrastructure management / enterprise system management tools
        - Web services integration
        - Shared databases and master data sets
        - Data analytics systems

- Outlining enterprise technology guiding principles and standards:
    - Agreeing on technology domains and taxonomy
    - Developing guiding principles on technology domain direction and decisions
    - Developing an immediate baseline of current assumptions regarding sunset, legacy, preferred, and standard application platforms, architectural stacks, and technologies
    - Using an involvement approach of a CIO Working Group with separation into Technology Domain Architecture Working Groups and review and confirmation by CIOC

4.6.4 STEP FOUR – DEVELOP ENTERPRISE TRANSFORMATION STRATEGY

The final work product from the Strategic Plan consists of analysis and structuring of actionable focus areas for future initiatives and high level considerations for the timing and sequencing of these initiatives. This should be viewed as the first iteration of the definition of a set of initiatives or projects needed in order to create the future state vision of the State and the EA. These initiatives are further expanded upon during the detailed segment architecture work to populate portions of the T&S Plan that in turn becomes part of the investment portfolio. Thus, the EA outlines the context of determining what projects need to be done, how to scope these projects, profile these projects, and sequence these projects within the T&S Plan for subsequent evaluation, approval, and funding as part of the PfM activities.

Figure 9 below identifies the general work plan for execution of the initial iteration of these tasks in FY2012.

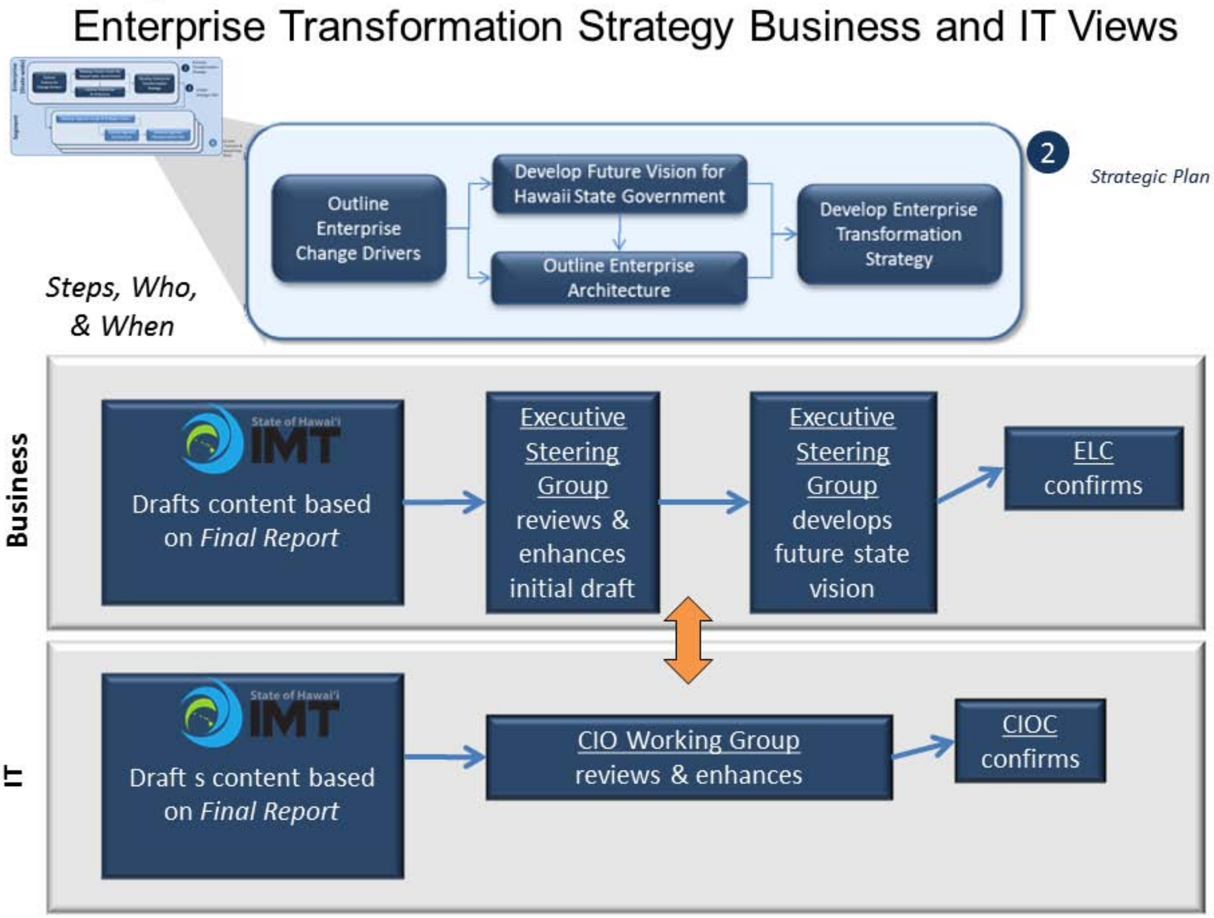

Enterprise Transformation Strategy Business and IT Views
2
Strategic Plan
Outline Enterprise Change Drivers
Develop Future Vision for Hawaii State Government
Outline Enterprise Architecture
Develop Enterprise Transformation Strategy
Steps, Who, & When
Business
State of Hawai'i IMT
Drafts content based on Final Report
Executive Steering Group reviews & enhances initial draft
Executive Steering Group develops future state vision
ELC confirms
IT
State of Hawai'i IMT
Draft s content based on Final Report
CIO Working Group reviews & enhances
CIOC confirms

Figure 9: Enterprise Transformation Strategy

4.7 DETAILED BUSINESS SEGMENT ARCHITECTURE DEVELOPMENT APPROACH

The segment level of the EA methodology for the State is intended to fill in the additional architecture detail for the four architectural layers in a step by step or incremental fashion for the scope of a defined segment at a time. The concept of a segment is used to allow the flexibility of scoping the detailed architecture development in most any direction (e.g., focused on an LOB architecture expansion or a technology domain architecture expansion).

Segments are being defined early on while the iteration at the enterprise level is being worked as the more detailed analysis and architecture development work is planned. Initially, filling in the details of the functioning of the new IT/IRM programs, services, and operations under the leadership of the CIO and OIMT will be accomplished consistent with a segment architecture approach.

Additionally, high-priority areas of the ETA will be developed in this manner. Then focus will shift to executing the detailed architecture development on business segments that are scoped consistent with one or more of the LOBs. These types of segment definitions are shown below in Figure 10.

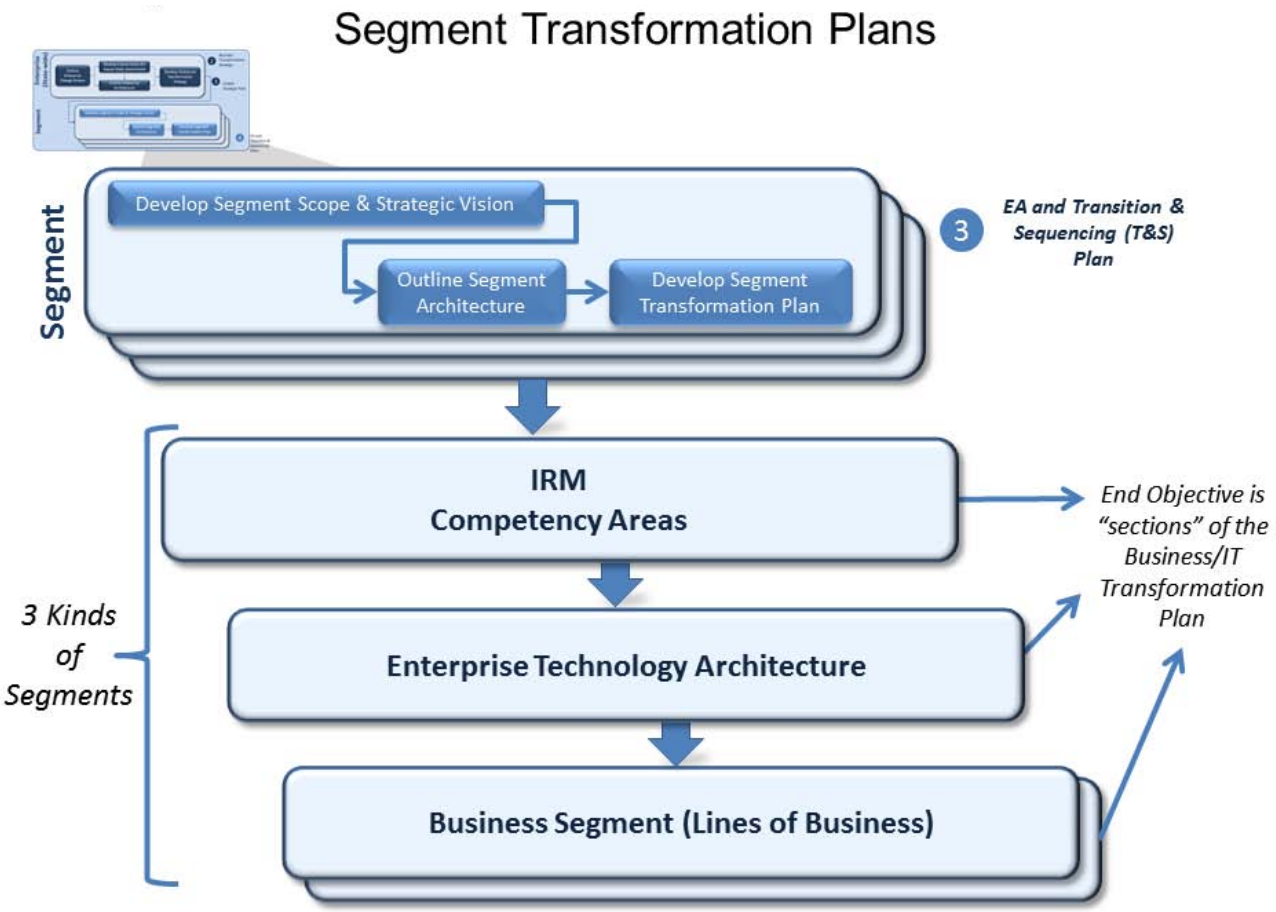

Segment Transformation Plans
Segment
Develop Segment Scope & Strategic Vision
Outline Segment Architecture
Develop Segment Transformation Plan
3
EA and Transition & Sequencing (T&S) Plan
IRM Competency Areas
Enterprise Technology Architecture
Business Segment (Lines of Business)
3 Kinds of Segments
End Objective is "sections" of the Business/IT Transformation Plan

Figure 10: Segment Transformation Plans

Business segment architecture efforts are intended to fill in the additional architecture details for primarily the top three architectural layers for the scope of the defined business segment and to expand upon the segment-level integration points involving the horizontal or cross-cutting LOB services or value chains, as well as the use of common or shared enterprise services and infrastructure. Figure 11 below outlines the Business and IT tracks and the activities and associated work products.

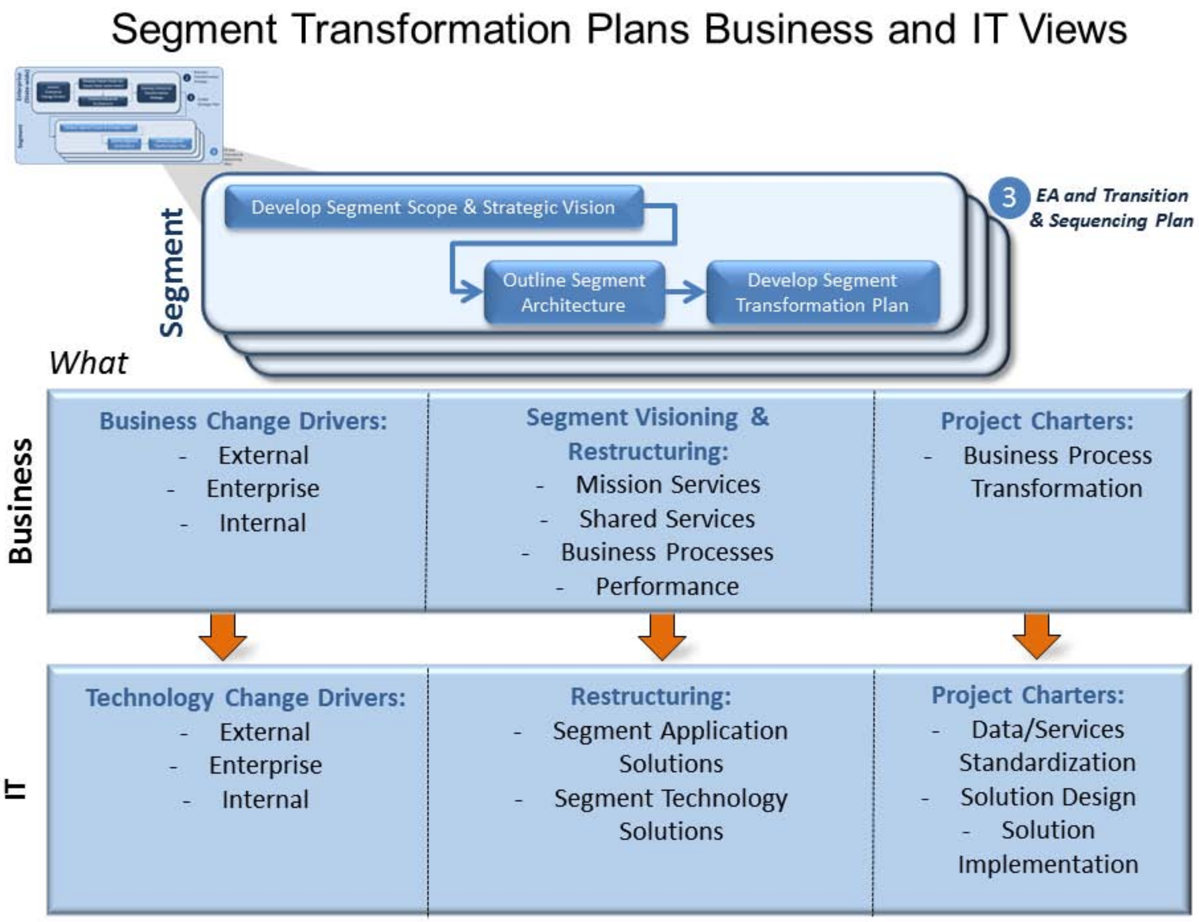

Segment Transformation Plans Business and IT Views
Segment
Develop Segment Scope & Strategic Vision
Outline Segment Architecture
Develop Segment Transformation Plan
3 EA and Transition & Sequencing Plan
What
Business
Business Change Drivers:
- External
- Enterprise
- Internal
Segment Visioning & Restructuring:
- Mission Services
- Shared Services
- Business Processes
- Performance
Project Charters:
- Business Process Transformation
IT
Technology Change Drivers:
- External
- Enterprise
- Internal
Restructuring:
- Segment Application Solutions
- Segment Technology Solutions
Project Charters:
- Data/Services Standardization
- Solution Design
- Solution Implementation

Figure 11: Business Segment Architecture Development – Business and IT Tracks

The following details regarding the three steps in the segment-level work process for business segments are described below. (Note: This work process mirrors the FSAM. Additional details on how to perform the specifics of each step, the questions to answer, and the techniques and tools to document can be found at http://www.fsam.gov/).

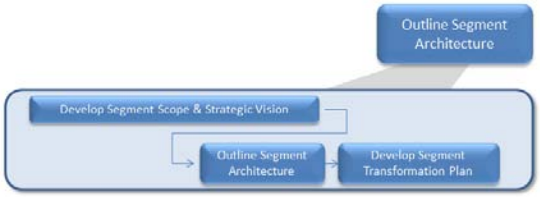
4.7.1 STEP ONE – DEVELOP SEGMENT SCOPE AND STRATEGIC VISION

Using identified strategic drivers at the enterprise level to determine what business segments to build first, Step One of the methodology addresses the launching of the effort with appropriate stewardship and stakeholder participation with an initial activity to determine the scope and strategic intent for the business segment. The segment strategic intent consists of the target state vision, performance goals, and common/mission services and their target maturity levels. This step is designed to allow to team to understand:

- What are the major common/mission services associated with the strategic improvement opportunities?
- Who are the segment stakeholders and what are their needs?
- What are the current segment investments, systems, and resources?
- What are the deficiencies within the segment or the inhibitors to success?
- What is the target state vision for the segment?

Develop Segment Scope & Strategic Vision
Develop Segment Scope & Strategic Vision
Outline Segment Architecture
Develop Segment Transformation Plan

4.7.2 STEP TWO – OUTLINE SEGMENT ARCHITECTURE


Outline Segment Architecture
Develop Segment Scope & Strategic Vision
Outline Segment Architecture
Develop Segment Transformation Plan

Step Two accomplishes two key activities: the definition of business and information requirements for the segment and the definition of the conceptual solution for the segment that meets the business, information, and performance requirements. This step expands the business and information architectures within the segment scope, and addresses the following questions:

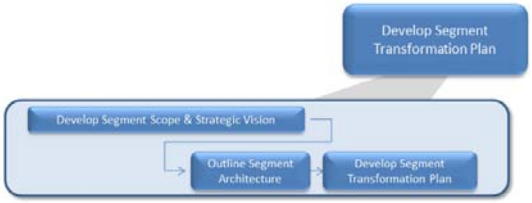
- How well does the current (As-Is) business and information environment perform?
- How should the target business and information environment be designed?
- Have the segment's goals and performance objectives been translated into an actionable and realistic target business and information architecture expressed within business functions, business processes, and information requirements?
- Have the business and information requirements been analyzed and documented to the lowest level of detail necessary to form actionable recommendations?
- Did the business and information analysis provide a synchronized and cohesive set of recommendations?
- Do both the business and IT leadership teams understand the adjustments that are required for the current business and information environments to fulfill the target performance architecture?

Next, the conceptual solution for the segment is restructured to meet the strategic business, information, and performance requirements that align with the future state vision for the involved LOBs. For IT personnel, this is where the development of solution architecture occurs following defined development processes and where system and service transition dependencies are recognized. This step also focuses on alignment with enterprise-level goals for common platforms and centralized computing. This step is integrated with the governance process for the State and provides input and also receives direction from the governance structure established for the State.

Guiding questions for this step include:

- What existing systems and services are deployed?
- How well do the existing systems and services currently support the mission? Which systems and services should be considered for retirement or consolidation or reengineering?
- What does the To-Be conceptual solution architecture need to include to fulfill the desired target performance?
- Are the selected target business functions, systems, and service components reusable?
- Does the conceptual solution architecture support the target performance, business, and data architectures developed in prior steps, along with recommendations for transitioning from the As-Is state to the To-Be state?
- Have the dependencies, constraints, risks, and issues associated with the transition to the future state EA been analyzed to identify alternatives to be considered?

4.7.3 STEP THREE – DEVELOP SEGMENT TRANSFORMATION (TRANSITION AND SEQUENCING) PLAN


Develop Segment Transformation Plan
Develop Segment Scope & Strategic Vision
Outline Segment Architecture
Develop Segment Transformation Plan

Step Three in the creation of the segment is the creation of the *T&S Plan* for the segment. This step outlines the investments in the form of projects (i.e., DME, migration, retirement, consolidation) and prioritization of activities required to close the gaps or transition to the To-Be segment architecture. This step requires the buy-in and participation by business and IT leadership to ensure success for the State.

These improvement investments will be defined by a formal business case submission and will include specific projects or activities to conduct BPR, systems integration or improvements, policy or capability development, or other transformational approaches and requirements[3]. The projects are organized and staged within the overall *T&S Plan* to ensure the transformation to the future state is achieved. The *T&S Plan* also provides visibility into all activities from the following perspectives or views:

- Overall transformation views (Business Architecture: LOB and Business Service, Organization: Department and Program, Portfolio Life Cycle; Solution Architecture, and Technology Architecture)
- Departmental transformation views
- Governance (IT/IRM competency areas) views

[3] The OIMT Portfolio Management (PfM) Methodology further defines the investment process and relationship to EA.

Input for the plan is aggregated from multiple streams: the current known projects from the *Final Report* results, the high-level EA development work, and the segment architecture development work. Figure 12 below identifies the general work plan for execution of the initial iteration of the segment architecture projects in FY2012

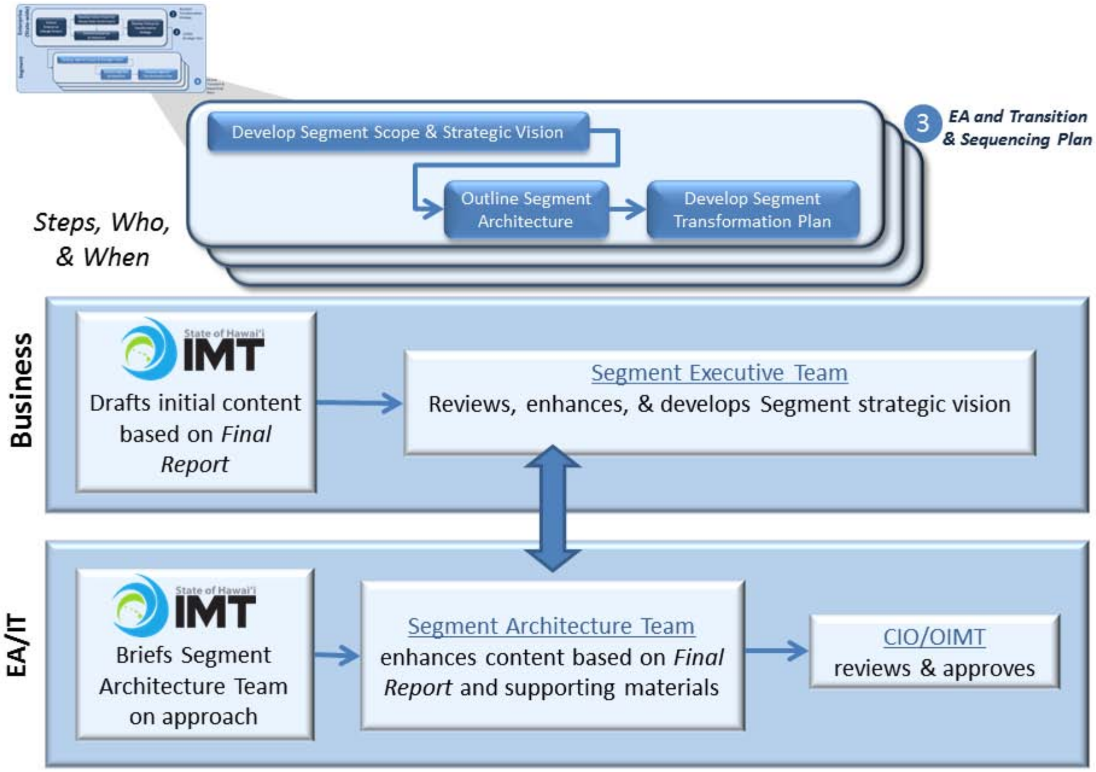

Develop Segment Scope & Strategic Vision
Outline Segment Architecture
Develop Segment Transformation Plan
3
EA and Transition & Sequencing Plan
Steps, Who, & When
Business
State of Hawai'i IMT
Drafts initial content based on Final Report
Segment Executive Team
Reviews, enhances, & develops Segment strategic vision
EA/IT
State of Hawai'i IMT
Briefs Segment Architecture Team on approach
Segment Architecture Team
enhances content based on Final Report and supporting materials
CIO/OIMT
reviews & approves

Figure 12: Business Segment Architecture Development Work Plan

Figure 13 below indicates the involvement of the two teams representing the dual business and IT tracks: the Segment Architecture Business Executive Team and the Segment Architecture IT Team.

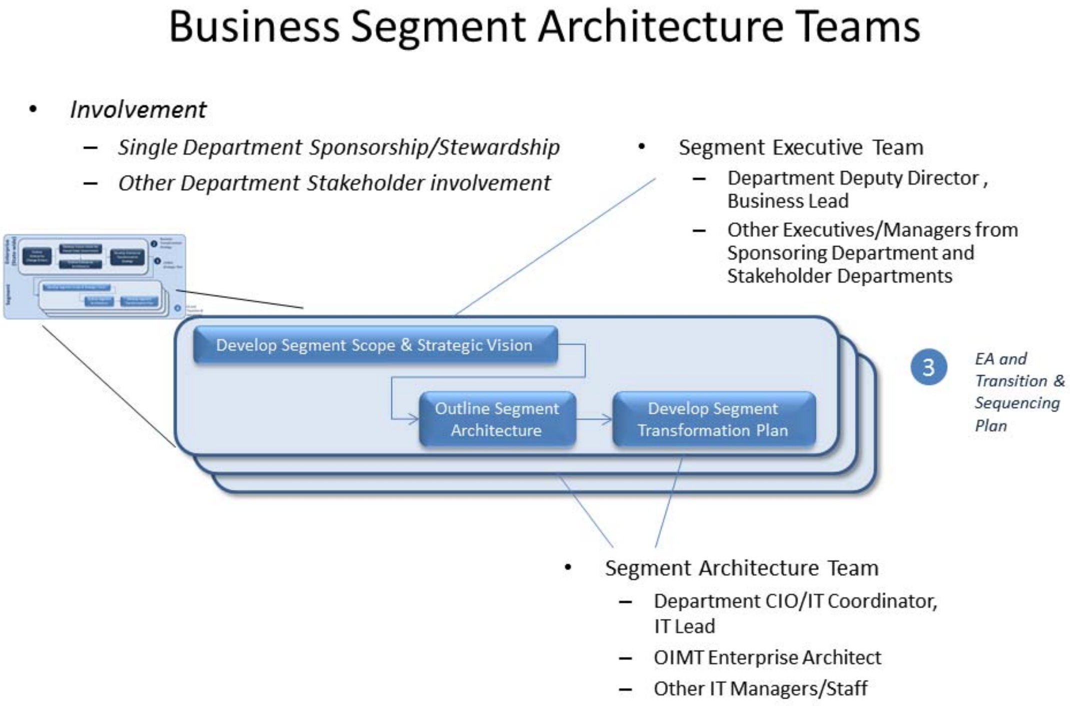

Business Segment Architecture Teams
Involvement
Single Department Sponsorship/Stewardship
Other Department Stakeholder involvement
Segment Executive Team
Department Deputy Director , Business Lead
Other Executives/Managers from Sponsoring Department and Stakeholder Departments
Develop Segment Scope & Strategic Vision
Outline Segment Architecture
Develop Segment Transformation Plan
3
EA and Transition & Sequencing Plan
Segment Architecture Team
Department CIO/IT Coordinator, IT Lead
OIMT Enterprise Architect
Other IT Managers/Staff

Figure 13: Business Segment Architecture Development (Involvement Model)

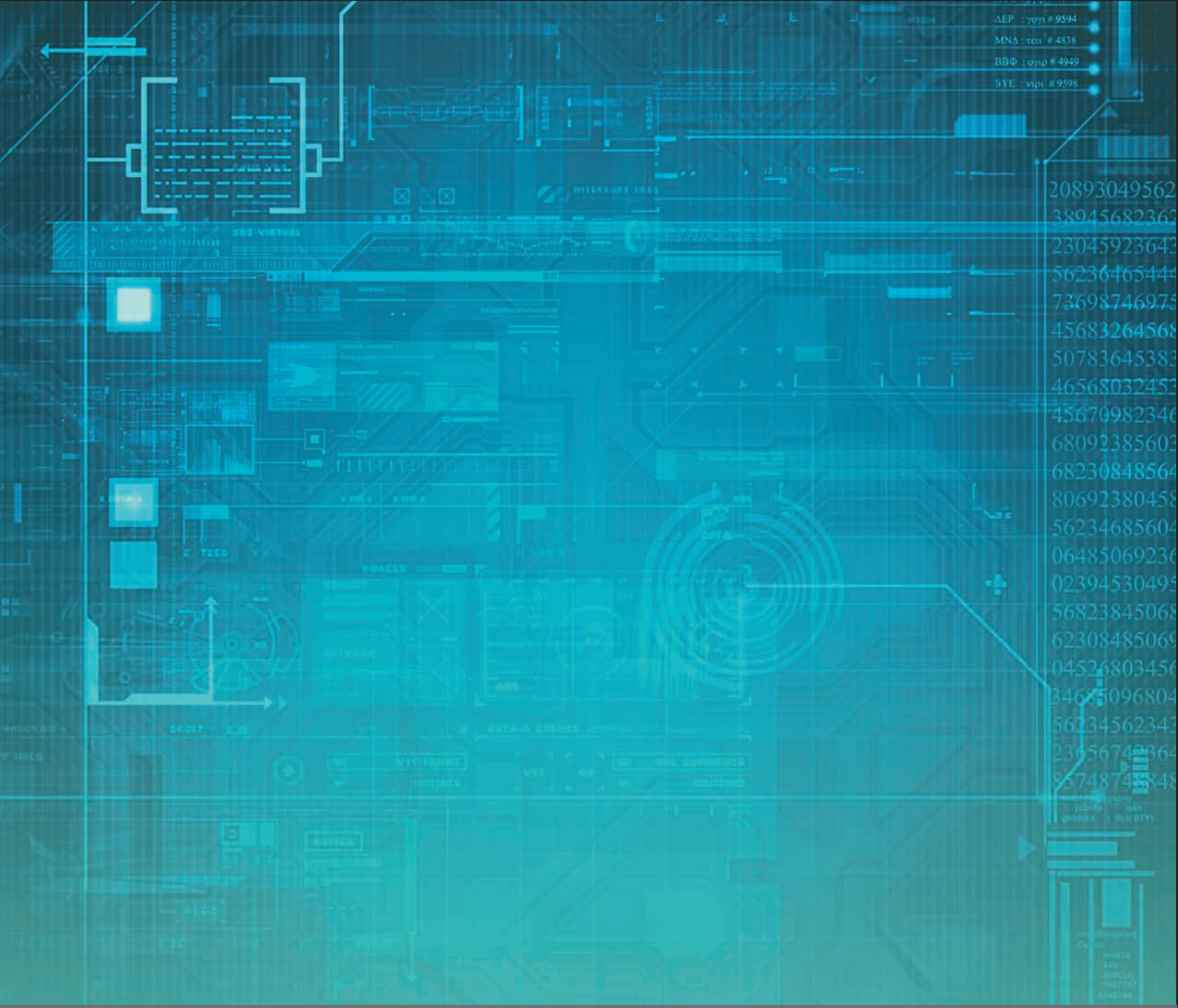
4.8 INSTITUTIONALIZING AND MAINTAINING THE EA PROGRAM

To benefit the State of Hawai'i for the long-term, the State must continually refine the EA in keeping with the needs of the State's *Strategic Plan*. The iterative, incremental, and time-boxed approach is intentional to:

- Balance the tendency to over-analyze or fall into analysis paralysis.
- Ensure that the EA is responsive and delivers direction that can be acted upon and achieved in a timely fashion.

A successful EA is not a one-time deliverable or effort but an ongoing management discipline featuring the continual evolution of alignment with the evolving business and transformation needs and the priorities in order to achieve the future state EA.

Note: This document communicates the approach for the initial major annual iteration to develop the State's EA for FY2012. OIMT will reestablish the new priorities for subsequent EA refinement for FY2013 and beyond.



5.0 PORTFOLIO MANAGEMENT (PFM)

5.0 PORTFOLIO MANAGEMENT (PFM)

The Portfolio Management (PfM) strategy is to create and maintain an understanding of all investments (and any subsequent projects) within the State in terms of the performance, risk, service provided, and return on investment (ROI) to support prudent and well-informed investment decisions that align with the long-term goals described in the *Strategic Plan* and the *Enterprise Architecture.*

The goal of PfM is to ensure that all IT investments within the State of Hawai'i are:

- Recorded in an information repository or portfolio as they are being conceived
- Judged based on their alignment with the Strategic Plan and EA and their benefits to the state in terms of mission accomplishment and best value
- Selected/approved, delayed, or denied using the portfolio information and an assessment process

The objectives of PfM include:

1. Develop an inventory or portfolio of all current programs, investments, Steady State (SS) operations and maintenance (O&M) activities; development, modernization, or enhancement projects; or initiatives.
2. Continually add new investment "ideas" to the portfolio in an iterative manner to ensure early visibility of Departmental IT needs and requirements and the ability to address needs from a statewide perspective, as appropriate.
3. Continually add new investment proposals to the portfolio based on investment dollar thresholds and/or streamlined procurement directives.
4. Provide appropriate analytic and data mining capabilities to assess investment information in a variety of views (e.g., statewide, business or organizational/department, architectural) and to support effective IT investment review, planning, prioritization, resourcing, reporting, and approval.
5. Provide viable rationale for IT investment requests as part of the budget planning and Legislative approval cycle.
6. Eliminate or minimize ad-hoc or one-off investment solutions that do not align with the EA and the strategic direction.
7. Manage all projects with the appropriate level of rigor using a formalized project management methodology (PMM) and control and monitor all SS O&M activities by applying the formalized configuration and change management processes.

5.1 CRITICAL SUCCESS FACTORS AND PERFORMANCE MEASURES FOR THE PORTFOLIO

To be successful, the State's IT investment management processes should generally include the following elements:

- Key organizational decision makers (e.g., Executive Sponsor, CIO, CIOC, or ELC) are committed to the process and are involved throughout each project's life cycle.
- Projects are assessed jointly by program, financial, and IT managers.
- The investment management process is repeatable, efficient, and conducted uniformly and completely across the State.
- The process includes provisions for continually selecting, managing, and evaluating projects in the investment portfolio.
- Decisions are made consistently throughout the process using uniform criteria.
- Decisions are driven by accurate and up-to-date cost, risk, and benefit information.
- Decisions are made from an overall mission focus. (There is an explicit link with the goals and objectives established in the State and in the IT Strategic Plan or annual operational plans and with the EA).
- Accountability and learning from previous projects is reinforced.
- The emphasis is on optimizing the portfolio mix in order to manage risk and maximize the rate of return.
- The process incorporates all IT investments, but recognizes and allows for differences between SS and DME project types (mission critical, administrative, infrastructure) and initiatives.
- The portfolio is reviewed when economic conditions or new administrations introduce new strategies and directions.
- Individual investments are designed to clearly identify and show the cause-and-effect relationship between inputs, outputs, and outcomes.

5.2 ROLES AND RESPONSIBILITIES

The following describes the roles and responsibilities for the individuals and organizations involved in PfM and investment review, planning, prioritization, resourcing, reporting, and approval.

5.2.2 CHIEF INFORMATION OFFICER (CIO)

The CIO is responsible for:

- Establishing the methodology and procedures to capture and review portfolio information
- Ensuring PfM is developed and maintained by the designated OIMT Investment Portfolio Manager (PfMgr)

- Providing management oversight for the complete IT portfolio
- Establishing and maintaining investment thresholds for review purposes in concert with the CIOC, ELC, and IT Steering Committee
- Approving investments of less than $100K
- Reviewing all IT investments initially as part of the Select Phase and then monitoring approved investments as part of the Control and Evaluate Phases in conjunction with the CIOC
- Making recommendations to the ELC regarding IT investment proposals
- Supporting IT investment requests (post ELC approval) through testimony before legislative committees and in discussions with legislators

5.2.3 EXECUTIVE LEADERSHIP COUNCIL (ELC)

The ELC is responsible for:

- Reviewing CIOC investment and prioritization recommendations for all investments greater than $1M
- Selecting, denying, or delaying CIOC investment recommendations
- Participating in periodic reviews of the approved investments that are >$1M as part of the Control and Evaluate Phases of investment management

5.2.4 CIO COUNCIL (CIOC)

The CIOC is responsible for:

- Recognizing and reporting investments not represented in the investment portfolio to allow for follow-up by the OIMT Portfolio Manager
- Reviewing CIOC investment and prioritization recommendations for all investments greater than $100K
- Ensuring proposed investments are aligned with Strategic Plan and EA and assessing/scoring the level of alignment
- Ensuring the risk ranking for all investments is accurate and that mitigation plans are implemented
- Recommending alternative approaches/solutions to proposed investments that leverage existing solutions and/or resources more effectively and/or represent a statewide solution
- Delaying investment proposals to allow the Organizational Investment Sponsor or Owner (Executive Sponsor) to gather additional information and/or assess alternate solution recommendations/considerations
- Selecting, denying, or delaying selection for investment proposals of $100K-$1M
- Recommending selection/denial actions to the ELC for investment proposals greater than $1M
- Ranking/prioritizing recommended investments of $1M for the ELC
- Appointing working groups, as needed, to facilitate more detailed investment reviews
- Participating in periodic reviews of the approved investments that are >$100K as part of the Control and Evaluate Phases of investment management

5.3 OIMT INVESTMENT PORTFOLIO MANAGER (PFMGR)

The OIMT PfMgr is responsible for:

- Managing and maintaining the investment portfolio throughout each investment's life cycle
- Interfacing with the Executive Sponsor, OIMT, CIO, and CIOC regarding PfM and investment proposal information, developing cost estimates, and supporting business case development
- Maintaining the PfM Methodology
- Ensuring investment information is correct, complete, and appropriately updated within the investment portfolio
- Serving as the OIMT technical expert for the PfM tool
- Analyzing investment portfolio information to support the Select Phase of the investment management process
- Ensuring accuracy and appropriate completeness (depending on the stage or the investment idea) of investment proposals and the supporting business cases
- Recommending alternative solutions, application or system retirements, and potential opportunities for information sharing based on understanding of the state-wide portfolio
- Preparing reports for OIMT, CIO, CIOC, and ELC, as appropriate
- Ensuring project activities for an investment remain in alignment with the CIOC and ELC approvals as part of the Control Phase
- Scheduling periodic progress reviews for the CIOC and/or ELC with the Executive Sponsor or PM as part of the Control and Evaluate Phases
- Serving as the administrative resource to the CIOC and ELC relative to PfM issues, decisions, recommendations, and Executive Sponsor notifications

5.4 EXECUTIVE SPONSOR

The Executive Sponsor is usually a member of the Department's or organization's leadership and is responsible for:

- Ensuring the organization follows the dollar boundaries (<$100K; $100K-$1M; >$1M) for investment actions and documentation

- Ensuring new investment proposals are appropriately documented and justified in preparation for the Select Phase of the investment management process with:
  - Accurate and current portfolio information
  - A business case
  - A risk assessment

- Ensuring the organization's existing projects (regardless of life cycle status) are complete within the OIMT investment portfolio

- Ensuring that portfolio components (i.e., projects, programs, applications, or systems) are evaluated on an annual basis and receive an appropriate level of funding to support its project life cycle stage (i.e., support SS or DME, or retirement)

- Addressing all recommendations issued by the CIOC and/or ELC relative to alternate approaches, denials, or delays and follow defined processes for the appeal/re-submission of any investment proposals, as appropriates

- Working collaboratively with the OIMT PfMgr

- Participating in progress reviews as part of the Control Phase and address any CIOC or ELC recommended corrective actions

- Participating in reviews associated with the Evaluate Phase and address any COIC or ELC recommendations and apply lessons learned, as appropriate

- Ensuring procurement requests contain CIOC or ELC approval documentation

5.5 INVESTMENT/PROJECT OR PROGRAM MANAGER (PM)

The PM is responsible for:

- Coordinating with the Executive Sponsor and PfMgr on project information

- Supporting business case development or updates for new investment proposals, as appropriate

- Updating newly approved investment information within the investment portfolio as it becomes available relative to subsequent projects

- Supporting evaluation and update of project components (i.e., projects, programs, applications, or systems) on an annual basis and recommending an appropriate level of funding for its life cycle stage (i.e., support SS or DME, or retirement)

- Ensuring project activities remain in alignment with the ELC approved investment

- Submitting CIOC and/or ELC investment approval documentation with any procurement request

5.6 STATE PROCUREMENT OFFICE (SPO)

The SPO, or its designee, is responsible for:

- Ensuring that all IT procurement requests have received investment approval from the ELC prior to the acquisition actions

- Denying IT procurement requests that do not have appropriate CIOC or ELC investment approvals ($100K-$1M and >$1M respectively) and alerting the PfMgr and CIO of any denials

5.7 DEPARTMENT OF BUDGET AND FINANCE (B&F)

The B&F is responsible for:

- Ensuring that IT investments submitted as part of the budget process have been selected by the CIOC and/or ELC prior to inclusion in the Governor's budget submittal

- Alerting the CIO regarding investments submitted without selection by the CIOC and/or ELC

- Notifying the CIO about investments that were not included in the Governor's budget submittal.

5.8 INVESTMENT PORTFOLIO INFORMATION

Portfolio information requires an inventory (comprehensive list) of all Departmental investments with the ability to sort and report on investments according to a number of information attributes. The information captured for each investment must be descriptive enough to allow for evaluation and comparison to other investments already in the portfolio as well as other proposed investments. Using the captured information along with business case justifications and risk analyses, investments can be assessed from a variety of perspectives or views (e.g., compliance, LOB, departmental/organization, technology, schedule).

Table 2 summarizes the investment information that will be collected and the benefits of that collection.

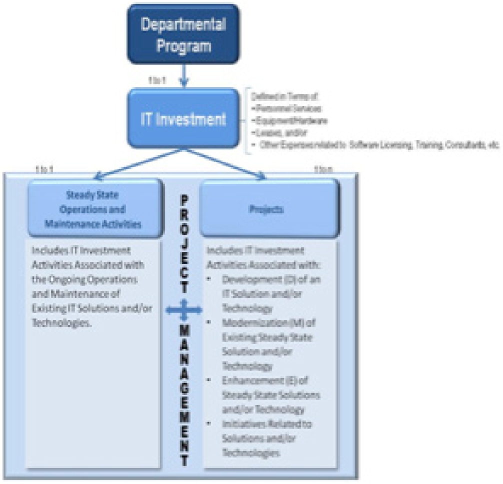

Departmental Program
1 to 1
IT Investment
Defined in Terms of:
•Personnel Services
•Equipment/Hardware
•Leases, and/or
• Other Expenses related to Software Licensing, Training, Consultants, etc.
1 to 1
1 to n
Steady State Operations and Maintenance Activities
Includes IT Investment Activities Associated with the Ongoing Operations and Maintenance of Existing IT Solutions and/or Technologies.
PROJECT MANAGEMENT
Projects
Includes IT Investment Activities Associated with:
• Development (D) of an IT Solution and/or Technology
• Modernization (M) of Existing Steady State Solution and/or Technology
• Enhancement (E) of Steady State Solutions and/or Technology
• Initiatives Related to Solutions and/or Technologies

Table 2: PfM Information Requirements and Benefits

PfM Information Element	Description and Benefit of Information Collection
Investment Basics	
Investment Title	Each investment is uniquely identified by a short descriptive name. This name serves as the key value in the linkage of any one investment to associated projects, architectural elements, programs, etc.
Investment Description	Each investment includes an elaborated description to provide a greater understanding of the nature of the investment.
Primary Sponsoring Organization	Each investment has a primary sponsoring organization. Capturing this information provides an organizational view or reporting capability.
Life Cycle State and Status	Each investment exists at any point in time in exactly one state in its life cycle. The values of the life cycle states can be modified as the actual life cycle is refined, but example states and statuses (non-exhaustive and in no particular order) would include: Draft, Awaiting Initial PfM Review, CIO Review Scheduled, CIO Selected, CIOC Review Scheduled, ELC Review Scheduled, CIOC Selected, CIOC Recommended, ELC Selected, etc. In addition to the life cycle state and status, a date will be kept to track when the investment entered the current state. This information helps manage the portfolio and the activities associated with PfM.
Planned and Actual Investment Start and Completion Dates	Provides dates for investment actions. Supports the overall ranking function as part of the Select Phase and transition and sequencing planning and supports the Control and Evaluate Life Cycle phases.
Business Case and Risk Analysis	At different points in an investment life cycle, some amount of business case and risk analysis is appropriate. There are information elements where a link can be made to these two documents. Templates are provided to guide the level of detail required. These two documents will be key elements of the investment portfolio during the evaluation process.
Progress Review Date	After an investment arrives at a Control state in its life cycle, periodic progress reviews are required to ensure that adequate progress is being made. A progress review date element provides the last date that the investment was reviewed. This date's visibility assists the PfM manager in ensuring that reviews are being conducted as required.
Investment Costs	
Investment Cost	Information elements are provided to capture the total cost (estimated and actual) by fiscal year. In addition, estimates and actuals are separated as being either SS costs or costs associated with DME. In addition, information elements are provided so that these SS and DME costs can be categorized by funding source (revenue bond funds, Federal funds, etc.) and funding category (Personnel Services, Equipment/Hardware, Other, etc.) Recording the funding source and category manager provides the ability to sort and analyze investments along these dimensions.

PfM Information Element	Description and Benefit of Information Collection
Programs and Projects	
Program	In most cases an investment aligns with one program. Each program has a defined set of Measures of Effectiveness (MoEs) that can be used to monitor the improvements being sought as part of the program. The information elements in the PfM provide for the linkage of an investment to multiple programs. The linkage also indicates the level of improvement expected to each MoE, providing a way to quantify the improvement to a MoE being provided by the program.
Project	Provides the projects (by project name) associated with an investment. Each project has a single investment owner.
Strategic Objectives	
Strategic Objective	A statewide set of strategic objectives are defined in the Strategic Plan and these objectives are identified to provide guidance to the evaluation of investment opportunities. Each strategic objective has set of performance measures similar in structure to those developed for individual programs. The PfM information element structure provides for the linkage of each investment back to one or more of these strategic objectives, as well as providing an indication as to the level of improvement expected for an associated MoE.
Certification & Accreditation (C&A) Status	
Certification & Accreditation (C&A) Status	An information element provided for each investment to describe and quantify the state of the investment with respect to the C&A status of any associated software systems.
Enterprise Architecture Alignment	
Enterprise Architecture	The PfM information structure provides a mechanism for linking each element to the corresponding elements of the four EAs (EBA, EIA, ESA, and ETA). This information supports the evaluation of the investment to ensure its alignment with areas of the EA that are being prioritized.

5.9 IT INVESTMENT MANAGEMENT PROCESS

Investment management is a highly integrated process that involves differing life cycles depending on what aspect or phase of the investment is being observed. For PfM, the process of Select/Control/Evaluate is a streamlined view for managing the portfolio in a holistic manner while Architect/Invest/Implement/Measure/Assess/Improve is an equally important process for managing IT investment performance. Both of these approaches align and are used effectively in the Federal government (Figure 14). For the State of Hawai'i, a combination of these two approaches was selected for use to ensure appropriate oversight for each investment.

IT Investment Life cycle[4]	IT Performance Improvement Life cycle
(Pre-select or Analyze)	Architect
Select	Invest
Control	Implement
Evaluate	Measure, Assess, Improve

Figure 14: Life Cycle and Management Perspectives and Alignment

Along with the integration of these two life cycles, a third dimension is required for effective investment portfolio management within the State. This dimension is the State's budget and appropriation process. For the State of Hawai'i, the resulting process is represented by Architect/Select/Invest/Implement/Control/Evaluate4 through Measurement, Assessment, and Improvement[5]. Figure 15 outlines the relational timeline of all three life cycle elements.

[4] Office of Management and Budget: Capital Planning Investment Control (CPIC) is a structured, integrated approach to managing IT investments.

[5] Office of Management and Budget: IT Performance Improvement is a structured, integrated approach to enhancing investment performance.

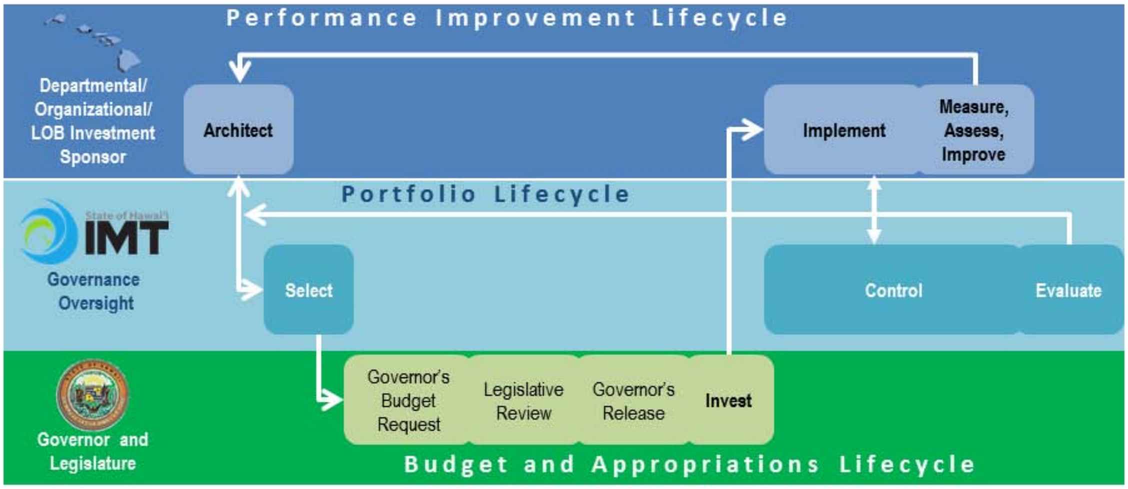
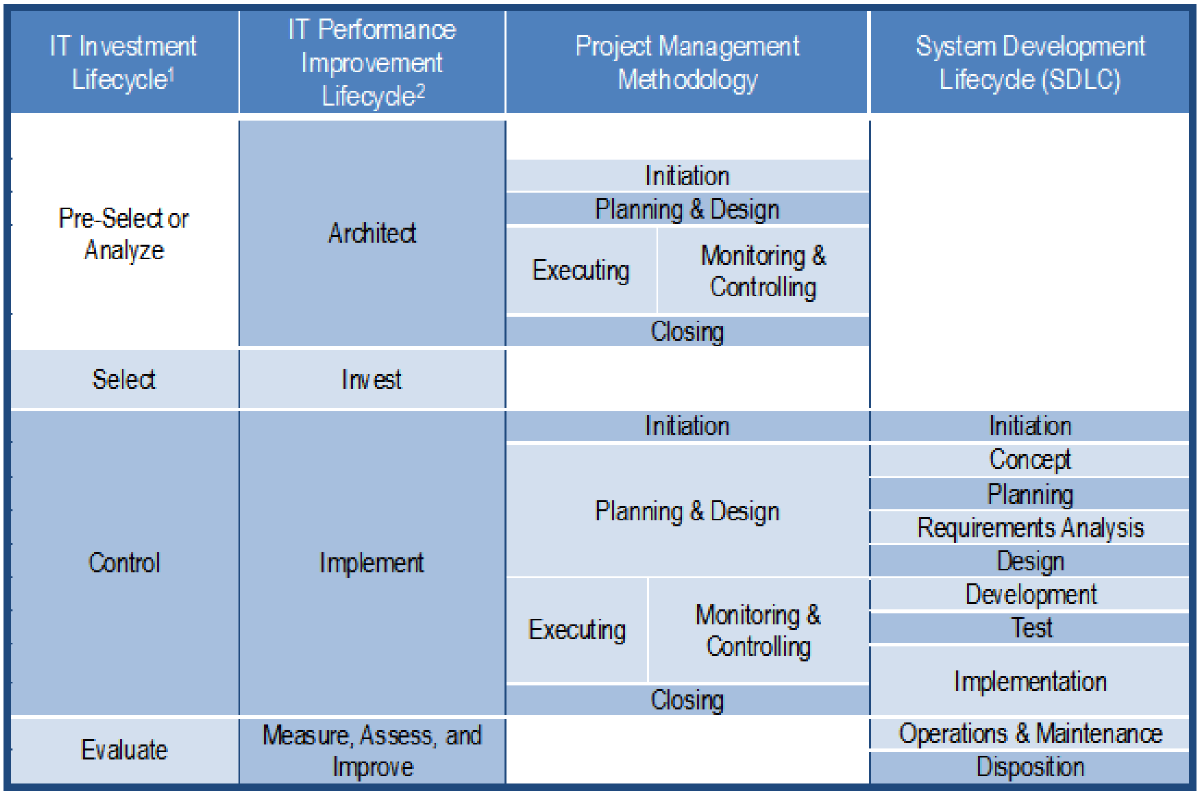


Figure 15: Investment, Improvement, and Budget and Appropriation Life cycle

Finally, there two other very important life cycles that influence and support the management of each investment, the project management (PM) methodology and system development life cycle (SDLC). While these life cycles will be referenced in terms of the significant integration points relative to investments they will be discussed thoroughly in their own methodologies and included as appendices to the Strategic Plan. Figure 16 illustrates the applicable life cycle elements associated with an investment as well as the performance monitoring and development functions.

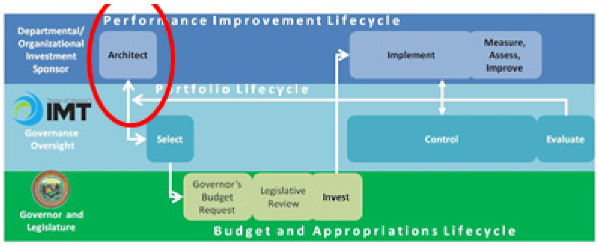


IT Investment Lifecycle[1]	IT Performance Improvement Lifecycle[2]	Project Management Methodology	System Development Lifecycle (SDLC)
Pre-Select or Analyze	Architect	Initiation	
		Planning & Design	
		Executing Monitoring & Controlling	
		Closing	
Select	Invest		
Control	Implement	Initiation	Initiation
		Planning & Design	Concept
			Planning
			Requirements Analysis
			Design
		Executing Monitoring & Controlling	Development
			Test
			Implementation
		Closing	
Evaluate	Measure, Assess, and Improve		Operations & Maintenance
			Disposition

Figure 16: Supporting Methodologies to Manage Selected Investments

The following sections describe each life cycle phase and its relationship to the budget and appropriation process in more detail.

5.10 PRE-SELECT OR ANALYZE/ARCHITECT PHASE AND PROCESS STEPS



This phase describes the timeframe required to initially architect the solution, document information about the proposed investment in the PfM tool, and prepare the business case, and perform a risk analysis depending on the estimated size of the investment. The following provides the process steps:

1. Executive Sponsor identifies the need for an IT investment to support a mission requirement.

2. From the identified need, ideas for IT support are architected and submitted to OIMT via the PfM tool with assistance from the PfMgr. This can be an iterative process that begins with an outline of an investment idea and grows to a fully developed investment request.(Note: Depending on the investment size and complexity, a request may be for funding to more fully architect the investment idea and alternative solutions ideas may be proposed by the PfMgr and OIMT team.)

3. Once the investment is sufficiently defined, it is submitted for review and approval/selection based on the defined thresholds <$100K, >$100K and <$1M, or >$1M.

Generally, for investments of >$100K, portfolio information including business cases will be collected and refined three to six months prior to the beginning of the legislative session depending of the investment size, risks, and benefits. This timing allows for the appropriate selection process by the CIOC and/or ELC and will ensure the Executive Sponsor has sufficient time to complete all required budget documentation. For funded investments that are<$100K, portfolio information will be entered into the PfM tool and then queued for review by the CIO.

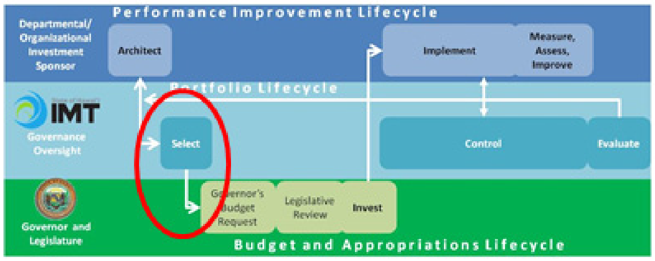
5.11 SELECT PHASE

In the Select phase, all investments within the portfolio are reviewed, ranked, and then pending/approved/recommended/denied/delayed. The process steps for this phase are as follows:

1. The Executive Sponsor and/or PM update all existing (previously submitted) investments information within the portfolio

2. The PfMgr, OIMT, and CIO screens, analyzes, and assesses the total portfolio including:
   - Portfolio information, business cases, and risk analysis for new investments with regard to the description of need/proposed benefits; LOB/mission needs and service delivery requirements. (Note: As part of the screening process, alternative recommendations relative to the investments proposed solution may be offered to the Executive Sponsor.)
   - Existing investments, specifically those identified as SS, relative to end-of-life status, retirement and replacement strategy, termination, modernization and/or enhancement needs, and transition[6] requirements to align with the Strategic Plan and EA (Note: Screening of existing investments and any forthcoming recommendations should occur early enough in the select process to allow for the Executive Sponsor to architect and create a new investment request, especially for the SS projects.)

3. The PfMgr coordinates the OIMT's and CIO's comparison and ranking of the new investment proposals against defined criteria[7] and the overall portfolio.



4. The CIO reviews and approves or denies investments <$100K, and the PfMgr notifies the Executive Sponsor regarding all decisions.

5. The PfMgr plans the agenda for the CIOC to review investments:
   - >$100K and <$1M and deny, delay, or select in a ranked order
   - >$1M deny, delay, or recommend selection to ELC

6. The PfMgr plans the agenda for the ELC to review investments:
   - >$1M deny, delay, or select in a ranked order

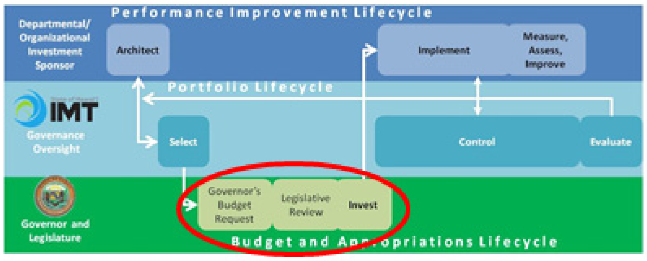
7. The CIO, supported by the PfMgr, coordinates with the Executive Sponsor and B&F regarding the inclusion of selected investments in the Governor's FY budget request based on the ranking and other known constraints (e.g., resource availability, budget guidance/expectations, or other priorities within the State).

[6] The need for transition will carry more weight for the next five to ten years until nonconforming technologies can be retired and/or replaced or modernized.

[7] Criteria for ranking new investments as part of the entire portfolio are available on the OIMT intranet site.

8. The PfMgr, regardless of the selection, denial, delay, or recommendation decision for the investment, communicates with the Executive Sponsor or PM regarding the CIO, CIOC and/or ELC comments relative to the investment proposal. For investments that are delayed or denied, as part of selection Select Phase, the rationale for the denial or delay are communicated immediately to allow the Executive Sponsor or PM to assess the impact, adjust investment proposal documentation, and/or prepare an appeal. Investment selections are also communicated expeditiously so that budget documentation can be prepared.

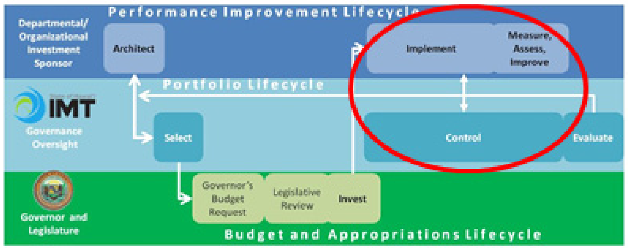
5.12 INVEST PHASE



It should be noted that even though the CIOC and/or ELC have selected or recommended an investment, there are three additional decision points where an investment request may be approved or denied. The first point is with the Governor where investments are included or not included in his/her budget submittal to the Legislature. The second point is with the Legislature's Ways and Means or Finance Committees where an investment can be recommended or not recommended for legislative consideration and funding/investment. Finally, the third decision point is with the Legislature where the investment is approved for funding or denied. Once an investment is funded by the Legislature, the investment is moved into the Implement through Control phases.

5.13 IMPLEMENT, MEASURE, ASSESS, IMPROVE, AND CONTROL PHASES

During these phases, funded investments in the portfolio are reviewed and monitored on a regular basis by the PfMgr, CIO, and CIOC and/or ELC, as appropriate, while the implementation of the investment (following a defined PM Methodology and SDLC Methodology) is performed by the Executive Sponsor and PM. The following are the process steps for these parallel phases:



1. The Executive Sponsor and the assigned PM complete all implementation plans and begin all implementation activities for the investment and its subsequent DME projects.

2. The Executive Sponsor and PM manages the project by continually measuring results, assessing progress against planned schedules, and improving/adjusting the implementation of the investment activity and associated projects as required to ensure the achievement of the desired results.

3. The PfMgr establishes a schedule for the investment's progress or project reviews that follow the guidance provided in the OIMT Project Management Methodology or other recognized PMM. (Note: The type and frequency of the progress reviews are usually determined based on the analysis of risk, complexity, and cost that were identified when the project was selected (and subsequently funded through the budget approval process). These reviews may coincide with investment events such as achievement of key deliverables.

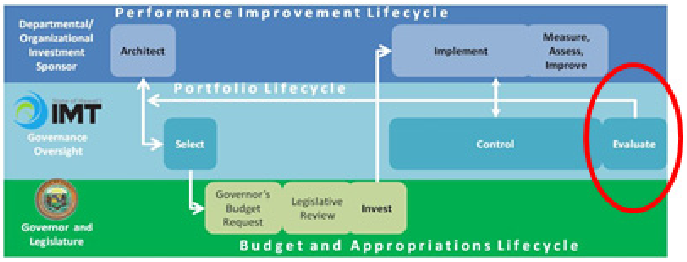
4. The CIO, and as appropriate, the CIOC and/or ELC, monitor the progress of each investment activity against planned schedules and spend plans on a regular basis in conjunction with the Executive Sponsor and/or PM as the implementation occurs through periodic reviews. The CIO, CIOC, and/or ELC recommended course corrections or corrective actions if progress is not on track (e.g., stated milestones are not being met, expenditure of funding is significantly over or under planning estimates, risk mitigation plans are not effective, additional risks have been identified).

5. If an implementation project is late, over cost, significantly under cost, or not meeting performance expectations, the CIO, CIOC and/or ELC will schedule a progress review and will make the decision whether the investment should be continued, modified, or canceled. Any CIOC and/or ELC recommendations and subsequent actions are immediately conveyed to the Executive Sponsor or PM to mitigate the effects of changes in risks and costs.

6. The PfMgr will ensure all actions and recommendations are updated within the portfolio.

Once an investment or project within an investment is fully implemented, it becomes a SS O&M Activity and is moved to the Evaluate Phase.

5.14 EVALUATE PHASE



In the Evaluate phase, the entire portfolio of investments and specifically the fully implemented or SS activities and any canceled investments undergo additional review in terms of actual or expected results. The following are the process steps for this phase:

1. The PfMgr and CIO continually evaluate the portfolio on mission performance, spending perspectives, and other defined objectives and measures and subsequently identify and recommend to the Executive Sponsor, CIOC, and/or ELC any changes or modifications to the portfolio and any specific SS activity that may be needed (e.g., activities nearing end-or-life and/or might require modernization or enhancement or retirement).

2. The PfMgr and CIO review any cancelled investments in detail for lessons learned and share this analysis with the CIOC and/or ELC, as appropriate.

3. The PfMgr and CIO implement revisions in the State's PfM processes based on lessons learned and provide input into the following year's investment identification and selection activities.

5.15 PFM AND OTHER IT GOVERNANCE AND MANAGEMENT ACTIVITIES

As noted above, PfM is tightly integrated with the State's defined IT/IRM governance processes and with project or program management in general. Within the State of Hawai'i, each of these activities has defined roles and responsibilities with specific goals and objectives, but they share an overarching focus on effectively:

- Identifying and securing funding for needed IT investments and their projects or programs
- Ensuring alignment with the Strategic Plan and EA and other processes (e.g., procurement, budget guidance)
- Monitoring and managing all investment activities based on estimated versus actual spend plans, risk identification and mitigation, delivery against milestones and deliverable schedules, and achievement of defined benefits
- Taking corrective actions, as appropriate
- Managing each IT investment and any subsequent projects or programs throughout their life cycle
- Documenting the processes required for effective process maintenance
- Continually improving processes associated with IT investments planning, tracking, and management
- Identifying opportunities for continuous improvement and applying lessons learned judiciously

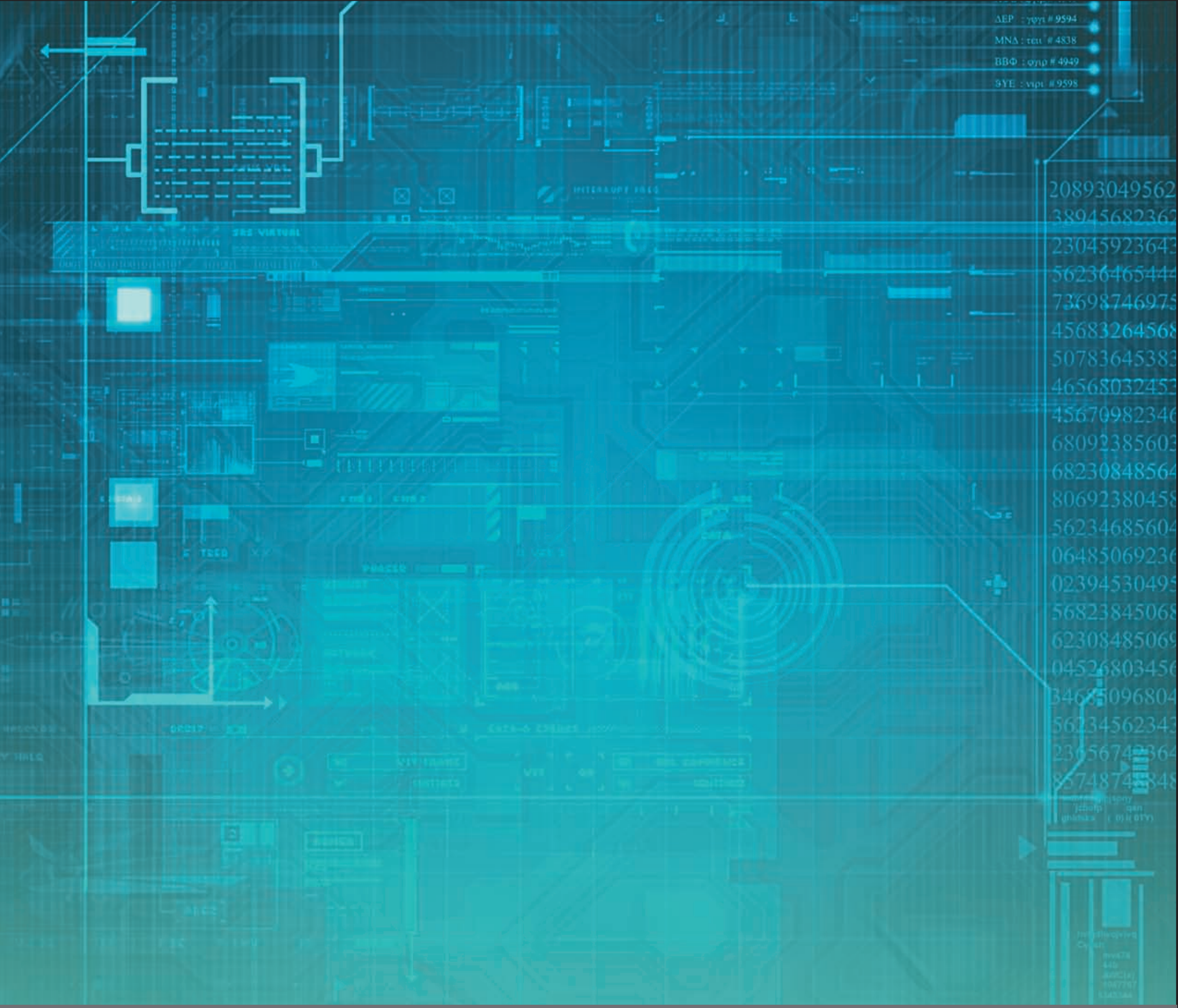
Integration of the IT portfolio and the selection of IT investments are tightly integrated with the State's budget process. The selection of money to invest in IT and the integration of this to either particular programs or to line items in the State's budget are to be synchronized. This will help ensure the money is there to start a new IT investment and that the money is reallocated to other budget needs at the proper time, so as not to leave a service with either two working investments doing duplicate work, or leave the new investment non-operational and the terminated investment shut off with citizens' service in a degraded state.

5.16 INVESTMENT PORTFOLIO MANAGEMENT TOOL SUITE

The information gathered as part of the PfM provides the opportunity for the CIO,CIOC, ELC, Departments, B&F, Executive Sponsors, PMs, legislative units, and other stakeholders to view the portfolio from many perspectives to make informed decisions about the State's existing and proposed IT investments. The information will be maintained in an automated tool[8] to facilitate tracking, analysis, and reporting against the numerous views including:

- Total portfolio view
- Departmental/organizational view
- SS view
- DME view
- Planned and actual start/completion data view
- Investment life cycle (Select, Control, Evaluate) view
- Progress review, status view

[8] While an integrated tool is being selected and acquired, the OIMT and the PfMgr will utilize the Enterprise Assessment Database (EAD) to capture portfolio information.



6.0 PROJECT MANAGEMENT

6.0 PROJECT MANAGEMENT

Management of government projects, programs, and portfolios—and the related expenditures of public funds—are major, visible areas of interest and concern. Emphasis on performance improvement in government continues to increase steadily, supported by mandates imposed by government laws and public pressure. Despite a growing understanding of the determinants of success, increasing maturity, and a stream of successful programs and projects, project failures continue at an alarming rate.

Project Management is a set of processes, tools, and templates used to effectively plan and manage project work. This section outlines the State of Hawai'i OIMT PMM. It is based upon the Project Management Institute's (PMI) *Project Management Body of Knowledge (PMBOK)*, and it has been enhanced to incorporate State of Hawaiʻi specific processes. The goal of the PMM is to institute a scalable framework of industry standard best practices to support and promote the successful delivery of projects. Although identified as distinct processes, in practice, the processes overlap and interrelate. Some processes are iterative, repeated, and revised throughout the life of a project. Seasoned project managers acknowledge there are many ways to manage a project. As organizations evolve in maturity level, PMs will be better equipped to determine which processes to utilize and how rigorously to apply these processes to deliver the project.

PMM is typically used in conjunction with a SDLC. The particular SDLC depends upon the standards and the type of project undertaken. Although terminology can differ, the PMM and SDLC methodologies can be easily integrated.

The advantages of establishing sound project management practices are:

- Improves overall project performance
- Increases projects delivered on-time and within budget
- Reduces project risk
- Enhances quality
- Improves inter- and intra-project communication
- Establishes a consistent standard that everyone can follow
- Complements standard System Development Life-Cycle Methodologies (SDLC)
- Promotes common project management terminology

This PMM document will share knowledge and support implementation of the methodology across the State of Hawaiʻi.

6.1 PURPOSE

The purpose of the PMM is to describe the approach that will be used by the State of Hawaiʻi to initiate, plan, execute, monitor/control, and close IT projects in alignment with the Program Management Methodology (PgM) and PfM Methodology established by the State of Hawaiʻi.

The PPM in this document is not intended to replace existing project management programs or processes within departments that have established processes designed for specific project types (e.g., construction). However, PMI's framework, concepts, tools, and techniques can be applied to virtually any project.

6.2 SCOPE

The scope of PMM is to establish a consolidated, consistent, and efficient project management processes that the State of Hawaiʻi will use to manage IT projects to ensure that projects are well planned and successfully deliver expected outcomes that are within funding, on time, and known risks; demonstrate effective communications, and are aligned with program and portfolio goals and objectives. The PMM defines the processes, tools, and techniques that support the efficient execution of projects from beginning to end and defines the roles and responsibilities of project participants and stakeholders.

The scope of the PPM initiative is to establish a project management process within OIMT that can adapt to non-technology projects and business process improvement initiatives. The project management process is a subordinate process to established programs and portfolios and should ensure alignment.

6.3 PROJECT MANAGEMENT GOALS AND OBJECTIVES

The goal of the PMM is to successfully deliver IT investments, products, services, or results according to a plan developed and executed through effective team planning and leadership.

Objectives for PMM include:

1. Establish a consolidated, consistent, and efficient project management processes to manage projects.

2. Define clear business objectives, understanding options via identifying their benefits, costs, and risks.

3. Increase process transparency and flexibility.

4. Effectively manage government funding.

5. Increase the probability that project outcomes meet user needs and expectations, resolve business problems, and reduce risk/variability.

6. Facilitate better decision making before project start and during project execution.

7. Reduce project risks of delays, cost overruns and failure.

8. Properly identify a project's expected outcomes.

9. Organize and develop a team capable of planning the work to achieve the expected outcomes.

10. Identify and manage risks to project success.

11. Identify expected key performance measures to ensure,

through planning, that the project outcomes will meet quality expectations.

12. Ensure timely and accurate communications to stakeholders and committees.

13. Ensure proper hand-off to operations or SS personnel.

14. Deliver project results to the established expectations.

15. Develop skilled project teams and encourage Project Management competencies.

6.4 PROJECT PERFORMANCE MEASURES

Every project will have performance measures related to the specific product, service, or result of the project and key performance indicators identified by the project sponsor and team. Performance measures may also apply from programs and portfolios. These measures will be planned, monitored, and controlled by the PM and team.

Standard performance measures for all projects shall be the following:

- Planned according to methodology
- Meet planned/re-baselined project end dates
- Meet planned/re-baselined project budget
- Meet strategic goals and performance measures established in the PgM and PfM

6.5 PMM PROCESS

The PMM provides project-planning information in a variety of ways and levels of detail to address the needs, knowledge, and work styles of the many interested parties across the State of Hawai'i. The PMM also sets forth a defined process, outlines required deliverables, and, in conjunction with the Enterprise Architecture and IT Investment Portfolio, provides a rigorous, detailed, and thorough process that should be adopted by the State of Hawai'i. By following the process outlined in the methodology, the departments should be able to take an initial concept to resolve a problem or gap and shepherd it successfully through the planning process. The roadmap that has been laid out should give the departments the confidence that IT projects should meet all of the regulatory requirements because the guide establishes a comprehensive, consistent, measurable, and repeatable process for IT project planning and management. In other words, this process should improve the success of IT projects in terms of budget, schedule, and outcome.

The PPM establishes clear lines of responsibility, organization, authority, and approval. At each stage of the PPM, the business representatives and the OIMT counterparts complete certain tasks in concert. The partnership must pass through control gates that are established to ensure compliance with the process before proceeding to the next phase. The project team can only move on to the next phase in the process when the control gate has been met successfully and approvals have been received.

The PMM incorporates best practices from the international project management organization, Project Management Institute (PMI), which is recognized globally. The methodology is based on the Project Management Body of Knowledge (PMBOK) and framework. The implementation of the methodology will account for various needs and levels of rigor needed to successfully complete different types of projects in differing environments. The implementation plan will include key performance indicators, alignment with program and project portfolios, and enterprise architecture. One of the primary goals of this effort is to ensure that everyone responsible for project development and solution implementation is aligned, supported, and communicating throughout the process.

The PMI project management framework applies globally and across industry groups. This does not mean that the knowledge, skills, and processes described should always be applied uniformly on all projects. For any given project, the PM, in collaboration with the project team, is always responsible for determining which processes are appropriate and the appropriate degree of rigor for each process.[9]

The proposed PPM consists of five fundamental processes that are used to guide the overall project and individual phases. Applying the processes during the phases of a project life cycle is expected. For the purposes of this document, processes are discussed from the perspective of how they apply to an overall project. The five processes are: Initiation, Planning, Executing, Monitoring and Controlling, and Closing (Figure 17).

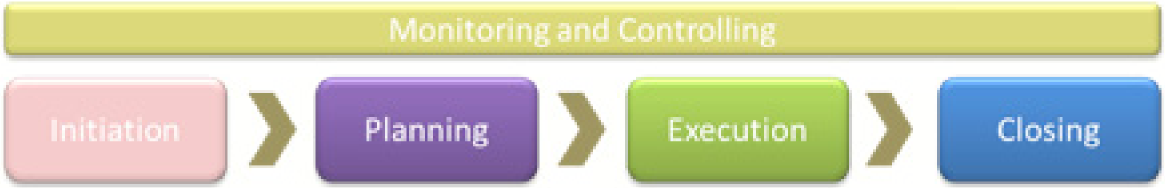


Figure 17: The Project Management Processes

[9] A Guide to the Project Management Body of Knowledge, Fourth Edition

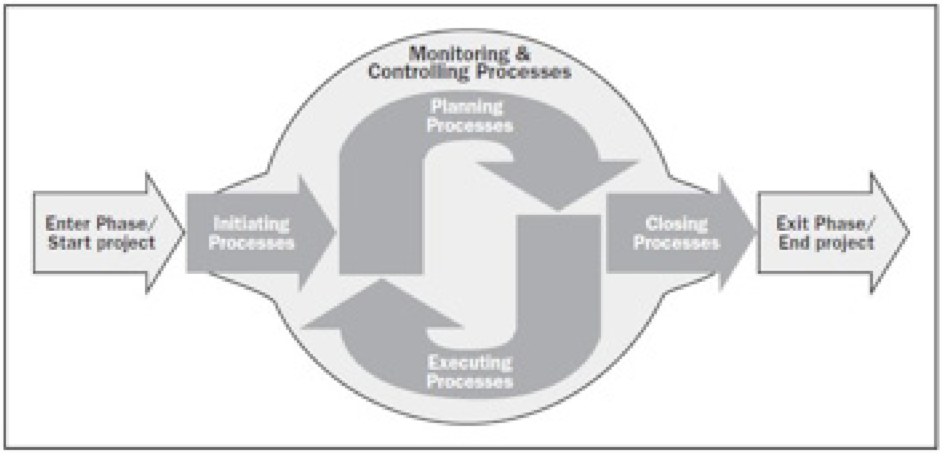


Figure 18: PMBOK Processes Iterative Diagram

The PM processes may be iterative (Figure 18) and apply to various phases of a project's life cycle (e.g., SDLC, ITIL) or may be applied as an overall life cycle as appropriate. Figure 19 illustrates the applicable project processes associated with IT Investment projects as well as the performance monitoring and development functions.

IT Investment Life Cycle[1]	OMB Performance Improvement Cycle[2]	Project Management/ Methodology	System Development Life Cycle (SCLC)
(Pre-Select or Analyze)	Architect	Initiation	
		Planning & Design	
		Executing Monitoring & Controlling	
		Closing	
Select	Invest		
Control	Implement	Initiation	Initiation
		Planning & Design	Concept
			Planning
			Requirements Analysis
			Design
		Executing Monitoring & Controlling	Development
			Test
		Closing	Implementation
			Operations & Management
Evaluate	Measure, Assess and Improve		Disposition

Figure 19: Project Processes

6.6 OTHER PROJECT MANAGEMENT METHODOLOGIES

The State of Hawaiʻi will incorporate other project management methodologies, tools, or techniques as appropriate to specific projects, but the primary PMI processes of Initiating, Planning, Executing, Monitoring and Controlling, and Closing shall apply as an overarching Project Management Framework for the State of Hawaiʻi.

6.7 AGILE DEVELOPMENT

Agile development involves breaking a project into user-identifiable pieces of functionality that can be deployed and actually used, and then producing these pieces approximately every 30 days. Agile development requires that the project team, management, oversight, and governance approve the concept that the project will plan, design, build, test and deploy as it produces the 30-day deliverables. All of these functions need to be embedded with the project team–in real time.

It should also be made clear that Agile development is not ad-hoc, chaotic programming. Instead, it follows a rigorous process for refining and periodically reprioritizing requirements, and for developing and deploying user functionality at regular intervals.

6.8 PMM CHECKPOINTS/APPROVAL GATES

All IT Investment projects are part of the portfolio and subject to review and approval through the OIMT, CIOC, and ELC.

This PMM is designed to address the Information Technology Management Reform Act of 1996 (Clinger-Cohen). From the perspective of the PM, the Act means PMs must be able to manage and report project status in terms of mission, business, and enterprise, as well as the more traditional performance terms.

The three functions of the IT Investment Life Cycle process are to: Select, Control, and Evaluate projects. The initial Select function occurs at the beginning of the life cycle; the Control function is conducted through the project's development phases, and the Evaluate function is performed after the project transitions to O&M.

- Projects with estimated budgets of less than $100,000 dollars may be submitted using the T205 process.
- Projects with estimated budget within $100,000 - $1,000,000 shall be reviewed by the CIOC.
- Projects with estimated budgets above $1,000,000 shall be reviewed by the CIOC and then the ELC.

Table 3: ITIL Reviews

		Select	Control	Evaluate
Project Budget	Documentation	Reviewed by	Status Updates	Performance Review
< $100,000	T205	CIO	As needed	TBD
$100,000 - $1,000,000	Project Charter and/or Business Case	CIOC	Quarterly	TBD
>$1,000,000	Project Charter and/or Business Case Project Plan	CIOC/ELC	Monthly	TBD

6.9 PROJECT STATUS REVIEWS

Once a project has been approved by the CIOC and/or ELC, regular interval updates to the councils shall be provided. These updates will include at minimum, a description of the project, list of top risks and issues, and an overall project status identifier as identified in Table 4.

Table 4: Project Status

Red	x>=10% behind in Scope, Cost, Schedule and Risk
Yellow	5>x>10% behind in Scope, Cost, Schedule and Risk
Green	0>x>5% behind in Scope, Cost, Schedule and Risk
Blue	Ahead of Scope, Cost, Schedule and Risk

Status updates will also include a Risk Register of the highest risks to the project.

Table 5 - Qualitative Risk Analysis

		Probability of Occurrence		
		Low	Medium	High
Severity	High	Yellow	Red	Red
	Med	Green	Yellow	Red
	Low	Green	Green	Yellow

6.10 PROPOSAL

Business case:

- Concept to address business problem
- Stakeholder analysis
- Research and Business Plan
- Alignment to objectives
- Rough Order of Magnitude (ROM) budget
- High-level timeline of project life cycle

6.11 APPROVED PROJECTS

Projects will be approved based on the following criteria:

- Alignment with EA
- Economies of scale
- Value of expected outcomes
- ROI or Service Value
- Risks
- Budget

6.12 COMPLETED PLANNING REVIEW

Projects will be approved based on the following criteria:

- Credibility of project plan
- Portfolio and program resource integration
- Available resources
- Identified risks and contingency plans
- Leadership support

6.13 PMM KNOWLEDGE AREAS

PMI outlines nine specific knowledge areas which are detailed below.

6.13.1 INTEGRATION MANAGEMENT

Project Integration Management includes the processes and activities needed to identify, define, combine, unify, and coordinate the various processes and project management activities within the Project Management Process Groups. In the project management context, integration includes characteristics of unification, consolidation, articulation, and integrative actions that are crucial to project completion, successfully managing stakeholder expectations, and meeting requirements. Project Integration Management entails making choices about resource allocation, making trade-offs among competing objectives and alternatives, and managing the interdependencies among the project management Knowledge Areas.[10]

Table 6: Integration Management Processes

Project Management Integration	Develop project charter	Develop Project Management Plan	Direct and manage project execution	Monitor and control project work Perform integrated change control	Close project or phase

6.13.2 SCOPE MANAGEMENT

Project Scope Management includes the processes required to ensure that the project includes all the work required, and only the work required, to complete the project successfully. Managing the project scope is primarily concerned with defining and controlling what is and is not included in the project.

Table 7: Scope Management Processes

Project Time Management	Collect requirements Define Scope Develop WBS	Verify scope Control scope

[10] *A Guide to the Project Management Body of Knowledge,* Fourth Edition

6.13.3 TIME MANAGEMENT

Project Time Management includes the processes required to manage timely completion of the project.

Table 8: Time Management Processes

Project Time Management	Define activities Sequence activities Estimate activity resources Develop schedule	Control schedule

6.13.4 COST MANAGEMENT

Project Cost Management includes the processes involved in estimating, budgeting, and controlling costs so that the project can be completed within the approved budget.

Table 9: Cost Management Processes

Project Cost Management	Estimate costs Determine budget	Control cost

6.13.5 QUALITY MANAGEMENT

Project Quality Management includes the processes and activities of the performing organization that determines quality policies, objectives, and responsibilities which enable the project to satisfy the needs for which it was undertaken. It implements the quality management system through policy and procedures with continuous process improvement activities conducted throughout as appropriate.

Table 10: Quality Management Processes

Project Quality Management	Plan Quality	Perform quality assurance	Perform quality control

6.13.6 HUMAN RESOURCES MANAGEMENT

Project Human Resource Management includes the processes that organize, manage, and lead the project team. The project team is comprised of the people with assigned roles and responsibilities for completing the project. The type and number of project team members can change frequently as the project progresses. Project team members may also be referred to as the project's staff. While the specific roles and responsibilities for the project team members are assigned, the involvement of all team members in project planning and decision making can be beneficial. Early involvement and participation of team members adds their expertise during the planning process.

Table 11: Human Resources Management Processes

Project Human Resources Management	Develop HR plan	Acquire project team Develop project team Manage project team	Manage project team

6.13.7 COMMUNICATIONS MANAGEMENT

Project Communications Management includes the processes required to ensure timely and appropriate generation, collection, distribution, storage, retrieval, and ultimate disposition of project information. Project managers spend the majority of their time communication with team members and other project stakeholders, whether they are internal (at all organizational levels) or external to the organization. Effective communication creates a bridge between diverse stakeholders involved in a project, connecting various cultural and organizational backgrounds, different levels of expertise, and various perspectives and interests in the project execution outcome.

Table 12: Communications Management Processes

Project Communications Management	Identify stakeholders	Plan Communications	Distribute information Manage stakeholder expectations	Report performance

6.13.9 RISK MANAGEMENT

Project Risk Management includes the processes of conducting risk management planning, identification, analysis, response planning, and monitoring and control on a project. The objectives of Project Risk Management are to increase the probability and impact of positive events, and decrease the probability and impact of negative events in the project.

Table 13: Risk Management Processes

Project Risk Management	Plan risk management Identify risks Perform qualitative risk analysis Perform quantitative risk analysis Plan risk responses	Monitor and control risks

6.13.10 PROCUREMENT MANAGEMENT

Project Procurement Management includes the processes necessary to purchase or acquire products, services, or results needed from outside the project team. The organization can be either the buyer or the seller of the products, services, or results of a project.

Project Procurement Management includes the contract management and the change control processes required to develop and administer contracts or purchase orders issued by authorized project team members.

Project Procurement Management also includes administering any contract issued by an outside organization (the buyer) that is acquiring the project from the performing organization (the seller), and administering contractual obligations placed on the project team by the contract.

Table 14: Procurement Management Processes

Project Procurement Management	Plan procurements	Conduct procurements	Administer procurements	Close procurements

6.13.12 PROGRAM AND PROJECT ORGANIZATION CHARTS

Programs consist of a group of related projects, subprograms, and program activities that are managed in a coordinated way to obtain benefits not available from managing them individually. The basic organizational structure for OIMT programs is depicted in Figure 20.

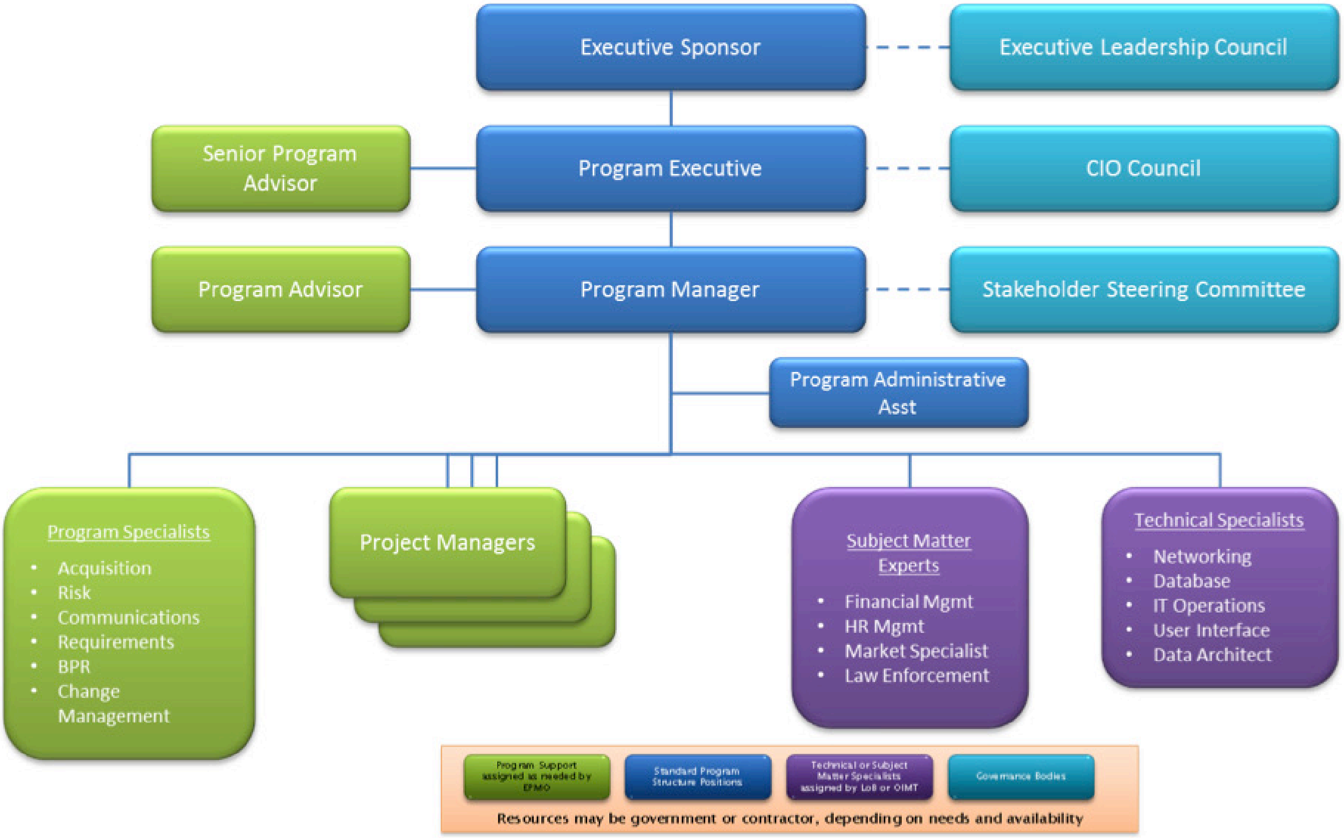
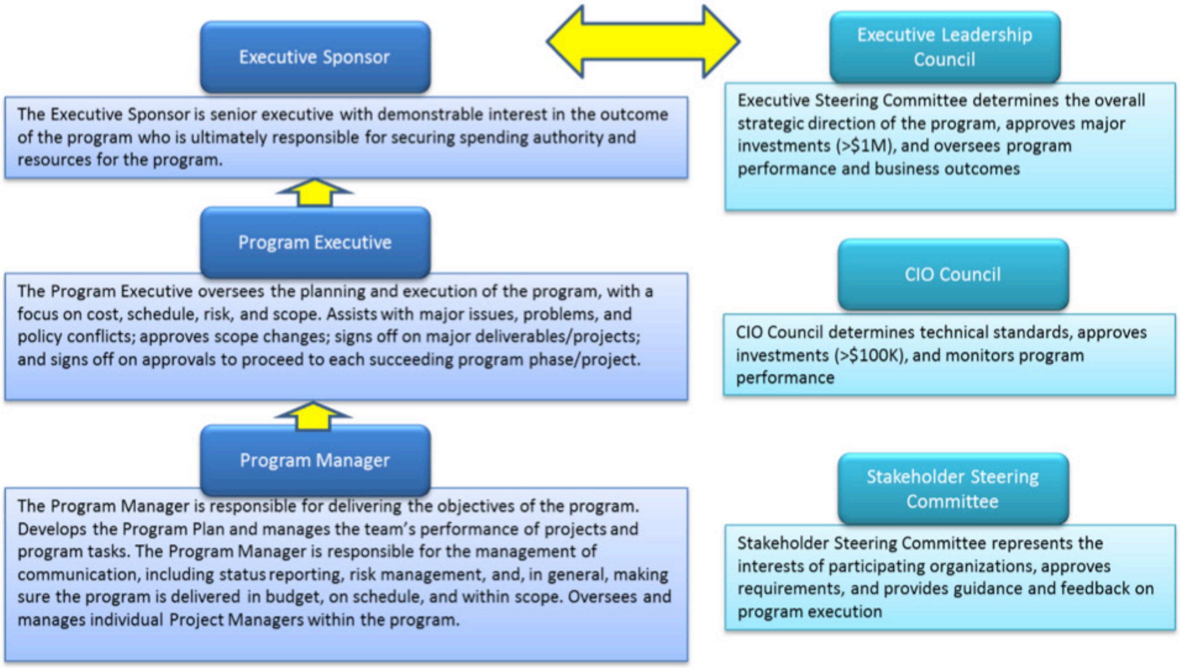


Figure 20: Basic OIMT Program Structure

The governance of a typical program is depicted in Figure 21.



Executive Sponsor

The Executive Sponsor is senior executive with demonstrable interest in the outcome of the program who is ultimately responsible for securing spending authority and resources for the program.

Program Executive

The Program Executive oversees the planning and execution of the program, with a focus on cost, schedule, risk, and scope. Assists with major issues, problems, and policy conflicts; approves scope changes; signs off on major deliverables/projects; and signs off on approvals to proceed to each succeeding program phase/project.

Program Manager

The Program Manager is responsible for delivering the objectives of the program. Develops the Program Plan and manages the team's performance of projects and program tasks. The Program Manager is responsible for the management of communication, including status reporting, risk management, and, in general, making sure the program is delivered in budget, on schedule, and within scope. Oversees and manages individual Project Managers within the program.

Executive Leadership Council

Executive Steering Committee determines the overall strategic direction of the program, approves major investments (>$1M), and oversees program performance and business outcomes

CIO Council

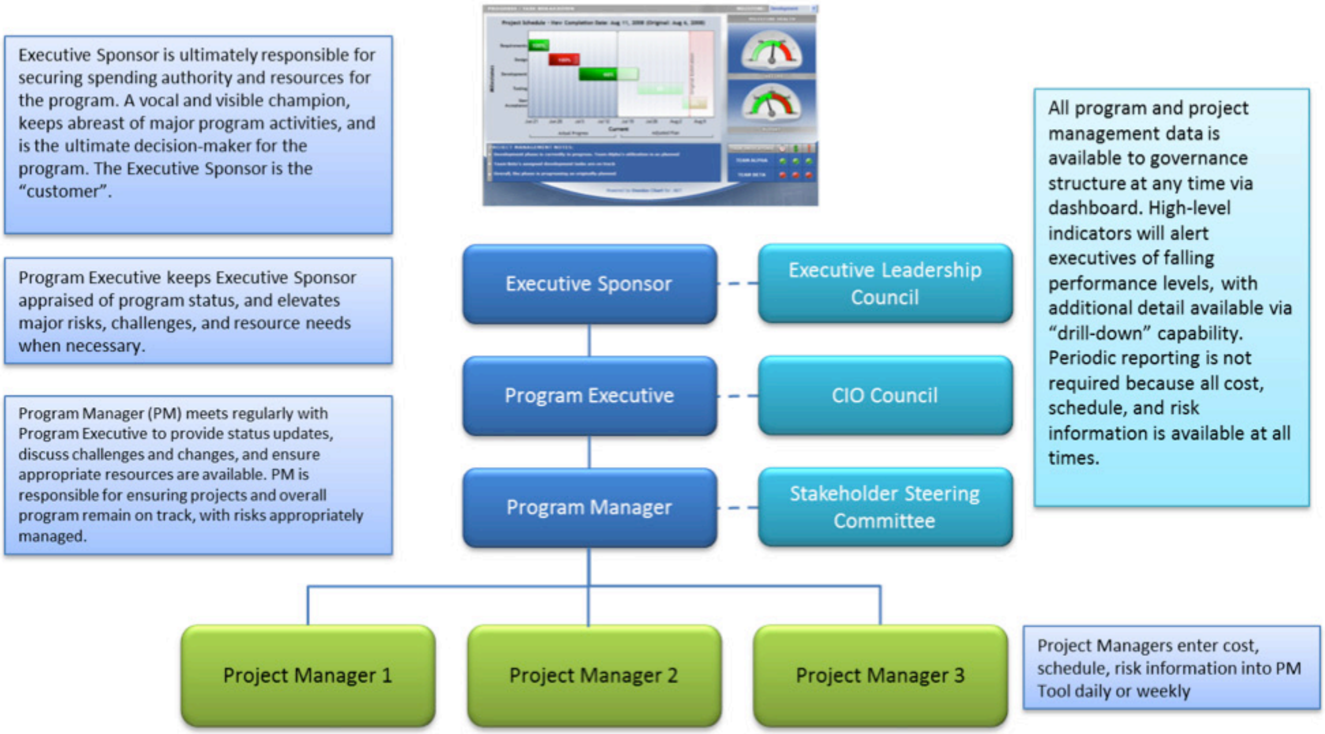
CIO Council determines technical standards, approves investments (>$100K), and monitors program performance

Stakeholder Steering Committee

Stakeholder Steering Committee represents the interests of participating organizations, approves requirements, and provides guidance and feedback on program execution

Figure 21: Program Governance

Programs are managed by the PgM, reporting to the Program Executive. Program performance information is captured in the Management Tool and reported via a dashboard. Meetings and presentations between the PgM and the governance structure are conducted on a by-exception basis to address specific shortcomings or risks (Figure 22).



Executive Sponsor is ultimately responsible for securing spending authority and resources for the program. A vocal and visible champion, keeps abreast of major program activities, and is the ultimate decision-maker for the program. The Executive Sponsor is the "customer".

Program Executive keeps Executive Sponsor appraised of program status, and elevates major risks, challenges, and resource needs when necessary.

Program Manager (PM) meets regularly with Program Executive to provide status updates, discuss challenges and changes, and ensure appropriate resources are available. PM is responsible for ensuring projects and overall program remain on track, with risks appropriately managed.

All program and project management data is available to governance structure at any time via dashboard. High-level indicators will alert executives of falling performance levels, with additional detail available via "drill-down" capability. Periodic reporting is not required because all cost, schedule, and risk information is available at all times.

Project Managers enter cost, schedule, risk information into PM Tool daily or weekly

Figure 22: Program Management

As illustrated in Figure 23, project teams are hierarchical in authority and reporting.

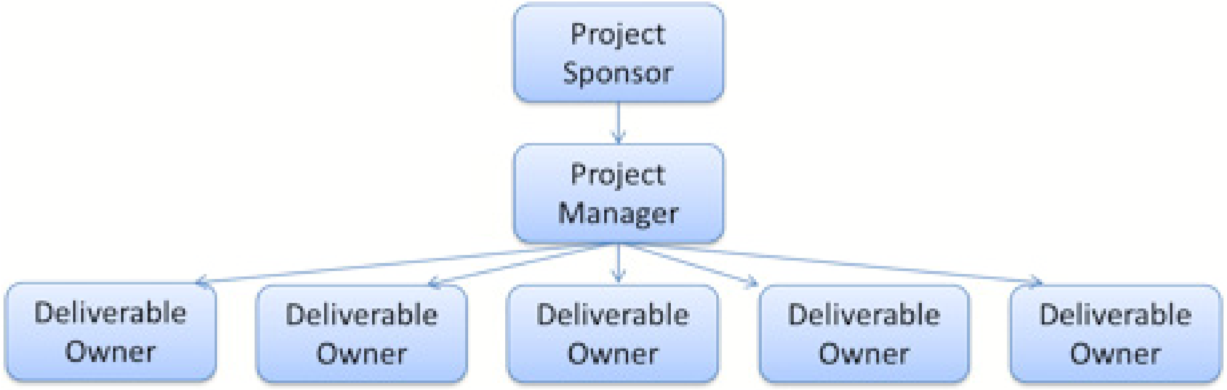


Figure 23: Project Team Organization Chart

Table 6: Integration Management Processes

Processes/ Knowledge Areas	Initiating Process	Planning Process	Executing Process	Monitoring and Controlling Process	Closing Process
Project Management Integration	Develop project charter	Develop Project Management Plan	Direct and manage project execution	Monitor and control project work Perform integrated change control.	Close project or phase
Project Scope Management		Collect requirements Define Scope Develop WBS		Verify scope Control scope	
Project Time Management		Define activities Sequence activities Estimate activity resources Develop schedule		Control schedule	
Project Cost Management		Estimate costs Determine budget		Control cost	
Project Quality Management		Plan Quality	Perform quality assurance	Perform quality control	
Project Human Resources Management		Develop HR plan	Acquire project team Develop project team Manage project team	Manage project team	
Project Communications Management	Identify stakeholders	Plan Communications	Distribute information Manage stakeholder expectations	Report performance	
Project Risk Management		Plan risk management Identify risks Perform qualitative risk analysis Perform quantitative risk analysis Plan risk responses		Monitor and control risks	
Project Procurement Management		Plan procurements	Conduct procurements	Administer procurements	Close procurements

6.14 PROJECT ROLES AND RESPONSIBILITIES

6.14.1 EXECUTIVE SPONSOR

The Executive Sponsor is typically a member of the Department's or organization's leadership and is responsible for:

- Ensuring the organization follows the dollar boundaries (<$100K; $100K-$1M; >$1M) for investment actions and documentation
- Ensuring new investment proposals are appropriately documented and justified in preparation for the Select phase of the investment management process with:|
  - Accurate and current portfolio information
  - A business case
  - A risk assessment
- Ensuring the organization's existing projects (regardless of life cycle status) are complete within the OIMT investment portfolio
- Ensuring that portfolio components (i.e., projects, programs, applications, or systems) are evaluated on an annual basis and receive an appropriate level of funding to support its project life cycle stage (i.e., support SS or DME, or retirement)
- Addressing all recommendations issued by the CIOC and/or ELC relative to alternate approaches, denials, or delays and follow defined processes for the appeal/re-submission of any investment proposals, as appropriate
- Working collaboratively with the OIMT PfMgr
- Participating in progress reviews as part of the Control phase and address any CIOC or ELC recommended corrective actions
- Participating in reviews associated with the Evaluate phase and address any COIC or ELC recommendations and apply lessons learned, as appropriate
- Ensuring procurement requests contain CIOC or ELC approval documentation

6.14.2 PROJECT MANAGER (PM)

The PM is responsible for:

- Coordinating with the OIS and PfMgr on project information
- Supporting business case development or update for new investment proposals, as appropriate
- Updating newly approved investment information within the investment portfolio as it becomes available relative to subsequent projects
- Supporting evaluation and update of project components (i.e., projects, programs, applications, or systems) on an annual basis and recommending an appropriate level of funding for its life cycle stage (i.e., support SS or DME, or retirement)
- Ensuring project activities remain in alignment with the ELC approved investment
- Submitting CIOC and/or ELC investment approval documentation with any procurement request
- Manages the project integration, scope, time, cost, quality, human resources, communication, risk, and procurement

6.14.3 SUBJECT MATTER EXPERT (SME)

SMEs have the functional or technical expertise in a specific area that can provide guidance to project team members. Responsibilities include:

- Providing technical or functional knowledge to guide project team in achieving project objectives and deliverables

6.14.4 FUNCTIONAL MANAGER

The Functional Manager has management authority over an organizational unit within a functional organization: the manager of any group that actually makes a product or performs a service.

Responsibilities include:

- Providing a project with qualified resources and checking resources work for accuracy, quality, and timely completion throughout project
- Prioritizing functional resource workloads according to Enterprise Portfolio and Group Portfolio priorities

6.14.5 DELIVERABLE OWNER

A Deliverable Owner is responsible for producing any unique and verifiable product, result, or capability to perform a service that must be produced to complete a process, phase, or project.

Responsibilities include:

- Leading the deliverable team to ensure timely creation, management, and completion of project work such as deliverables, sub-deliverables, and work packages

6.14.6 PROJECT RESOURCE

Project resources are skilled human resources (specific disciplines either individually, in crews, or teams), equipment, services, supplies, commodities, material, budgets, or funds.

Responsibilities include:

- Accomplishing deliverables by completing assigned deliverables, sub-deliverables, work packages, activities, and tasks

6.14.7 STAKEHOLDER

Stakeholders are persons or organizations (customer, sponsor, performing organization, the public) that are actively involved in the project, or whose interests may be positively or negatively affected by execution or completion of the project. A stakeholder may also exert influence over the project and its deliverables.

Responsibilities include:

- Ensuring prioritized needs and interests are met by attending selected meetings, staying current with project status reports, and providing feedback to project team throughout project life cycle.

6.14.9 PROJECT RISK MANAGER

In projects with high levels of risk, a team member may serve as a leader responsible to document identified risks, monitor, ensure prioritization, and provide communication. The risk manager keeps the team apprised of triggered risks, executes planned contingencies, or coordinates team contingency planning for unplanned events.

6.14.10 PROJECT COMMUNICATIONS MANAGER

In projects with high levels of risk in the area of communications, a team member may serve as a leader responsible to ensure a communications management plan is developed and executed during the project phases. The project communications manager keeps the team apprised of communications internal/external, inbound and outbound, and executes planned communications or coordinates team appropriately.

6.14.11 PROJECT ISSUE MANAGER

In projects with high levels of risk, a team member may serve as a leader responsible to document identified risks, monitor, ensure prioritization, and communication. The issue manager keeps the team apprised of triggered risks, and executes planned contingencies or coordinates team contingency planning for unplanned events.

6.14.12 PROJECT MANAGEMENT TRAINING

Project Management training sessions will be provided at least once per year.

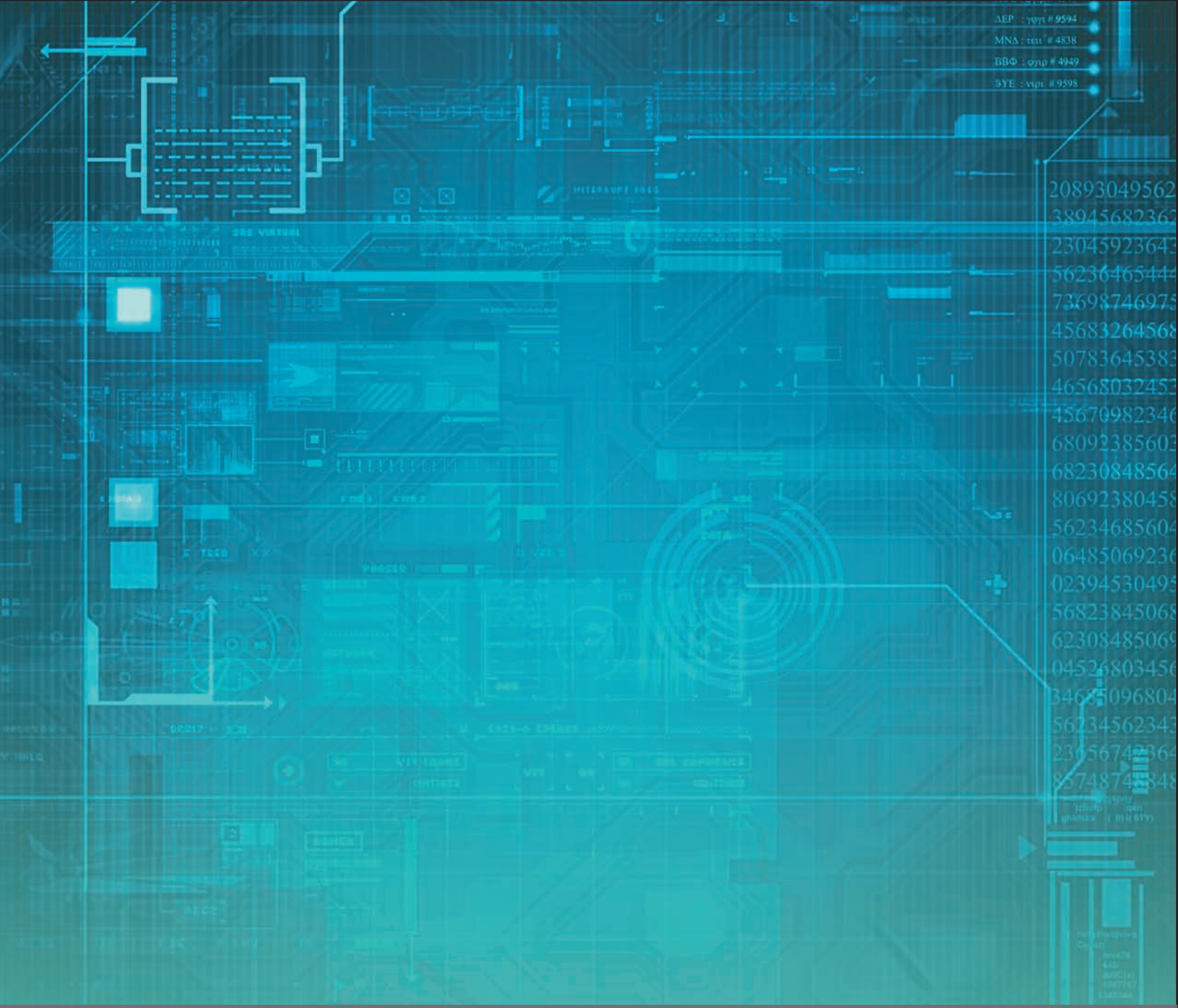
- Team PM Training—a general overview of the project management processes, knowledge areas, and templates. This training will have emphasis on team roles and responsibilities. Overview of the knowledge areas with special attention to Risk Management and Communications Management.

- Introductory PM Training—a more in-depth training for those assigned to projects without formal training.

- Intermediate PM Training—for those who have completed the fundamentals and are assigned to larger projects.

- Advanced PM Training—for those who have completed the fundamentals and intermediate training and are assigned to large state-wide projects.

The Project Management Office will provide ongoing coaching and mentoring, as well as ongoing competency training.



7.0 BUSINESS PROCESS REENGINEERING

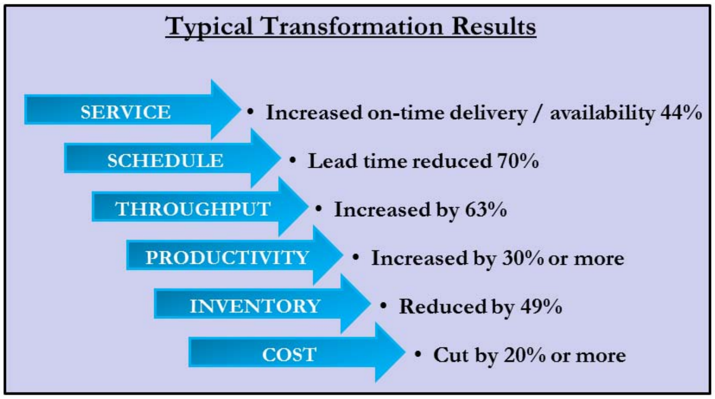
7.0 BUSINESS PROCESS REENGINEERING

This document provides a description of the Business Process Management (BPM) methodology recommended by the OIMT for use within the State of Hawaiʻi as business processes are assessed, addressed, and improved.

7.1 SCOPE

This document outlines the BPM methodology using the Theory of Constraints (TOC), Lean, Six Sigma, and integrated TOC, Lean, Six Sigma (iTLS), which is a combination of the previous three. It provides an overview of the different processes and a framework for the selection of Business Process Projects, the match of project results to the appropriate methodology, and the roles and responsibilities of BPM.

This document introduces the methodology or approaches that have been selected by the CIO for conducting BPR within the State of Hawaiʻi. The selected approaches are known as TOC, Lean, Six Sigma, and iTLS, and have been used effectively to reengineer processes in both the public and private sectors.



Typical Transformation Results

SERVICE • Increased on-time delivery / availability 44%

SCHEDULE • Lead time reduced 70%

THROUGHPUT • Increased by 63%

PRODUCTIVITY • Increased by 30% or more

INVENTORY • Reduced by 49%

COST • Cut by 20% or more

Transformation must begin with re-evaluating the processes that deliver services to internal and external customers. Only through investigating the purpose, outputs, assumptions, and constraints along with the business rules that are associated with a process can transformation begin. Transformation is to change what is now into something different. If we expect different results from the State of Hawaiʻi in the quality, timeliness, cost, and productivity of our services, and then evaluating, reengineering, and managing the business processes is an integral step in the development of a government aligned to service the people of Hawaiʻi.

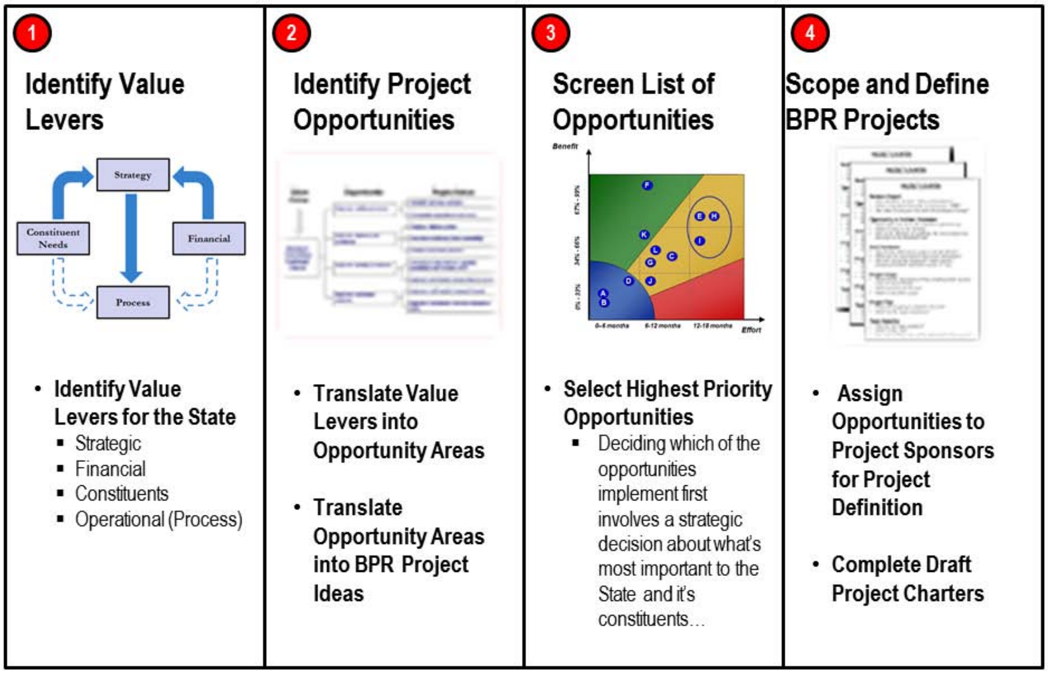
Note: This document is a living document that will be maintained by OIMT and the Business Transformation Executive (BTE). The intended audience for this document is anyone within the State who is interested in learning about TOC and how it is used to reengineer a process. This document outlines major methodologies which may be used in future business process initiatives.

7.2 ASSOCIATED DOCUMENTS

- *The Goal,* by Dr. Eli Goldratt
- *State of Hawaiʻi Business Transformation Strategy and IT/IRM Strategic Plan,* 2012
- *OIMT Project Management Methodology (PPM)*, 2012
- *Overview of the Theory of Constraints,* Viable Vision, 2012
- *Training Presentation,* Viable Vision, 2012
- *Profitability with No Boundaries,* by Reza (Russ) M. Pirasteh and Robert E. Fox, 2012

7.3 SELECTING AND MANAGING A BUSINESS PROCESS REENGINEERING (BPR) PROJECT

The Executive Leadership Steering Group will be engaged in making final decisions relative to BPM activities that have an enterprise or state-wide impact. Department leadership is encouraged to identify and select BPR activities that will improve mission performance and service delivery to constituents. Figure 24 provides examples of considerations for screening BRP activities.



1 Identify Value Levers

- Identify Value Levers for the State
  - Strategic
  - Financial
  - Constituents
  - Operational (Process)

2 Identify Project Opportunities

- Translate Value Levers into Opportunity Areas
- Translate Opportunity Areas into BPR Project Ideas

3 Screen List of Opportunities

- Select Highest Priority Opportunities
  - Deciding which of the opportunities implement first involves a strategic decision about what's most important to the State and it's constituents…

4 Scope and Define BPR Projects

- Assign Opportunities to Project Sponsors for Project Definition
- Complete Draft Project Charters

Figure 24: BPR Project Screening Considerations

When undertaking a BPR activity, it is the responsibility of the project sponsor (Department management or BTE) to ensure that a project schedule is created and that the activities, milestones, and deliverables are achieved. The OIMT Office will provide program and project management oversight to any statewide BPR activity or as requested to the extent resources are available. At a minimum, the basic elements of the OIMT recommended PMM should be followed when managing a BPR activity (illustrated in Figure 25).

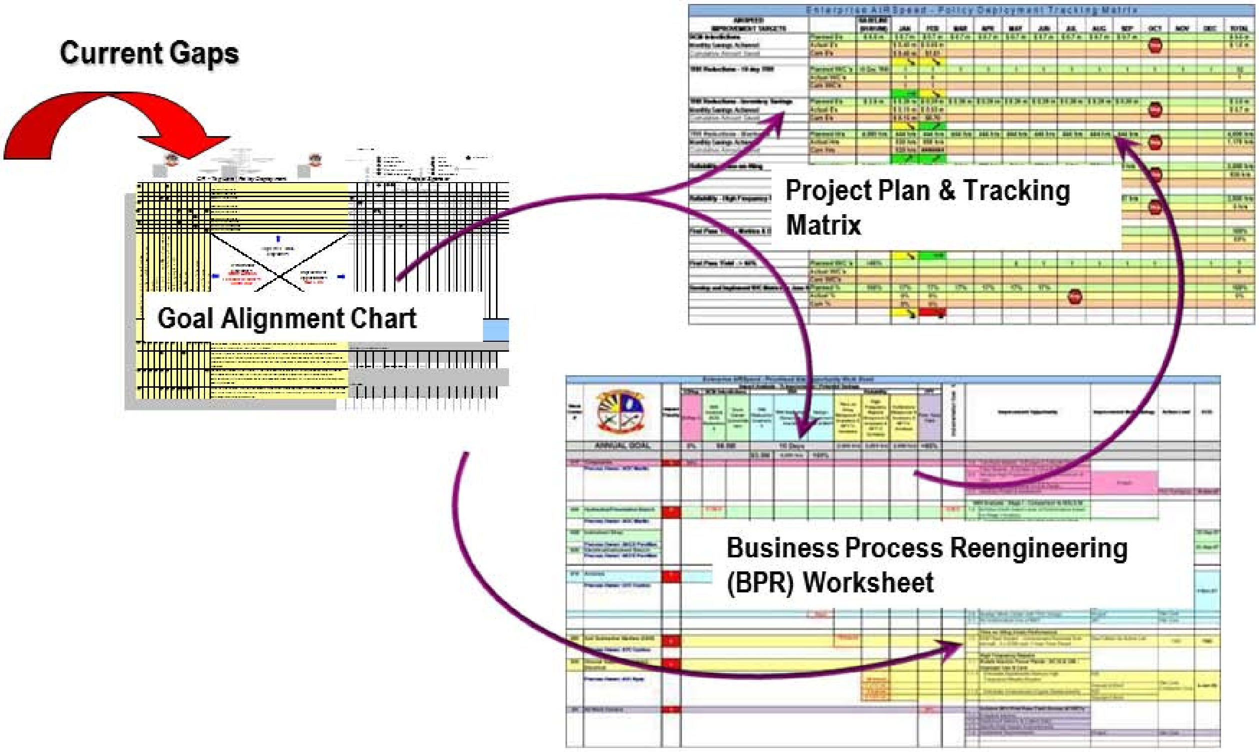
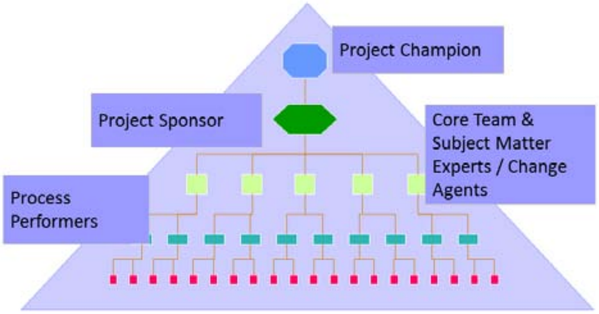

Current Gaps
Goal Alignment Chart
Project Plan & Tracking Matrix
Business Process Reengineering (BPR) Worksheet

Figure 25: Managing BPR Projects

7.4 BPR ROLES AND RESPONSIBILITIES

This section describes BPR roles and responsibilities.

7.4.1 BPR PROJECT CHAMPIONS FOR THE STATE



The Executive Leadership Steering Group provides guidance; oversees policy, validates resource requirements, and serves as the point of contact and BPR Project Champion. The Project Champion monitors all BPR Projects. It is imperative that Champions promote BPR within the State through consistent words and actions. They ensure that the necessary resources are available to the project sponsors, support teams, and work groups while monitoring the implementation and sustainment of BPR improvements across the State.

Champions continually perform an organizational scan to identify emerging BPR challenges and opportunities. They prioritize available resources to sustain progress and encourage a cultural environment of continuous improvement. Specific responsibilities of the Project Champion include:

- Support the prioritized efforts of all BPR-related projects.
- Conduct periodic reviews of BPR-related resource allocations with the support teams.
- Assess BPR projects' effectiveness via progress against aligned metrics and encourage sharing of ideas and lessons learned across the organization.
- Promote the exchange of BPR knowledge both inside and outside the organization and remove barriers or inhibitors to improvement opportunities.
- Remove fear of failure (punishment) to encourage appropriate risk taking.
- Publicly recognize BPR successes.
- Continually convey a sense of urgency and dissatisfaction with the status quo.

7.4.2 BPR PROJECT SPONSOR

Of all the project roles illustrated above, the Project Sponsor is the key role in the BPR deployment. The Project Sponsor integrates the strategic guidance and direction provided by the Executive Leadership Steering Group with the tactical efforts of the project teams. The Project Sponsor is the organizational leader who owns the process and resources under consideration. He/she has the responsibility to ensure that the project core team understands the expectations of the leadership and is responsible for delivering project results that meet the strategic objectives of the organization. Specific responsibilities of the Project Sponsor include:

- Working with the Subject Matter Experts/Change Agents to determine the baseline data and status of the process being examined and developing specific metrics or targets for improvement
- Identifying organizational gaps and opportunities and nominating potential opportunities to the organization senior leadership or steering committee for prioritization
- Approving the project charter that provides initial guidance to the core team
- Providing resources and guidance to the core team to ensure project success
- Removing or mitigating obstacles that the core team may encounter
- Overseeing the project status reviews
- Reviewing and validating the financial, operational, and process improvement benefits and results at the appropriate phases
- Reviewing and approving solutions derived by the project teams
- Recognizing team successes
- Capturing and sustaining the improvement results to include assessing control metrics (output metrics) after project completion to ensure that performance improvement gains are maintained
- Supporting the strategic communications efforts of the organization

7.4.4 SUBJECT MATTER EXPERT/CHANGE AGENT

The Subject Matter Expert (SME)/Change Agent coordinates the Strategy, Design, Analyze, Improve, and Sustain (SDAIS) phases and provides leadership for Core Team's BPR Project. He/she serves as the deployment lead under the direction of the Project Sponsor and with the support of the Project Champion. Specific responsibilities of the Change Agent include:

- Leading Transformational Change. The SME/Change Agent serves as the catalyst for the BPR within the organization. He/she provides the necessary training, coaching, and mentorship to spread understanding to the project sponsors, core team and process performers to ensure a successful transformation effort.
- Major Project Leadership. The SME/Change Agent leads the BPR deployment, ensures the deliverables in each of the phases are met and coordinates multiple subordinate elements within each phase. He/she must coordinate the BPR project with the Project Sponsor and the various Core Team

members. SME/Change Agent leadership includes identifying opportunities; defining and justifying improvement initiatives; negotiating resources; launching improvement activities; managing deployment activities; training, coaching, and mentoring of team members; leading teams to execute action plans; tracking project status and results; anticipating and removing barriers; and developing team members.

- Technical Leadership. The SME/Change Agent provides direction on the application of BPM tools and methods to the organization's leadership, process leads, project sponsors, and team members.

- Measuring Results. The SME/Change Agent provides the Project Sponsor and Champion with project improvement results versus baseline measurements and recommends corrective action, as required, if overall results do not meet expectations. The SME/Change Agent is also responsible for validating the operational benefits of the BPR project before completion of the Sustain phase.

7.4.5 CORE TEAM

The Core Team is composed of five to seven team members facilitated by the SME/Change Agent. These team members include Department supervision and process performers with expertise in the processes under examination. They are the individuals who have ultimate responsibility and authority for the performance and results of the processes being improved.

The Core Team is ultimately responsible for studying and changing processes to improve their effectiveness and efficiency in accomplishing the organization's goals. The most important task for Core Team is to align the goals and activities of their respective processes with those of the organization. The team accepts process ownership and employs applicable tools and methods in each phase to analyze the current situation, identify ways to improve operations, seek approval for change, and execute business process transformation. These groups utilize the know-how and experience of the individual members and consult, as necessary, with peer groups and other stakeholders to accelerate process improvement. Specific responsibilities of the Core Team include:

- Leading individual projects that can be conducted within their level of expertise

- Supporting more complex projects by leading specific efforts within their functional area of responsibility

- Advising Project Sponsors on the selection of team members

- Managing the administration and daily work assignments of team members

- Assisting the Project Sponsor in implementing approved process improvement recommendations

- Ensuring projects are integrated with other organizational activities and the overall mission and strategic objectives

- Coordinating and facilitate team activity

- Implementing continuous process improvement activities using BPR tools, techniques, and processes

- Seeking simplified and/or new ideas and ways to perform their jobs

- Participating in ongoing education and training to continuously improve their performance contributions

- Participating in regular team meetings to identify, analyze, and select possible solutions to problems

- Implementing solutions under the supervision of Process Leads and/or Project Sponsors

- Identifying other project opportunities that fit within the organization's priorities

7.4.6 CRITERIA FOR IDENTIFICATION OF BPR PROJECTS

The criteria for identifying a BPR project are described in the Business Transformation Strategy as part of the IT/IRM Strategic Plan. Once a candidate initiative is identified, the following should also be added to the selection process:

- Willingness of the organization's leadership to spearhead and promote the reengineering process

- Urgency to complete a BPR activity to improve services to constituents, support management decisions, and/or reduce costs

- Opportunity for success

7.4.7 DOCUMENTING THE ORIGINAL AND IMPROVED PROCESS

To support the implementation of this methodology, the original and improved process is documented (based on Gartner's "just enough" recommendations, thus avoiding analysis paralysis). Microsoft Visio and the standard Business Process Model and Notation (BPMN) typographical and illustrative conventions will be used until the State identifies a specific tool for creating the BPMN and Business Process Execution Language (BPEL)[11]. The Visio-based documentation allows the State to take advantage of the ultimate goal for BPMN which is to provide a simple means of communicating process steps and throughput information to other business managers, users, process implementers, and system developers, as appropriate.

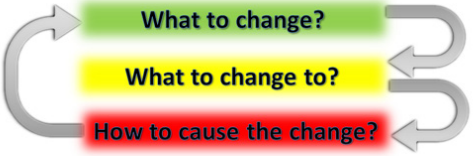
7.4.8 IDENTIFYING AND RECORDING IT CHANGES OR REQUIREMENTS

Throughout the process IT changes and/or requirements that are logical outflows from the TOC BPR process are captured in a Systems Requirements Document (SRD) that includes full traceability to processes. The resulting SRD can be used to improve existing systems, if appropriate, and/or in the acquisition of new systems.

[11] The BPMN tool requires funding, acquisition, implementation, and a certain amount of training. MS Visio is an easy-to-learn, easy-to-use tool that is fairly prevalent within the State. Files can be saved as in .PDF format for viewing by non-Visio users.

7.4.9 ORGANIZATIONAL CHANGE MANAGEMENT

Managing the change process is an integral element of a successful BPR implementation. The over-arching structure for organizational change management is a three-step process of identifying:



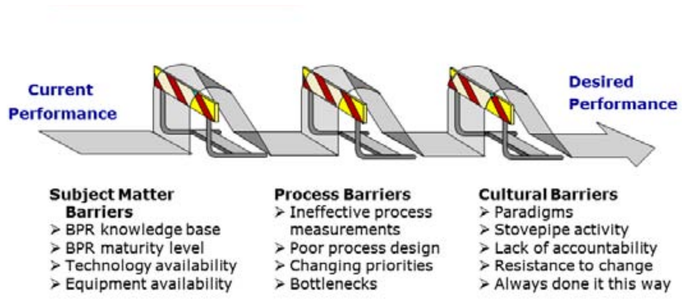
1. What to change?
2. What to change to?
3. How to cause the change?

Organizational change management begins with reviewing current performance and measuring it against the standard set by the organization's management. It is not possible to improve what is not measured. This measurement gauges the current level of performance against the desired future performance level. The resulting analysis can highlight a variance that needs to be corrected, as well as performance that is inconsistent with achieving the overall goals.

At the heart of the change process is the third element of "How to cause the change." BPM incorporates an effective set of change management tools directed at overcoming the barriers to change, whether they are subject matter barriers, process barriers or cultural barriers.

Overcoming the barriers to change involves deploying effective means for project management of the BPR, knowledge transfer, coaching and facilitation, and managing people. One of the big challenges in any type of change initiative is people issues.

Managing the change process is an integral element of a successful CPI implementation. In the SDAIS approach, the following are considered keys to systematic change management:



1. **Educate leaders.** Educate key organization leaders on the concepts of TOC, the roles and responsibilities during the BPM, initial and long-term decisions critical to successful change, and why the change is important.

2. **Challenge presumptions.** Challenge the status quo, empirically demonstrate the competitive benefits of change, and answer the "What's in it for me?" question with a compelling rationale.

3. **Secure agreement.** Secure the agreement of key leaders on the need for change, the objectives necessary to implement that change, and the course of action to begin implementing that change.

4. **Prepare leaders to lead.** Educate and train leaders in defining the new standards for success, and creating the mechanisms necessary to set new expectations and generate results.

5. **Prepare staff to manage the change.** Educate and train the staff to manage the transition from the usual way of doing things to the new business processes, and assume new roles during the change.

6. **Educate the organization's membership.** Educate and train everyone about the new standards and expectations. The investment in this process saves difficulties downstream and helps to ensure a successful process.

7. **Use process to identify and carry through with the business process initiatives.** A formal approach provides the structure for the implementation and execution of the project. Using the deployment cycle creates a model for several important aspects of CPI implementation:

   - Management's input to the process is more predictable and explicit.
   - Management has clearly communicated what is important and who is responsible for what actions.
   - The focus is on coaching and facilitating to achieve successful results.
   - Successes should be celebrated and communicated to reward and encourage continued improvement.

7.5 CONDUCTING A BRP ACTIVITY USING DIFFERENT METHODOLOGY

An organization or Department may decide to use a BPR process that is not based on TOC. When using a different methodology ensure:

- Metrics are identified to document/measure process improvement.
- The As-Is and To-Be processes are documented using BPMN standard notation and that BPEL is achievable.
- The OIMT-selected tool, when available, is utilized for documenting the BPR process.

7.5.1 SELECTION OF THE RIGHT BPR METHODOLOGY

It is important to match the expected outcome of a process change with the methodology that is aligned with producing those results. A quality-focused methodology might not be a match for a process change that is heavily focused on increasing time efficiencies. All process development and reengineering must take into account all aspects: quality, time, resources, and costs. There is usually one of the aspects which is a driving factor by which the other aspects are subordinate, but not eliminated.

Table 16 gives a quick view of some of the features of the various methodologies outlined in this document.

Table 16: Comparison of Methodologies

Program	Six Sigma	Lean Thinking	Theory of Constraints
Theory	Reduce variation	Remove waste	Manage constraints
Application guidelines	1. Define 2. Measure 3. Analyze 4. Improve 5. Control	1. Identify value 2. Identify value stream 3. Flow 4. Pull 5. Perfection	1. Identify constraints 2. Exploit constraint 3. Subordinate processes 4. Elevate constraint 5. Repeat cycle
Focus	Problem focused	Flow focused	System constraints
Assumptions	A problem exists Figures and numbers are valued System output improves if variation in all processes is reduced	Waste removal will improve business performance Many small improvements are better than systems analysis	Emphasis on speed and volume Use existing systems Process interdependence
Primary effect	Uniform process output	Reduced flow time	Fast throughput
Secondary effect	Less waste Fast throughput Fluctuation—performance measures for managers Improved quality	Less variation Uniform output Less inventory New accounting system Flow—performance measure for managers Improved quality	Less inventory/waste Throughput cost accounting Throughput—performance measurement system Improved quality
Criticisms	System interaction not considered Processes improved independently	Statistical or system analysis not valued	Minimal worker input Data analysis not valued

7.6 BPR USING TOC

The five-step TOC process is based on focusing process participants and process managers on the identification of a control point (weakest link) within any process and then understanding how this control point can be enhanced or improved. TOC further enables any process (large or small) to be viewed from the system perspective without necessarily having to dissect it into smaller units. The development of a Throughput Operating Strategy (TOS), which describes how the operation or process should function to maximize both effectiveness and efficiency, serves as the improvement roadmap for the process participants (i.e., process leaders, stakeholders, and/or performers). The TOS also documents how the improvements are measured.

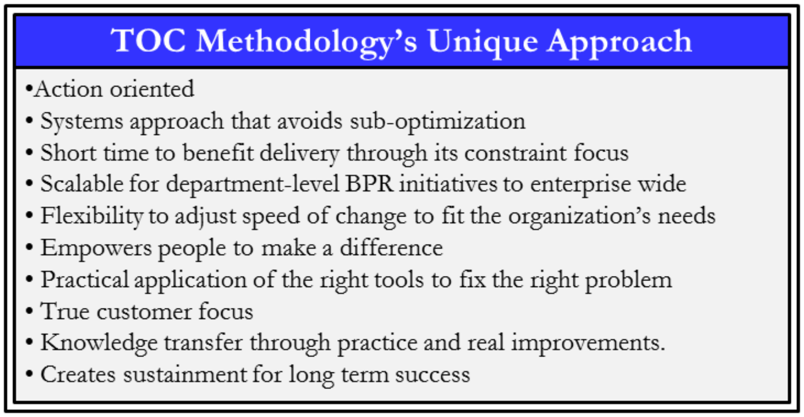
Identify Processes
BPR
Design To-Be
Test & Implement

Coaching and counseling the process leadership and performers via throughput rounds as they implement the TOS actions or long levers, in addition to tracking process implementation success through the defined measurements, are the final element in the any TOC.

The benefits of the TOC approach to BPR are the straightforward and streamlined method, training, and engagement of all process participants in reengineering activities and visible measurement of success factors throughout the process. The training of each individual in the TOC ensures that process performers and their management can continue to improve processes themselves going forward.

The TOC methodology was first formulated in the mid-1980s and made popular through the best-selling book The Goal, by Dr. Eli Goldratt. The TOC has been successfully used to reengineer thousands of processes of various sizes and complexities with the Department of Defense, U.S. Navy, commercial clients such as Intel, Pfizer, Kroger, Proctor and Gamble, Hewlett-Packard, and most recently, in the State of Utah (with resounding success).

TOC methodology enables a process (large or small) to be viewed from the system[12] perspective without necessarily having to dissect it into smaller units like other methodologies do, thereby often creating distortions leading to actions which may improve one process at the expense of another. This common failure of most BPR approaches all too often leads to isolated gains at best and at their worst to erosion in the performance of the system as a whole. TOC functions equally well for a large process or system, such as the overall operations of a government department or agency fulfilling its function and on small, sub-processes such as the process to make an eligibility determination on an application for Medicaid or food stamps or to collect revenue from underpaid tax returns.



TOC Methodology's Unique Approach

- Action oriented
- Systems approach that avoids sub-optimization
- Short time to benefit delivery through its constraint focus
- Scalable for department-level BPR initiatives to enterprise wide
- Flexibility to adjust speed of change to fit the organization's needs
- Empowers people to make a difference
- Practical application of the right tools to fix the right problem
- True customer focus
- Knowledge transfer through practice and real improvements.
- Creates sustainment for long term success

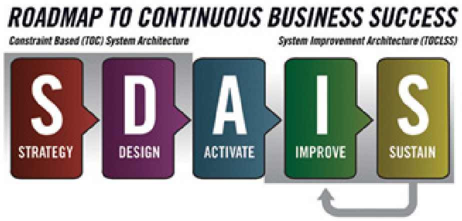
Figure 26: TOC's Unique Approach

The TOC methodology as described in Figure 26 has been applied to thousands of processes and organizations of all types, from government to manufacturing, the military, health-care, education, and nearly every type of private industry. The fundamental breakthrough of TOC is generic—that every system (process, organization, etc.) has a control point, constraint, or weakest link, and the best way to maximize that system's performance is to manage it through that constraint.

But every application is customized because it begins with the unique process or organization it is being applied to. This application results in the development of a Throughput Operating Strategy (TOS) which describes how the operation or process should function to maximize both effectiveness and efficiency. The constraint for each system or process might be different and result in a slightly different TOS than another system that has a very similar purpose and flow. The customization comes in the application of the Five Steps of TOC, enabling each TOS to be defined by the unique characteristics (e.g., throughput, process steps, time) of that process.

[12] System is a set of interacting or interdependent components forming an integrated whole.

7.7 THEORY OF CONSTRAINT (TOC)


ROADMAP TO CONTINUOUS BUSINESS SUCCESS
Constraint Based (TOC) System Architecture
System Improvement Architecture (TOCLSS)
S
STRATEGY
D
DESIGN
A
ACTIVATE
I
IMPROVE
S
SUSTAIN

The TOC views any process as an interconnected system or chain and provides a common-sense focusing approach for optimizing it. TOC is applied using a step-by-step methodology: Strategy, Design, Analyze, Improve, and Sustain (SDAIS).

The TOC is an overall management philosophy and continuous improvement approach first introduced by Eliyahu M. Goldratt. The TOC methodology is geared to help organizations continually achieve better performance toward their goals by a continuous improvement cycle of identifying and eliminating the limiting factors or constraints that impede better performance.

Because any organization is comprised of interdependencies between its parts, TOC often uses the analogy of a chain to describe these processes and systems:

> The strength of the chain is dependent upon the strength of the weakest link, and the constraint limits the flow of work through a system in the same way as the slowest vehicle in a convoy sets the pace of all the vehicles.

Since any system has a constraint that limits it from achieving more of its goals, the TOC's ongoing improvement process seeks to identify the constraint and improve the rest of the organization around it through the use of five focusing steps:

1. Identify the constraint.

2. Exploit the constraint.

3. Subordinate to the constraint.

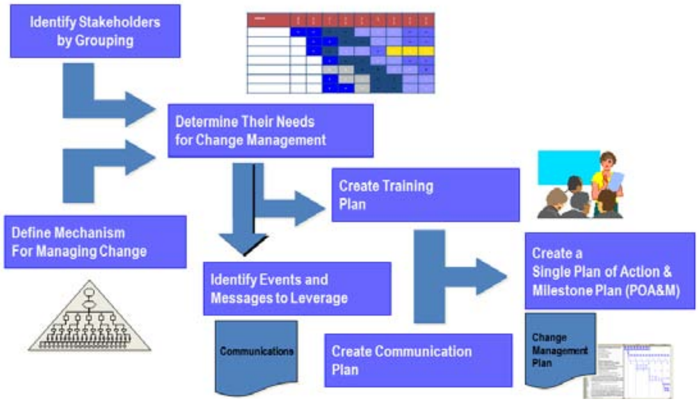
4. Elevate the constraint.

5. Re-evaluate, and then go back to step one.

The continuous process improvement TOC methodology is utilized within an implementation planning framework that can be used by any organization. The business process framework is separated into sections that align with the deployment cycle and is designed to include tasks that are necessary to gain the support and involvement of the organization, identify root causes of current issues in the current state, develop an improved future state for the organization, and to guide the transformation actions to the future state. Appropriate inputs and approval for planning should be obtained from organizational leaders as well as members of the steering committee and support team. Publication of formal plans, where appropriate, will provide an effective means to communicate with each member of the organization and are discussed in more detail below.

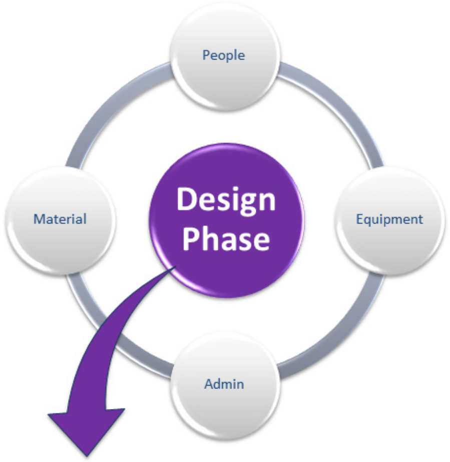
7.7.1 CONSTRAINT-BASED (TOC) SYSTEM ARCHITECTURE

In the Strategy or Pre-deployment phase, TOC approaches any process first from the perspective of defining its purpose for existing and its place/function within the larger organization. Utilizing proven tools, TOC allows the organization that owns the process to re-define and re-build it in order to fulfill its purposes in a more efficient and effective manner.


Identify Stakeholders by Grouping
Determine Their Needs for Change Management
Create Training Plan
Define Mechanism For Managing Change
Identify Events and Messages to Leverage
Create a Single Plan of Action & Milestone Plan (POA&M)
Communications
Create Communication Plan
Change Management Plan

A disciplined and consistent pre-deployment approach to pursuing BPR is an integral part of the leadership required to successfully deliver BPR projects. To succeed, the Strategy phase provides for the application of a project methodology or practice including creation of a formal project charter, communication plans, organizational change management plans, and a plan of actions and milestones (POA&M). The Strategy phase supports the BPR implementation with project management methods, appropriate governance, policy, organizational constructs, and a full complement of the tools required for the deployment of BPR initiatives and the successful completion of the BPR project. This phase is essential to providing a working framework and foundation for integrating the BPR activities within the organizational structure and culture. The pre-deployment activities are shown in the diagram above.

Once the Strategy phase is completed, the TOC Five Focusing Steps are applied in the Design phase to create an operating model for the process or business, or a TOS. The TOS is a common-sense picture of how the process ought to function when operating efficiently and effectively, including an articulation of the key operating metrics or measures for managing it effectively. In other words, "What does good look like today?" and "How is good measured?" The TOS serves as the basis for activating, improving, and sustaining the process in the final three phases.



High Leverage Opportunities that close the gap between the current performance and the designed TOS.

TOC Five Focusing Steps

- Identify the **constraint** of the system or process (the weakest link in the chain).
- Decide how to **squeeze** the most out of the constraint or improve the activities associated with the constraint.
- **Subordinate** everything else within the process to the constraint (so that all steps in the process are synchronized in their operation and in relation to the identified constraint).
- **Elevate** the constraint (to increase the efficiency of the operation, and lower costs).
- When a constraint is broken, **return to Step 1** and repeat the process (creating a model for on-going improvement or roadmap for continuous business success).

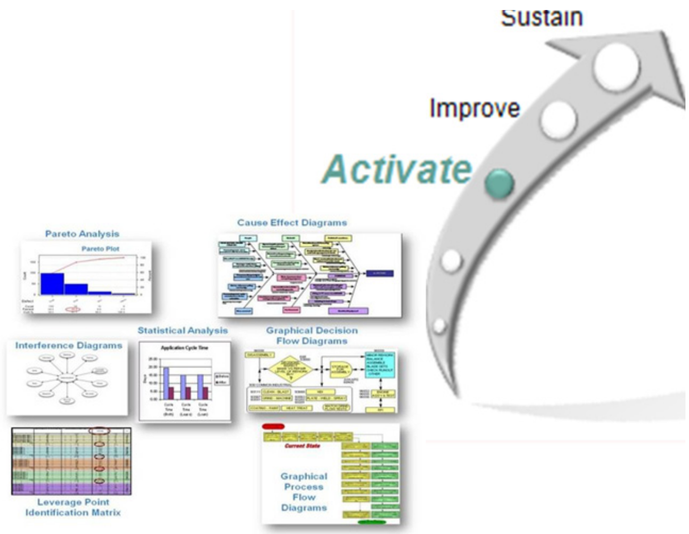
The TOS is a high-level future state process map that represents the combined end-to-end process elements that create or add value as defined by stakeholders, customers, or constituents requesting a product or service. Because it is a high-level map, it is designed to fit onto a single page and only represents the major end-to-end business process linkages. Constructing the TOS as a future-state map describes the vision for the desired future process, and the operational performance metrics for success. The TOC Five Focusing Steps are applied to identify the constraint (control point) at the enterprise level.

After creating the TOS, a gap analysis review with process participants reveals potential leverage points for improving the end-to-end process performance. Typically, this gap analysis follows steps 2 through 4 of the TOC Five Focusing Steps and uncovers issues between the current state and the TOS future state. Because the gap analysis focuses on the overall end-to-end process constraint, it uncovers significant enterprise-level quick win improvement opportunities for the organization. These are called the "long levers" for improvement and drive the next step of the process.

Rapid resolution action plans are developed to address the identified long levers. The execution of the action plan then commences and brings about the first wave of improvement to the organization. This first improvement results are described in more detail below.

To prepare for gap closure, the departmental leadership, supervisors, and process performers are trained in the fundamentals of TOC and the new TOS in a half-day work session. Follow-on training in concepts and tools is conducted through just-in-time, on-the-job training, coaching, and mentoring. This minimizes the organization's classroom training time while permitting an effective knowledge transfer to individuals and teams as needed. This approach to knowledge transfer creates a short cycle between the acquisition of new knowledge, its use, and the delivery of improvement results.

In the Activate phase a more thorough deep dive process mapping and root cause analysis is conducted to fully understand and document the current state (As-Is) processes and sub-processes. A full suite of proven analytical tools are utilized to more thoroughly understand and validate the root causes of process issues and provide a more detailed consideration of the people, processes, materials, and information systems associated with the As-Is process. The Activate phase engages the knowledgeable representatives, process performers, supervision, and other stakeholders to achieve a fully coordinated understanding of the root causes and additional improvement opportunities. This phase is essential to the subsequent Improve and Sustain phases because it is during the Activate phase that process owners and process performers begin to understand the causes of performance gaps at a level aligned to their authority to effect change and take ownership for the improvement process.


Sustain
Improve
Activate
Pareto Analysis
Cause Effect Diagrams
Interference Diagrams
Statistical Analysis
Graphical Decision Flow Diagrams
Leverage Point Identification Matrix
Graphical Process Flow Diagrams

The process mapping and root cause analysis conducted during the Activate phase employs only those tools required to develop the current state understanding. This phase may include:

- Process swim-lane mapping
- Interference diagrams
- Fish-bone root cause diagrams
- Pareto analysis
- Process flow charting
- Statistical data analysis
- Process capability analysis
- Capacity analysis
- Variation analysis
- Defects rate

Once the process and root cause analysis is complete, the As-Is process is redesigned and the To-Be process is completed. This redesign establishes a clear vision of "what good looks like" for each of the lower-level processes that is aligned with the higher-level TOS vision. A further gap analysis between the As-Is and To-Be states are converted into actions (small or large) to close the gaps and bring the process more in line with the desired end state. Prioritization of the opportunities by their business impact guides the sequencing of efforts in addressing the transformation and moving into the improve phase.

The Activate phase closes out with a detailed and concrete plan of action to move the transformation effort through the Improve phase on multiple vectors:

- Bottom-up improvement initiatives led by process supervision and process performers to effect improvement on a daily- and weekly-level on initiatives within the span of control of the organization. Examples include the Throughput Rounds improvement process and work-center improvement initiatives.

- Cross-cutting improvement initiatives led by a core team (or a selected individual) that spearheads cross-cutting improvement initiatives with other organizations or functional silos.

- Top-down improvement initiatives led by a more senior sponsor or improvement team that focuses on systemic policy constraints, structural impediments, or initiatives requiring budgetary authorization. Typically, the implementation lead time for these initiatives is the longest of the three types.

7.7.2 SYSTEM IMPROVEMENT ARCHITECTURE

The Improvement phase is where the actual transformation of the organization takes place. Figure 27 identifies the three initiative-types created as an output of the Activate phase. The TOS is communicated broadly within the organization in combination with concise workshops on the TOC principles that help people understand the rationale behind the changes and get them engaged in how they can better support the TOS. A two-pronged approach is utilized, in parallel, to drive rapid local and cross-cutting improvement initiatives and demonstrate tangible results based on the identified measures of success. A crosscutting functional core team is created to address the identified long levers at the system level. Their responsibility is to design and execute changes which cannot be made solely at the front-line level. These may include changes in performance metrics, policies, procedures, and other systemic changes that require organizational shifts.

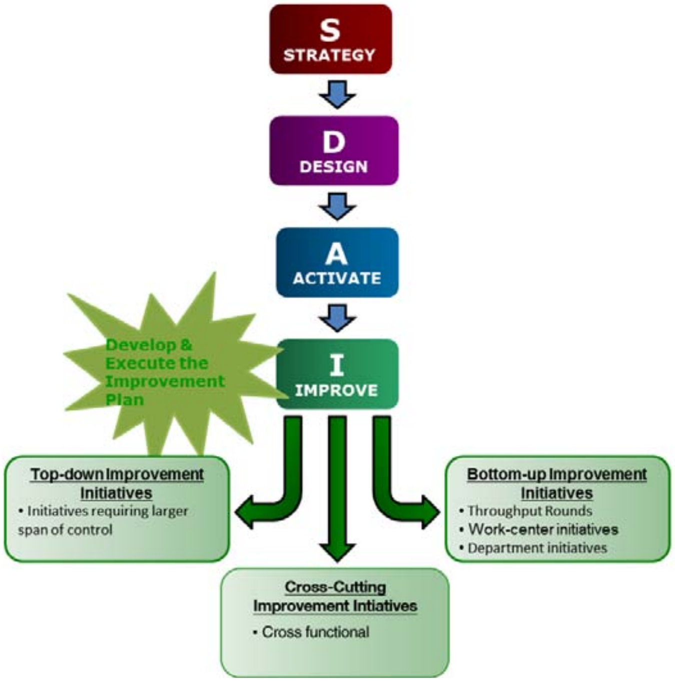

S
STRATEGY
D
DESIGN
A
ACTIVATE
Develop & Execute the Improvement Plan
I
IMPROVE
Top-down Improvement Initiatives
• Initiatives requiring larger span of control
Bottom-up Improvement Initiatives
• Throughput Rounds
• Work-center initiatives
• Department initiatives
Cross-Cutting Improvement Intiatives
• Cross functional

Figure 27: Improvement Phase Initiatives

At the same time, the change process is driven broadly across the organization through a regular (daily or weekly) process known as Throughput Rounds. Throughput Rounds are led by management or supervision and involve the front line staff responsible for executing the various steps of the process. These are short stand-up meetings where the staff compares the TOS to what is actually going on day-to-day to identify areas where things are out of step with the TOS. Fixes to local process issues or course corrections are developed on the spot and, to the extent possible, implemented that day or managed through an action register. Issues that cannot be addressed by the staff themselves are referred to the core team along with useful suggestions or best practices that can then be propagated to other departments for adoption.

The actual changes are designed and executed by the managers and staff of the process. This promotes a high-degree of ownership in the changes and greatly accelerates implementation and results. Great care is taken to ensure that the changes not only improve the process as a whole but also the lives of the people involved in the process. This keeps everyone motivated and ensures incentive for continued improvement.

A third track of improvement initiatives proceeds in parallel with the other two tracks, but it is driven by a top-down process led by leadership and project sponsors to address larger, more systemic issues that require high-level resolution or where the improvement initiatives require budgetary authorization.

Together the three parallel tracks of improvement initiatives drive the BPR and organizational performance to a significantly higher level.

Toward the end of the SDAIS methodology, the focus of all activities shifts to actions that will sustain the new process or mode of operation. The entire BPR using TOC is designed, not as a one-time improvement, but as a methodology for continuous improvement, and the close coaching and mentoring of management and staff are integral parts of the work.

During the Sustain phase, monitoring plans and a measurement dashboard are developed and used to ensure the process gains are maintained. The dashboard metrics provide continuous monitoring capability of the critical process parameters and leading metrics of process performance. If not monitored, improved processes often revert back to what they were before. As soon as processes are changed, it is important to document the changes and standardize the new processes. In conjunction with the dashboard, the Sustain phase develops the response plans for the organization if a problem with the process develops and the metrics indicates degradation in performance. The response plan provides for automatic response to the indicators of sustainment loss (or backsliding).

Two significant components of the Sustain phase are:

1. To ensure there are updated documents and operating procedures for the improved processes. (Note: Failure to document the improved SOPs can be a significant source of backsliding on the improvement gains.)

2. To expand on the organic expertise to apply the next wave of improvement initiatives—a second wave of improve and sustain initiatives—independently.

While the above constitute the majority of the time required for the Sustain phase activities, several other important activities take place to promote the sustainment of the BPR activities:

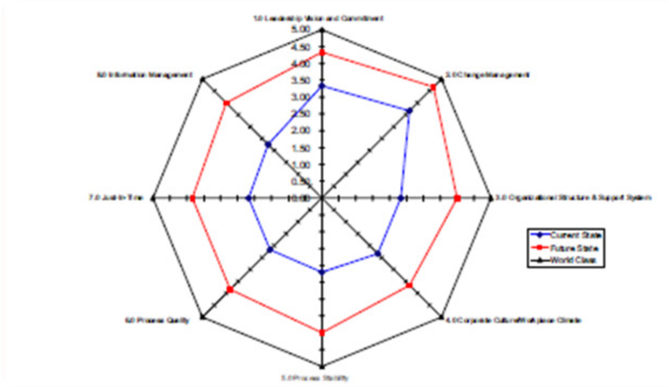
- **Reviews for any replication opportunities.** The replication of successful improvement solutions to similar processes in the organization saves time and effort from unnecessary reinvention and duplication. It can be a force multiplier of the improvement gains. During the Sustain phase, a concerted effort is made to identify those opportunities for replicating successful solutions.

- **Celebrate BPR project success.** Successes should be recognized, celebrated, and communicated to reward and encourage continued improvement.

- **Communicate publicize, and promote results.** Close-out of the Sustain phase includes creating documentation for the BPR, the performance gains, lessons learned, and other project documentation so that the transformation may be communicated as needed.

- **Conduct self-assessment periodically.** Periodically using a tool such as a maturity assessment will keep the organization focused on proper criteria to support the BPR deployment.

BPR Assessment Example – Spider Diagram

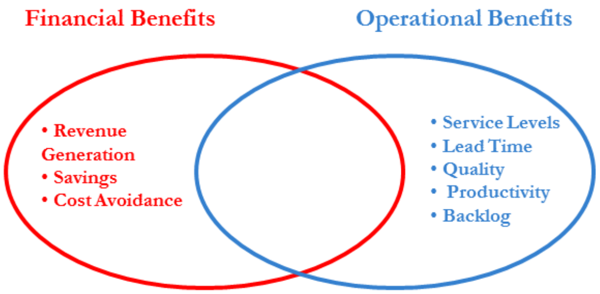


The SDAIS BPR model is one of continuous improvement. Once the SDAIS reaches its end, the process recycles back for a second wave of improvement initiatives to reach for an even higher level of performance. If additional analysis of process issues is required, then the follow-up waves may recycle back to include elements of the Analyze phase.

7.8 MEASURING PROCESS IMPROVEMENT

7.8.1 OUTCOME METRICS

TOC BPR projects yield a wide range of benefits that are categorized as having either financial or operational benefits. Any BPR improvement project must have the potential to generate some type of financial or operational benefit in order to merit the obligation of resources. Financial benefits are those that conserve or produce resources that can be measured and aggregated in dollars.



There are generally three types of financial benefits:

- Revenue generation
- Savings
- Cost avoidance

Operational benefits are normally associated with meeting external critical constituent or stakeholder requirements and/or internal critical business requirements that improve the services to other organizations. Operational performance benefits are measured in non-monetary terms. For example, constituents may want faster service times of a certain service or product where a product or service is delivered faster or more consistently.

Error! Reference source not found. illustrates the fact that financial and operational benefits are ot distinct and independent categories. There is a dynamic relationship between the two. For example, improvements in operational performance will usually produce revenue generation/direct savings/cost avoidance.

While financial benefits are measured in terms of dollars, the metrics for operational benefits can vary greatly, depending upon how the critical constituent requirements and/or critical business requirements associated with a process are articulated.

The several common metrics for operational benefits include:

- **Improvements in process lead time/process cycle efficiency.** If a BPR project reduces lead time, the process cycle efficiency will be improved.
- **Man-hour reductions.** Process improvements often result in the conservation of significant human resources. Man-hour reductions will also generate financial benefits in the form of savings or cost avoidance.
- **Reductions in defects.** If the BPR project reduces the number of defects in a process, the improvement may be measured.
- **Backlog reduction.** When a BPR project improves the constraining process, the average rate of completion increases and there is a corresponding reduction in the workload backlog.
- **Productivity.** BPR improvements often result in improvements in more than one operational factor that can be related in a single measure. Productivity for example, is a measure of the ratio between output and human resources.

As part of the Design stage described above, and in concert with the organizational leadership, the operational outcomes that have value in supporting the process mission are articulated: constituent-oriented, outcome-based operational metrics. A set of agreed-upon relevant, meaningful, and quantifiable baseline metrics are then developed for the BPR project. These baseline measures are utilized throughout the duration of the BPR to monitor and communicate the BPR project's value delivery in terms that matter to the leadership and are relevant to constituent's needs.

A measurement system analysis, conducted in the Design phase, of the process ensures that relevant measurements and metrics meet the criteria for baseline measurements and the validity of the data used.

BPR financial and operational baseline metrics must meet five key characteristics:

1. **Valid** metrics that actually measure what they are intended to measure.
2. **Obtainable** metrics that can actually (and practically) be gathered in a timely manner.
3. **Accurate** metrics that can be trusted to give the right information.
4. **Repeatable** metrics that give the same answer under the same conditions every time.
5. **Actionable** metrics that allow us to do something with the information they provide, which requires both relevance and timeliness.

7.8.2 LEADING METRICS VERSUS LAGGING METRICS

To effectively measure the BPR, an XY Matrix process is used to develop both leading and lagging metrics. Measures are called lagging metrics because they are collected and reported after something has happened. They are results-oriented and fine for tracking overall performance trends, but by the time a lagging metric reflects a problem, it may already be having a major impact.

Leading metrics help predict what will happen, allowing at least some problems to be anticipated and avoided. A leading metric might be a frequently recorded basic process metric coupled with a defined set of expectations or limits. Process performers need leading metrics to minimize problems.

As part of the Design stage described above, the management of the process articulates what the key metrics or measures should be in order to motivate the right actions from the process performers and the organization as a whole. Measures are documented as part of the one-page process definition and TOS. The TOS succinctly describes how the process ought to function when operating efficiently and effectively, including the key operating metrics or measures for managing it effectively.

7.9 NOTIONAL TIMELINE FOR A BPR USING THE TOC METHODOLOGY

The TOC five-phase SDAIS Methodology delivers a rapid launch-to-benefit realization through its focus on the key constraining processes. Unlike other BPR processes, the SDAIS process does not involve spending months in planning, defining, and development phases before delivering on the promise of improved results.

Long BPR project cycle times, such as the typical eight or nine months needed for Define, Measure, Analyze, Implement, and Control (DMAIC) Six Sigma projects, is opportunity lost. Relative to other BPR methodologies, SDAIS provides a significantly compressed timeline for benefit realization.

The disciplined and focused SDAIS process results in a two-pronged benefit delivery pattern (illustrated in Figure 28). The first wave of improvements is launched at the completion of the Design phase, usually one to two weeks after initiation of the BPR project. The next waves of improvements result from the multiple initiatives launched in the Improve phase to be carried forward through to the Sustain phase. Since time to execute the different initiatives will vary, a mixture of both short- and medium-range improvement initiatives is combined to produce an accelerated benefit realization curve.

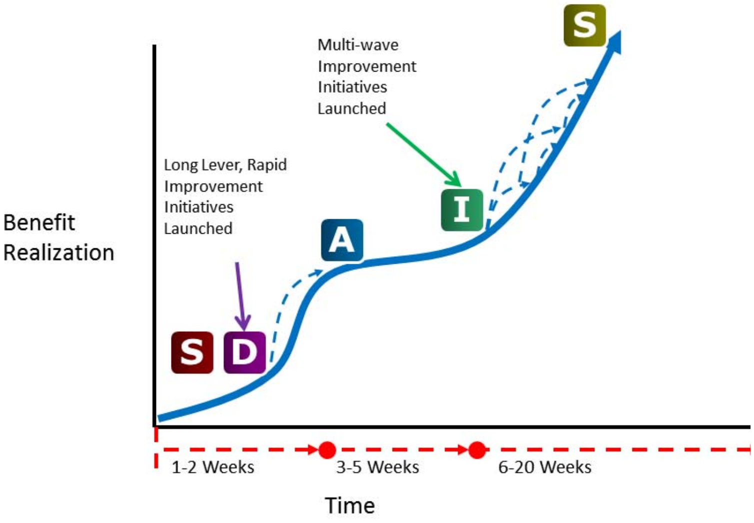


Figure 28: SDAIS Improvement Curve

Table 17 - Notional Schedule and Time Commitment for a BPR Activity Using TOC

SDAIS Stage	Schedule and Milestone	Activities
S	One week or less	• Half-day kick-off and TOC training for Organizational Leadership • Project charter development • Structuring roles and responsibilities • Project Plan of Action and Milestones (POA&M) • Communication Plan
D	One week or less	• Half-day workshop to document a simple diagram of the process flow and TOS and the As-Is process in standard BPMN notation • Half-day kick-off and training of all process performers (trained in groups) • Capture IT/IRM requirements, as appropriate • Calculate baseline performance measures • Identify and define key process performance indicators • Apply five-steps process to identify long-leverage, quick-win opportunities
A	Three-five days Long levers milestone	• Less than a half-day: Long-levers milestone workshop • Gain concurrence on the long levers for improvement with Organizational Leadership and establish teams to address each • Launch improvement plans to address long levers
A	Three-five weeks	• Process and root cause analysis; document and understand the As-Is process and sub-processes • Redesign the process based on its purpose and true business requirements, including "what good looks like" for each local area (To-Be) • Document To-Be process in standard BPMN notation • Perform gap analysis • Capture IT/IRM requirements • Implement new process-level metrics
I, S	6-20 Weeks	• Implement throughput rounds to engage everyone in the improvement process and address issues • Generate solution ideas to close performance gaps • Prioritize and implement improvement waves • Project manage the improvement waves to completion • Measure and quantify results versus baseline performance • Coaching and mentor the organization • Provide over-the-shoulder training • Meet with Organizational Leadership as a Steering Committee • Capture IT/IRM requirements • Develop process monitoring, Control and Response Plan (dashboard) to sustain improvement gains • Document and standardize process solutions (SOPs) to sustain improvement gains • Implement process review/operational reviews to sustain improvement gains • Identify replication opportunities • Training to expand the organization's expertise • Prepare next wave of improvement initiatives
S	Deliverable	• Complete BPR and document results to date • Sustain and build on initial results • Deliver SRD

7.10 LEAN

Over the years, Lean has been adopted, modified, changed, and in many ways mashed to a point where now it is often seen as an almost Zen-like experience for an organization to strive toward. At a very high level, Lean systems give people at all levels of a Department common skills and a shared way of thinking to systematically drive out waste through designing and improving activities, connections, and process flows. Commonly seen as being created and fine-tuned by Taichi Ohno and often referred to as the Toyota Production System, Lean has changed from Ohno's original intent of improving internal activities so that an organization can process at a greater flow.

Essentially, Lean is an all-encompassing process that requires the involvement of all functions of a Department within the State. Lean is highly disciplined approach that, while it can product revolutionary results for a Department, does take a considerable amount of time, effort, and persistence to implement. Lean is best suited for high-volume operations within the state where they are repetitive activities required to achieve service to citizens or other government functions. Focus is on improvement processes and implementing discipline, practice, tools (both IT and non-IT) and strongly emphasizes developing and fostering a culture of looking to eliminate wasted movement.

Lean focuses on the elimination of wasted (the Lean word for this is muda) activities in the following areas:

- Transportation—the movement of items
- Waiting—how long does something sit idle with no activity being performed
- Overproduction—producing more of something or service than required by the end user
- Defects—doing something wrong
- Inventory—creating something or performing a service so it will be waiting
- Motion—movement that does not provide value to the end user
- Extra processing—functionality that is not required by the end user

The Lean Methodology for the State attempts to remove waste and non-value added activities from a system or process. The goal is to either eliminate this waste from the process or system or to transform the process into a value-added process to either citizens or to the government.

7.11 LEAN PRINCIPLES TO PRACTICE

The following principles are applied when attempting to perform a Lean reengineering project. It is important to note that for Lean to reach its full potential for a State Department, the concept of performing Lean needs to be based on what can be considered a value chain. A value chain can be described as what are all the different processes that are linked together to create the entire system that provides service to citizens or support for service to other Departments. A simple analogy is to think of each link in a chain as an individual process with all the various links intertwined together making the entire chain. Lean should work with an entire chain view.

7.11.1 SPECIFY VALUE

A value-added activity can be described as an activity that satisfies an end-user's requirement that the user would be willing to pay your organization a service fee. These activities need to be the focal point and are what delivered with maximum efficiency. Value-add is the core contribution that a Department provides to the citizens of Hawai'i or to other Departments in the State and are what are to be delivered with high quality, high availability.

7.11.2 DEFINE THE VALUE STREAM

The value stream is the actual process map that identifies every action required to deliver service to citizens or to another State Department. This map clearly shows the how value being provided flows thorough the organization to the end consumer. The initial objective of this defining and laying out the value stream is to explore the system for elimination of waste or optimization of the process. A valid value steam should begin and end with either a citizen of the State for external systems or with a Department for internal process supporting other State Departments.

7.11.3 VALUE FLOW

Processes that provide service have to be organized in a manner to facilitate a smooth flow of services throughout all the processes that create the entire system. The following principles need to be considered to help in creating an optimized flow:

- Schedule processes for level loads across all the processes. The key component is to synchronize the rate of flow through the system to the acceptable level of the user.
- Physical layout of the office could facilitate the smooth flow of the service being provided to the citizen.
- Statistical process controls at the source to help with monitoring and controlling the processes to reduce rework of service to citizens.

7.11.3.1 THE CONCEPT OF KAIZEN (ONGOING IMPROVEMENT)

Often in an office environment or in a State work area the largest hindrance to process is clutter or lack of standardization in the space. The removal of clutter or arrangement of work items brings the following benefits for the State:

- Improved maintenance—for example, motor vehicles
- Improved safety, better maintenance of equipment—State-owned mowing or leaf removal equipment
- Ownership of workspace—employees will take pride in their work area
- Improved productivity—less waste from workers losing or misplacing equipment
- Improved morale—evidences exists that clean, organized workspaces improve employees' morale

This is where the concept of Kaizen (meaning ongoing improvement) is implemented for an organization. The execution of Kaizen uses specific tools and techniques that a Department in the State would deploy though the entire Department. Successful Kaizen required management attention and commitment, workforce involvement (this includes union and exempt employees), quantifying and communicating the benefits of continuous improvement, and standardization.

7.11.4 END-USER PULL

Lean systems work best with the flow of the process is based upon and driven by citizen or Department demand for service. Department resources will be activated on to perform service when a trigger is activated for work to begin. Additionally end-user pull is ideal when performed in a one-piece flow in which each operation work only on piece at a time and had does not wait for buildup of multiple items such as forms or applications.

By working each item in a one-piece flow identifies problems and addresses quality issues and increases communication within and across Departments in the State. One-piece flow also assists in identifying waste in a system or process more quickly from the elimination of any noise that a system naturally causes from sometimes getting a process right.

7.11.5 KANBAN

Setting up a kanban system for the State of Hawai‘i while based upon a kanban system for a manufacturing system represents a reverse order. The primary technique of a kanban system for the State is the use of small lot sizes and the ability to improve communication. The following kanban areas are important for the State:

- All work has a specified content, sequence, timing and outcome.
- Connection points must be direct in an almost yes-no manner for request for service.
- The path to the next step in the process must be simple and clearly understood (workflow).

An item of note: quality assurance is an important element of any Lean process, and a pull system will not function properly in the absence of high-quality work. All kanban systems require:

- Worker responsibility
- Measurement
- Enforcement of compliance
- Automatic inspection of product or service

7.11.6 PERFECTION

The last phase of Lean is to refine the process to remove as much variability in the execution as possible. By this point in the project, the majority of the waste should have been identified and addressed so as to remove the waste from the system or process. The system should contain only activities that add value to the service that is being provided to a citizen or to another Department. This is the phase where standard operating procedures are created and put in place as well as controls for the system to ensure that the optimized system is followed and followed every time.

7.11.7 AGILITY

When waste in a process is identified to be eliminated, it is imperative that speed of elimination of this waste is a priority to position the State to make further advancement in eliminating waste. When followed as designed by Ohno, Lean is a quick method of process improvement by activating all resources involved in the process from primary resources to stakeholders in the removal of waste in the system.

Project management needs to focus on desired results and how to quickly enhance the ability of the project to increase customer satisfaction take into account the human factor of the waste to be eliminated, and any financial or budgetary factors. To achieve the desired goals quickly for a Department, the following must be addressed:

- Kick-off and planning
- The establishment of urgency to improve
- Vision of the desired end result or voice of the customer (VOC)
- Training requirements
- Goal setting
- Identification of roadblocks and barriers that are to be removed to achieve
- Use of the State's project management processes

While developed and refined by discrete manufacturing like Toyota, Lean is a tool that is effective for areas where processing of information is needed. Areas such as accounting, citizen communication, and legislative communication are all areas for consideration for Lean.

7.12 SIX SIGMA

Six Sigma is a disciplined methodology using data and statistical analysis to measure and improve an organizations operational performance. The main focus of Six Sigma is the identification and elimination of defects in a process. Six Sigma's name is derived from the statistical reference to six standard deviations or 3.4 defects per million opportunities.

Originally developed in the 1980s by Motorola to respond to quality assurance standards that did not provide the level of granularity that Motorola needed to keep up with competition, Motorola developed this new methodology to assist in the transformation of the culture. Over time, Six Sigma evolved from a metric to a methodology to a management system for the company. In the 1990s, Motorola saw the positive impact to their organization, and then they began to sell this methodology to other organizations which then allowed for Six Sigma to develop into what it is today.

Six Sigma is a project-oriented approach to quality assurance improvement that typically revolves around two sub-methodologies that have the tools and techniques necessary to achieve sustainable quality improvement. The first is the DMAIC methodology, and the second is Design for Six Sigma or DFSS.

7.12.1 DEFINE, MEASURE, ANALYZE, IMPLEMENT, AND CONTROL (DMAIC)

DMAIC is focused on operational improvement in a process. The DMAIC method is aimed at improving an existing process in the State, and it is a step-by-step method to review and improve the process or system.

7.12.2 DEFINE

The Define phase is typically the most important phase of DMAIC process. It is in this step of the methodology that the problem needing resolution is defined. In addition to defining the issue, this phase of the methodology is where goals are also set in place. The perspective of the end user has to be taken into account and can be understood using VOC techniques. Six Sigma places high importance to identifying and defining the problem with often quantitative and qualitative definition provided to explain the problem.

7.12.3 MEASURE

In the Measure phase, the data necessary for understanding the process is gathered and centralized. The key aspects of the current process are taken into consideration and noted down. In this phase the gathered data is also data is measured against different parameters using statistical tool. This information is used to create baseline performance and put operational performance of the As-Is in place.

7.12.4 ANALYZE

The Analyze phase is where the gathered data is analyzed using different statistical tools. The analysis helps in deeper understanding of the problem. The cause-and-effect relationship of various factors is taken into consideration. Measures are taken so that no factor of the process is left out of the analysis. With the root cause identified, it becomes easier to work on the process and solve the problem.

7.12.5 IMPROVE

During the Improve phase, the process development is carried out using different techniques, such as design of experiments (DOE), which are used in establishing process capability. The data gathered and analyzed has an important role to play in the improvement phase. Different solutions to the problems are first identified, and then after analyzing the pros and cons of each of them, the best of them is adopted.

7.12.6 CONTROL

The last phase is Control. So that changes to processes do not deviate from the set goal created in the define phase, control mechanisms are set up. In case of any variance, the problem is identified immediately and measures are taken to rectify the problem. Various methods such as standards and procedures, pilot and solution results, and training are performed to ensure deviation does not occur.

7.13 DESIGN FOR SIX SIGMA (DFSS)

Design for Six Sigma (DFSS) is similar to DMAIC and is used for the designing of services to be provided to an end user that do not exist. To accomplish the desired goals, design, optimize, and verify (DOV) is used. DFSS is comprised of four phases which have detailed steps with each phase. DFSS phases include Identify, Design, Optimize, and Validate.

7.13.1 IDENTIFY

This phase begins the process of creating a formal tie of the design to specification given or from a VOC exercise. The Identify phase involves developing a team and chartering this team to gather VOC or specifications of what is required for success. Essential steps in this phase include:

- Establishment of the business case
- Identification of the technical requirements
- Determination of roles and responsibilities
- Setting milestones
- Identify and outline customer requirements

This phase also includes specific tools and techniques for accomplishment of the realizing the above items:

- Quality functional deployment
- Failure means and effects analysis
- Integrated product (service) delivery system
- Target costing
- Benchmarking

7.13.2 DESIGN

Design is the second phase and consists of identifying functional requirements, development of alternative concepts, and the evaluation of these alternative concepts and selection of the best concept. The essential steps for this phase include:

- Formulate a concept of design

- Identify potential risk

- For each technical requirement identify the design parameters

- Prepare the procurement plan

- Use DOE or other analysis tools to determine influence of various concepts for technical requirements

The key tool set for this phase includes:

- Risk assessment
- Engineering analysis
- DOE
- Analysis tool
- System engineering tool sets

This phase should be given to the complexity of the process. As steps are added to address this the complexity of the solution increases, and thus introduces more risk; if complexity can be reduced, the potential for success increases.

7.13.3 OPTIMIZE

For the Optimize phase, the use of process capability information and statistical tolerance must be considered in the approach. Developing detailed design elements, prediction of performance, and optimizing design all take place in the optimize phase. This is where the desired sigma level or quality level is established and then incorporated into the design of the process. The essential steps for this phase include:

- Assess the process capabilities to achieve quality requirements
- Optimize the design to minimize variance to the process
- Design the system for performance and reliability
- Use the Lean technique of error-proofing or poka-yoke
- Establish quality tolerances
- Optimize the cost

The key tool set for this phase includes:

- Process capability models
- Monte Carlo analysis

7.13.4 VALIDATE

The Validate phase consists of testing and validating the design. As increased testing using formal techniques and pilots occur, the feedback of accomplishing the requirements should be shared. The essential steps for this phase include:

- Prototype test and validation
- Assess performance, failure modes, reliability, and risk
- Design iterations
- Final phase review

The key tool set for this phase includes:

- Risk assessment
- Disciplined new process introduction
- Acceptance testing

7.14 INTEGRATED TOC, LEAN, SIX SIGMA (ITLS)

The iTLS method combines various aspects of the TOC, Lean, and Six Sigma processes. This method emphasizes long-term improvement by first identifying the main problem, measuring possible success, highlighting specific aspects, and finally, committing to a solution. iTLS acknowledges that goods and services are network based, with many problems limiting their production. By using iTLS, users can limit some of these major factors.

iTLS takes certain aspects from the TOC, Lean, and Six Sigma methods and combines them into a single unified method which results in better financial results than the three methods done separately. iTLS produces results from basic business understanding as well as various systematic instruments to improve the overall wellbeing of a company. This method can be used for any aspect of the company, ranging from its basic production to its final product or service. By utilizing the iTLS method, a company can keep customers happy, increase profit, and create a stronger core of business leaders.

iTLS uses the main functions of each of the three other practices to produce the best results possible. TOC can identify which problems are the biggest and, when fixed, can result in the greatest profit. Lean methods focus on removing waste from a system, using more efficient and safer practices. Six Sigma techniques aim for the perfection of the system, limiting the variability in it and therefore creating a more consistent environment. By integrating all three, iTLS catalyzes results, obtaining much larger benefits than each would bring separately. To recap, TOC identifies the biggest blockages in a system, and Lean and Six Sigma create solutions to eliminate the problems so the system can run as efficiently as possible.

Mobilize and Focus
Exploit the Constraint
Eliminate Sources of Waste
Control Process Variability
Control Supporting Activities
Remove the Constraint and Stabilize
Reevaluate the System

Figure 29: iTLS Approach

Why choose iTLS?

iTLS is the only solution that has both quantitative and empirical evidence to support its claims. It is the only method that combines the other three approaches, using each one's main focus to create the best possible solution. By only using the most efficient practices from the three methods, iTLS has virtually no holes in its system. By using its seven-step process, one can reap the benefits iTLS has to offer.

7.14.1 WHAT ARE THE ITLS STEPS?

The combined iTLS approach uses the following seven-step process:

1. Mobilize and focus
2. Decide how to exploit the constraint.
3. Eliminate sources of waste from the constraint.
4. Control process variability and error.
5. Control supporting activities.
6. Remove the constraint and stabilize.
7. Reevaluate system performance and go after the next constraint.

7.14.1.1 MOBILIZE AND FOCUS TO IDENTIFY THE CORE PROBLEM

The first step is the most vital. Without identifying where the main problem is, the biggest benefits cannot be obtained. Thus, this step needs to properly identify where effort should be put in to achieve these results. Various tools can help identify the core problem. By identifying what the problem is, the proper tools of use can be identified as well.

If there is a single step that causes the most problems, it must first be identified. This can be done by examining the overall flow of the process, taking it step-by-step to identify the major cause. After identifying the problem, the next step lies in quantifying the possible benefits. Do we expect an immediate increase in throughput? (Throughput is not just how much we can produce, but both how much we can produce and sell.) If we also want future throughput, other actions need to be identified to guarantee we sell and produce more.

If the benefit sought is decreased expenses and overall cost, how much is expected to be saved, and is this a realistic goal? If the solution results in fewer people needed, what will we do with the extra employees? Floor-space represents a similar problem. If less floor-space is needed as a result, will the rent also cost less? What will be done with the savings? These questions need to be addressed so we can focus on immediate versus future benefits.

Once the goals have been properly identified, along with the possible benefits, we can rank the efforts in terms of priority. Afterwards, employees can be organized and a schedule can be created.

When the problem doesn't have an easily identified root, a different method is needed. This situation occurs when various policies prevent the proper action from being identified. When this happens, the cause-effect-cause way of thinking is the best technique for identifying the major problem and finding a viable solution.

7.14.1.2 DECIDE HOW TO EXPLOIT THE CONSTRAINT

When a physical constraint is the main problem, many actions can result in an increased throughput. If the setup is faulty or the technology continues to fail, Lean is the best method for solving the problem. If the problem is a lack of control in the process, Six Sigma techniques will reduce the amount of waste produced due to random variation.

Before breaking a constraint, a time buffer should be implemented so damage is mitigated from feeding operations. Time buffers also help to identify the core problems in a system. Once the constraint is eliminated, the time buffers can be limited or removed.

A number of solutions can be implemented to improve throughput and eliminate constraints. There is a valuable distinction to be made between value-added and non-value-added activities. Although both activities can be viable solutions, a value-added activity can be the better improvement action. Before choosing which method is better, one should analyze both to see which produces better results.

7.14.1.3 ELIMINATE SOURCES OF WASTE FROM THE CONSTRAINT

At this phase, we create various measurements to keep track of our benefits as well as to ensure that although wastes are eliminated; regression doesn't occur. If we are off-schedule and are not able to meet the proposed benefits, improvement efforts should be analyzed to prevent resources from being wasted. Further methods should be identified so that we can continually increase throughput and reduce operating costs. CE-CNX (Cause and Effect with Control, Noise, X-factor characterization), and Failure Mode Effect Analysis (FMEA) can assist in this effort.

7.14.1.4 CONTROL PROCESS VARIABILITY AND ERROR

Improvements tend to regress over time. Controls and measurements should be implemented to limit the regression.

7.14.1.5 CONTROL SUPPORTING ACTIVITIES

In order to coordinate feeding and following operations with constraint activities, a few steps are needed. Actions that are focused on the constraint needs should be prioritized. It is beneficial for the people dealing with these activities to know why these changes are being made.

7.14.1.6 REMOVE THE CONSTRAINT AND STABILIZE THE PROCESS

While various methods (poka-yoke, MBR, and QBR standardization, monitoring dashboards, etc.) can be used to see if the new process is working, the best method is to educate the affected employees in understanding VOC and VOP and the process behavior.

7.14.1.7 REEVALUATE THE SYSTEM PERFORMANCE AND GO AFTER THE NEXT CONSTRAINT

At this point, the results should be analyzed. Did they meet the expectations? Furthermore, the method of measuring the employees must be reevaluated, especially if the constraint has been removed. Finally, we must decide whether additional improvements should be made or whether the focus should be shifted to different problems. 7.15 Conclusion

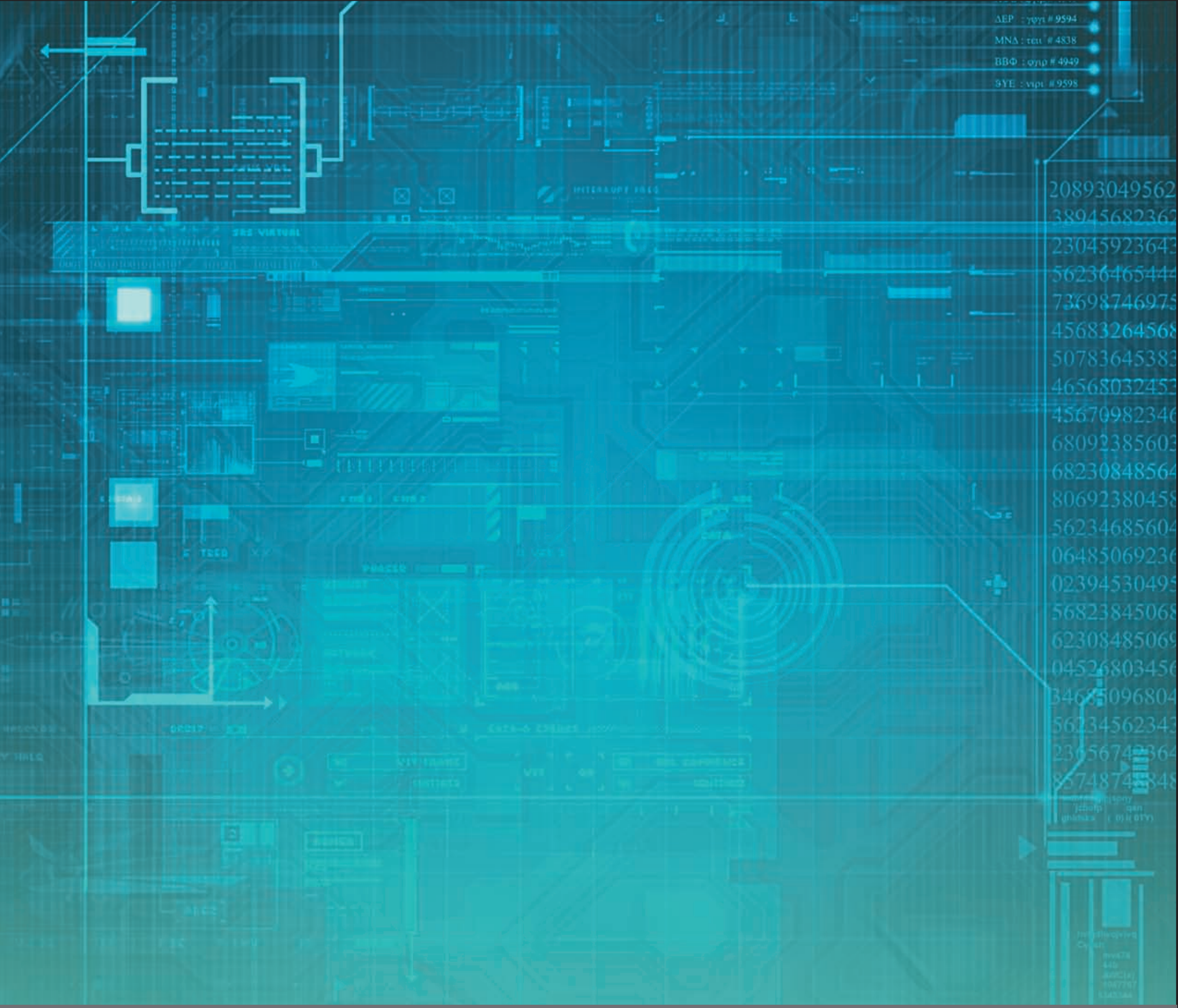
Each of the continuous improvement methodologies for the State has its specific strengths and weaknesses. But each of the methodologies outlined can complement each other to produce a robust and dynamic approach to transforming how Hawai'i does government.

TOC's primary strength is its focus on where to make improvements in the process and where to devote energy and resources to improving the service to citizens or other Departments in the State. TOC focuses on how much of a constraints time is used to actually deliver service. TOC is a good indicator of available capacity to deliver service to citizens or Department. TOC also offers several thinking process tools that are useful in identifying what to change. While TOC has strengths, TOC's shortcoming lies in the absence of robust tools to solve the specific problems it identifies.

Lean offers an impressive and proven array of tools to reduce waste in a process, but Lean lacks focus to point at the most important waste to eliminate. Often this means that Lean efforts do not produce the desired impact on the first try, leading to future problems in delivering service. Lean is effective in improving everything in the system and the holistic approach is important to delivering results.

Six Sigma brings a variety of statistical tools to any continuous improvement effort. The focus of Six Sigma on the reduction of variation of performance of a sieve or process can contribute mightily to the improvement in quality and reliability of a service provided. The defined stop for the SMAIC process does assist in focusing efforts on higher potential opportunities. However, Six Sigma lacks the global approach to process improving and can lead to the problem of improving one area of a system but the entire system is not functioning effectively.

While results can be accomplished with any one of these methodologies, it the combined use of all these methodologies that can accomplish a transformation with how the State does government. It is the use of each of the strengths of the various methodologies used in unison that will deliver results that matter to the citizens of Hawai'i.



8.0 PERFORMANCE MANAGEMENT

8.0 PERFORMANCE MANAGEMENT

8.1 METRICS

Performance metrics enable leadership to see how well each investment is delivering on its mission and business goals and achieve insight into where operations can be improved or resources redirected to deliver better value to citizens. There are typically three layers of performance measures: outcomes, outputs, and inputs. Outcome measures are the most important, as they measure how well we are accomplishing our mission. However, measuring the inputs to and outputs from our processes and activities is also vitally important to provide managers with the information they need to make decisions about how to improve the outcome measures.

8.1.1 OUTCOMES (MISSION AND BUSINESS RESULTS, CUSTOMER RESULTS)

Outcome measures tell us how we are Hawai_ing: how well we are meeting our mission goals of protecting the environment, preserving our cultural heritage, and providing recreation opportunities to citizens. The point of every tax dollar we spend is to deliver on our mission. It is critical that our leaders and managers understand not only how well we are accomplishing that mission, but what impact investment decisions have on improving our mission performance.

8.1.2 OUTPUTS (PROCESSES AND ACTIVITIES)

Outputs are the measures that managers can use to determine whether the processes and activities of the enterprise are being efficient and effective. We look at five categories of output measurements:

- Financial
- Productivity
- Cycle time and timeliness
- Quality
- Security and privacy

8.1.3 INPUTS (HUMAN CAPITAL, TECHNOLOGY, OTHER FIXED ASSETS)

The last type of measure is the inputs or resources we use to achieve our desired outcomes. Improving outcomes would be easy if we had unlimited resources. In a resource-constrained world, however, we need to make the best use of the resources we have. Therefore, our performance is measured not only by the outcomes we achieve, but also by the amount of resources we have.

While all resources can ultimately be described in terms of dollars, the input measures we use fall into three basic types: human capital, technology, and other fixed assets. This categorization is used because dollars allocated to one of these categories are not easily converted to another category, so it is more useful to see what the funding was spent on than just the total amount spent.

PMO DEVELOPMENT PLAN

TABLE OF CONTENTS

1. EXECUTIVE SUMMARY....5

2. INTRODUCTION....7

2.1 Purpose 8

2.2 Associated Documents....8

3. MISSION, VISION, GOALS, AND OBJECTIVES....9

3.1 Mission 9

3.2 Vision....9

3.3 Goals.................. 9

3.4 objectives....9

4. PMO FUNCTIONS AND SERVICES....10

4.1 PMO Functions....11

4.2 PMO Services....11

4.3 PMO Support Role....11

5. PMO MAJOR MILESTONES....13

5.1 FY-2012 Priorities (Milestones)....14

5.2 FY-2013 Priorities (Milestones)....14

6. PMO ORGANIZATION AND RESOURCES....15

7. CRITICAL SUCCESS FACTORS....16

8. ASSUMPTIONS AND BUSINESS CONSTRAINTS....17

8.1 Organizational Structure, Functions, and Services....19

8.2 Functional Capability and Responding to Capacity Demands....20

8.3 Project Management Office FTEs: Position Staffing, Percentage of Time for Assignment and Vacancies....21

9. RISKS AND ISSUES....22

10. ROLES AND RESPONSIBILITIES....24

11. PROJECT MANAGEMENT FTES – OPERATIONAL REQUIREMENTS....27

12. CONTRACT SERVICES REQUIREMENTS........28

13. DELIVERABLES........30

13.1 Program Service Deliverable........30

13.2 Program Deliverables........30

14. PROGRAM MANAGEMENT DELIVERABLES........31

15. PROGRAM/PROJECT CONTROL........31

15.1 Action Item List........31

15.2 Issue Log........31

15.3 Risk Register........31

15.4 Deliverable Review and Approval........31

15.5 Quality Assurance:........31

APPENDIX A: PROGRAM SUMMARY DESCRIPTION........32

APPENDIX B: PROGRAM SCHEDULE........34

APPENDIX C: PROGRAM FY-2012 COST ANALYSIS (SUMMARY)........36

APPENDIX D: PROJECT MANAGEMENT SERVICE........38

APPENDIX E: ADDITIONAL INFORMATION........42

FIGURES

Figure 1: Functions and Focus........6

Figure 2: Domain of Responsibilities........8

Figure 3: PMO's High-level Functions and Focus........11

Figure 4: PMO Responsibilities........12

Figure 5: The PMO Deliverables and Functions........12

Figure 6: PMO's Target Structure (Positions, Services, Functions, and Grades)........18

Figure 7: PMO Personnel Requirements........19

Figure 8: PMO Functional Priorities and Maturity Strategy........20

TABLES

Table 1: FY-2013 Priorities (Milestones)........14

Table 2: FY-2013 Priorities/Responsibilities (Milestones)........14

Table 3: Project Management Office FTEs: Position Staffing, Percentage of Time for Assignment........21

Table 4: Risks and Issues........23

Table 5: Relationships and Responsibility Matrix........23

Table 6: Project Management Office FTEs – Operational Requirements........27

Table 7: Contractor Requirements........29

Table 8: Program Deliverables (Milestones)........30

1. EXECUTIVE SUMMARY

1. EXECUTIVE SUMMARY

To mitigate the trends[1] such as those documented by The Standish Group, and in support the Office of Information Management Technology's (OIMT) commitment to management excellence, the Program Management Office (PMO) will deliver the State of Hawai`i's mission and services to citizens of Hawai`i. The PMO will use best practices as the catalyst for organizational and cultural change. Through the promotion and use of best practices, the PMO will:

- Increase the probability of meeting users' needs and expectations.
- Improve project planning.
- Define clear business objectives, understanding options by identifying their benefits, costs and risks.
- Facilitate better decision making before a project's start and during a project's execution.
- Increase probability of executing projects successfully, on time and within budget.
- Reduce project risks of delays, cost overruns, and failure.

As a trusted partner, the PMO vision is to facilitate, guide, and assist all statewide IT programs and projects to success. The PMO's outcome goals are that projects achieve success according to the program and portfolio objectives. Its performance goals are to successfully guide and support all projects to successful project objectives derived from the portfolio and strategic plan. Its organizational goals are to provide support to all projects and project practitioners in the form of appropriate best practice leadership and just-in-time services. The PMO's objectives are to develop a world-class best practice capability and capacity to assist all statewide IT programs and projects and provide support and guidance for State of Hawai`i departments. Figure 1 below illustrates the functions and focus of the PMO.

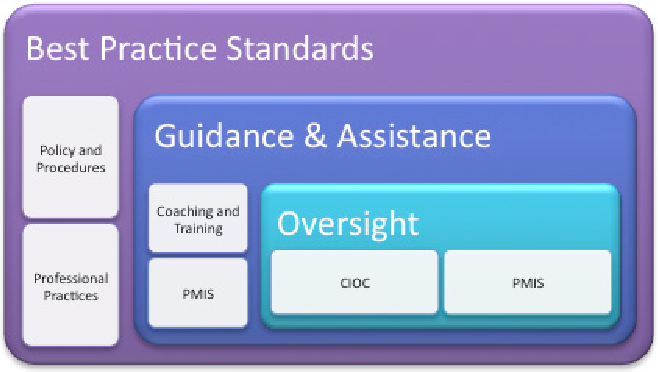


Figure 1: Functions and Focus

PMO Functions. The PMO's business services can be summarized into three high-level functional responsibilities:

1. Guidance
2. Assistance
3. Oversight.

These high-level functions apply to three primary focus areas: practitioners, practices, and management tools across the State of Hawai`i's government.

PMO Services. The PMO has the inherent responsibilities to perform specific services. These services facilitate the key high-level functions of guidance, assistance, and oversight. The services are:

- Program and project management policy
- Best practice standards
- Oversight—project performance accountability
- Central tool management
- Central PM artifact repository management
- Portfolio project management/inter-project coordination
- Workforce assessment—practitioners and teams
- Training and education—curriculum identification, design and development, and delivery
- Resource (Project Manager) coordination

[1] Source: The Standish Group's report CHAOS Summary 2009, April 23, 2009. This report is an annual follow-up to the hallmark baseline report, The Standish Group Report, 1994, that surveyed over 1,200 U.S. Information Technology (IT) users.

2. INTRODUCTION

3. MISSION, VISION, GOALS, AND OBJECTIVES

2. INTRODUCTION

2.1 PURPOSE

The PMO of the OIMT provides project management planning and best practices services to statewide IT initiatives.

As a trusted partner, the PMO vision is to facilitate, guide, and assist all State of Hawai`i IT projects to success. In support of this vision, the PMO's responsibilities include: administrative support to the project review process (Chief Information Officer Council [CIOC]); coordination with department PMOs; and guidance, oversight, and assistance to projects as outlined in Figure 2.

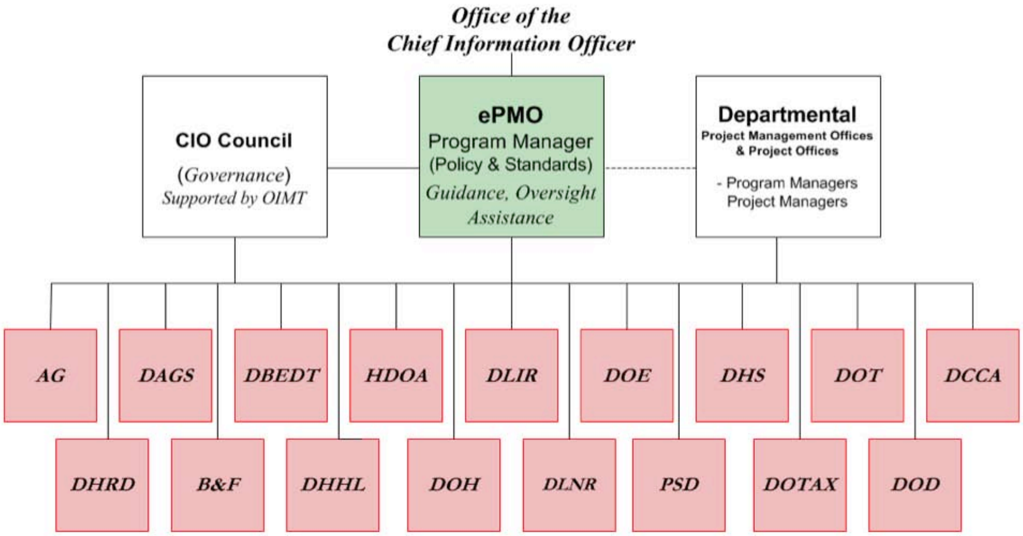


Figure 2: Domain of Responsibilities

- The PMO functional value proposition can be summarized as the following:
- Identifies, develops, and coordinates organization-wide program and project management policy and best practice standards and procedures
- Manages the enterprise management tool that supports both the projects and the portfolio of project needs
- Identifies, coordinates, and manages the cross-project dependencies of all projects. In concert with Enterprise Architecture (EA), this is inherently the PMO's co-responsibility to coordinate.
- Coordinates with the Portfolio Management Office (PfMO) regarding project, program, and portfolio objectives serving the strategic plan
- Provides project start-up capability needed for new projects, bridging the initial gap for projects to get organized
- Plans, designs, develops and/or coordinates PM training and educational requirements and curriculum
- Provides specialized just-in-time skillsets that would be prohibitively expensive for any one project to develop
- Identifies and coordinates program and project manager resources for enterprise programs and projects

2.2 ASSOCIATED DOCUMENTS

- State of Hawai`i PfM
- State of Hawai`i BPM
- State of Hawai`i PMM
- Clinger-Cohen Act (CCA) of 1996
- ANSI Earned Value Management System Standard (ANSI/EIA-748-A), November 2006

- Project Management Body of Knowledge (PMBOK® Guide), ANSI/PMI 99-001-2004
- State of Hawai`i Business Transformation Strategy and IT/IRM Strategic Plan, 2013
- Baseline of Information Management and Technology and Comprehensive View of State Services (referred to as the Final Report) prepared by SAIC
- Program and Portfolio Management Key Initiative Overview, Gartner, July 2011

3. MISSION, VISION, GOALS, AND OBJECTIVES

3.1 MISSION

The mission of the PMO is to provide program and project management leadership, expertise, experience, and training to teams for initiating, planning, and guiding implementations and completions. The primary responsibilities are to manage and control the constraints by ensuring plans are implemented on schedule, within budget, and within scope. Maintaining alignment to the strategic goals and mission of the State of Hawai`i is critical to successful program and project management, whether projects are managed for the benefit of a department or for statewide critical functions that benefit the entire enterprise and surrounding community. Incorporating program and project management administration with best practice methods and standards that are either based on State of Hawai`i's Strategic Plan or single in purpose and scope ensure consistency is applied effectively and is scalable to be administered across various sized projects.

3.2 VISION

Promote best practice standards and methodologies into a program and project management discipline that advances the core vision and mission of the State of Hawai'i's Strategic Plan through comprehensive and iterative development comprising education, training, and a set of guiding principles.

3.3 GOALS

The PMO's outcome goals are that all projects achieve success. Its performance goals are to successfully guide and support all projects to success. Its organizational goals are to provide to all project and project practitioners support in the form of appropriate best practice leadership and just-in-time services.

3.4 OBJECTIVES

The PMO's objectives are to develop a world-class best practice capability and capacity to assist programs and provide well-planned projects that successfully deliver expected outcomes within budget, on time, and aligned with program and portfolio goals and objectives.

4. PMO FUNCTIONS AND SERVICES

4. PMO FUNCTIONS AND SERVICES

4.1 PMO FUNCTIONS

The PMO's business services can be summarized into three high-level functional responsibilities:

1. Guidance
2. Assistance
3. Oversight.

These high-level functions (shown in Figure 3) apply to three primary areas of focus: practitioners, practices, and management tools.

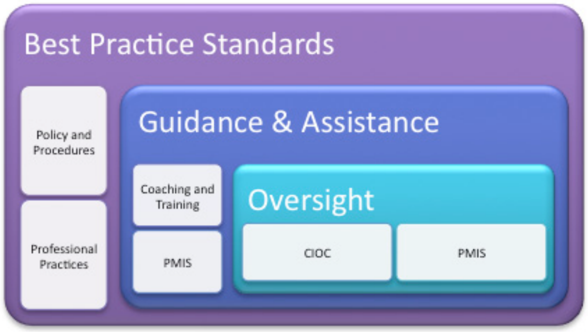


Figure 3: PMO's High-level Functions and Focus

4.2 PMO SERVICES

The PMO has the inherent responsibilities to perform specific services. These services facilitate the key high-level functions of guidance, assistance, and oversight. The services include:

- Project management policy
- Best practice standards—identification, development, and coordination
- Oversight—project performance accountability
- Central tool management
- Central PM artifact repository management and archival
- Portfolio project management/inter-project coordination
- Workforce assessment—practitioners and team evaluation
- Training and education—curriculum identification, design and development, and delivery
- Project support—guidance, coaching, mentoring, and just-in-time assistance
- Resource (Project Manager) coordination

4.3 PMO SUPPORT ROLE

Focus Areas: The PMO's project management (business) focuses on 1) people/practitioners, 2) professional practices, and 3) management tools. Each of these focus areas have their respective standards for performance and best practices.

Responsibility Domain: The PMO's project management responsibility domain for each service is unique, varying from statewide to what's defined by the respective Investment Review Board (IRB). For example, the span of responsibilities for project management policy and standards are statewide. For direct project oversight, the span of responsibility is from OIMT for enterprise infrastructure and mission systems to the departments for performing oversight of their specific mission and non-major systems. Department mission projects that are well run remain within their oversight domain of responsibility (refer to Figure 4 below).

The PMO will provide value across the State of Hawai`i by specifically assisting with the following:

- Identify, develop, and coordinate organization-wide project management policy, best practice standards, and procedures.
- Manage the enterprise management tool that supports both the project and the portfolio of project's needs
- Identify, coordinate, and manage the cross-project dependencies of all projects in concert with EA.
- Provide project start-up capability needed for new projects, bridging the initial gap for projects to get organized.
- Plan, design, develop, and/or coordinate PM training and educational requirements and curriculum.
- Provide specialized just-in-time skillsets that would be prohibitively expensive for any one project to develop.
- Identify and coordinate project manager resources for enterprise projects. For economies of scale, this is inherently the PMO's responsibility to provide and coordinate.

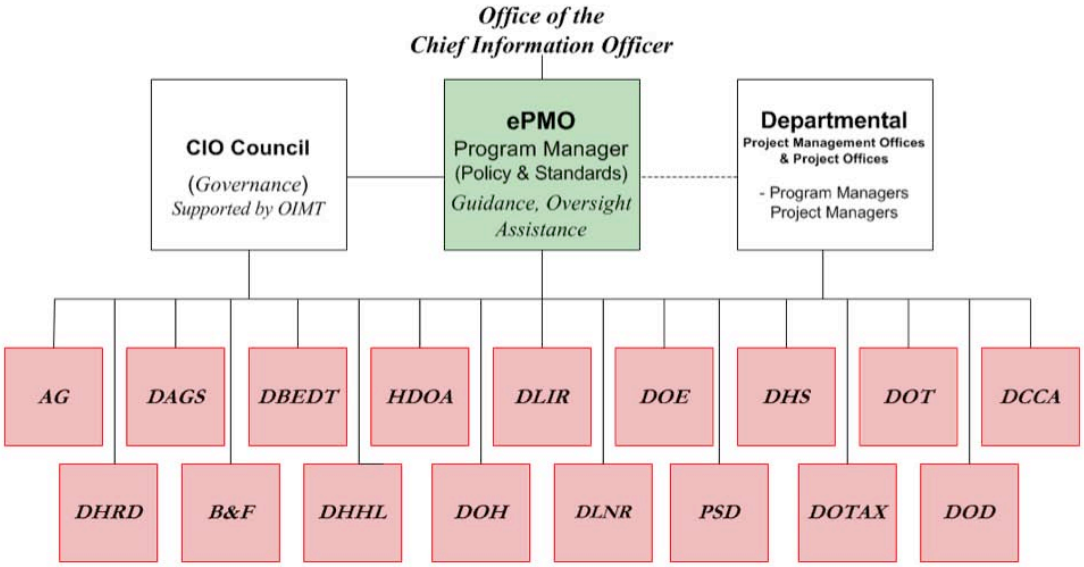
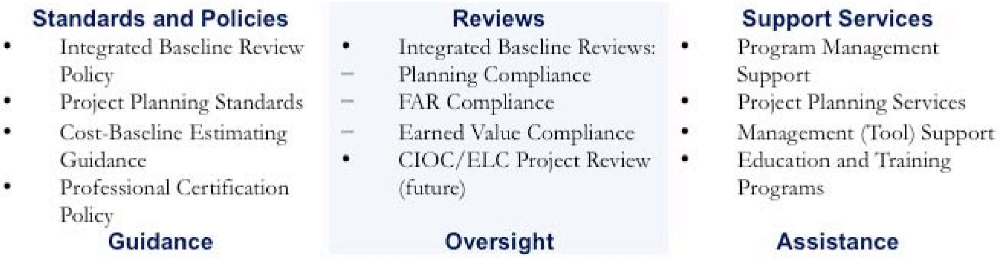


Figure 4: PMO Responsibilities

Other Responsibilities: The PMO will administratively support the Project Review at the CIOC. Additionally; the PMO coordinates with Department Project Management Offices[2] and Project Offices (PO) as shown in Figure 5. The PMO provides guidance, performs oversight, and provides assistance to projects within their domain. Guidance is delivered via **best practice** standards and policies. As seen in Figure 5, oversight is delivered via the **integrated baseline review** (at the CIOC) program and Project Review activities. Project assistance is provided via the Project Management Planning Services (PMPS) program, and the Project Management Information System (PMIS) management tool support.



Standards and Policies

- Integrated Baseline Review Policy
- Project Planning Standards
- Cost-Baseline Estimating Guidance
- Professional Certification Policy

Guidance

Reviews

- Integrated Baseline Reviews:
  - Planning Compliance
  - FAR Compliance
  - Earned Value Compliance
- CIOC/ELC Project Review (future)

Oversight

Support Services

- Program Management Support
- Project Planning Services
- Management (Tool) Support
- Education and Training Programs

Assistance

Figure 5: The PMO Deliverables and Functions

[2] The PMO coordinates with department PMOs to identify and coordinate Project Manager resources for enterprise efforts.

5. PMO MAJOR MILESTONES

6. PMO ORGANIZATION AND RESOURCES

7. CRITICAL SUCCESS FACTORS

5. PMO MAJOR MILESTONES

5.1 FY-2012 PRIORITIES (MILESTONES)

Table 1: FY-2013 Priorities (Milestones)

FY-2012 Prioritites	Responsible Person or Team	Planned Completion Date
2012 Priority 1: Project Management Office Start-up		
2012 Priority 2: Central PMIS Tool (Project Guidance) Initiate the integrated state-wide project and portfolio management tool, including process on demand (POD).		
2012 Priority 3: Planning (Project Assistance) Complete OIMT project plans with scheduling to the 85% confidence level.		

5.2 FY-2013 PRIORITIES (MILESTONES)

Table 2: FY-2013 Priorities/Responsibilities (Milestones)

FY-2013 Prioritites	Responsible Person or Team	Planned Completion Date
2013 Priority 1: Mature the Project Management Office Mature the Project Management Office with full capabilities to fully perform all PMO services and capacity to fully support all projects (as needed).		
2013 Priority 2: Central Tool Management (Guidance and Assistance) Mature the PMIS tool (Phase 2), including loading key projects and their project artifacts onto the PMIS, specifically charters.		
2013 Priority 3: Project Review Process (CIOC) (Oversight) Continue to mature the projects oversight, providing management and administrative support to the start-up of the Project Review at CIOC.		
2013 Priority 4: Project Planning (Assistance) Expand PMO's capabilities and capacity (grow and mature), providing guidance and assistance to priority projects.		
2013 Priority 5: Project Execution (Assistance) Oversee or directly manage OIMT projects. When necessary, take management receivership of any project. Projects include OIMT projects.		

PMO Project Started Date: ______________________________

PMO Program Plan - Draft Date: ______________________________

PMM Framework and Planning Standards Date: ______________________________

PMO Program Plan - Authorization Date: ______________________________

CIOC Review and Planning Standards - Review Started Date: ______________________________

PMO Department Manual - Draft Date: ______________________________

PMPS Contracting Vehicle Starts Date: ______________________________

PMO First Hire Date: ______________________________

PMO Start-up Project Completed Date: ______________________________

6. PMO ORGANIZATION AND RESOURCES

Mature the PMO to baseline best practice capability and capacity to support all projects.

The overall objective is to build and provide the following PMO services for all projects through a series of objectives:

- Objective 1: Project oversight
- Objective 2: Central tool management
- Objective 3: Central PM artifact repository management
- Objective 4: Portfolio project management
- Objective 5: Human and team resource assessment and coordination
- Objective 6: Training and education—planning, design, and development
- Objective 7: Training and education—delivery and delivery coordination
- Objective 8: Project support—guidance and just-in-time assistance
- Objective 9: Resource sharing coordination

7. CRITICAL SUCCESS FACTORS

Critical success factors (CSF) increase the probability of success when management focuses attention in these areas. This program's CSFs are:

- All major projects (investments that have Development Modernization Enhancement (DME) components are registered, meaning they have signed project charters (or authorizing documentation) and are authorized.
- Performance Measure: A percentage of major projects (investments that have DME components) have registered projects, meaning they have signed project charters (or authorizing documentation) and are authorized.
- Most major projects (investments that have DME components) have validated project plans, adhering to State of Hawai`i's OIMT policy.
- Performance Measure: Percentage of major projects (investments that have DME components) have registered projects, meaning they have signed project charters (or authorizing documentation) and are authorized.
- All major projects (investments that have DME components) continuously report project performance via the State of Hawai`i dashboard.
- Performance Measure: A percentage of major projects (investments that have DME components) have continuous project performance reporting via the State of dashboard, adhering to the reporting requirements.
- Most major projects (investments that have DME components) perform successfully within
- +/- 20% of cost and schedule.
- Performance Measure: Percentage of major projects (investments that have DME components) performs successfully within +/- 20% of cost and schedule.

8. ASSUMPTIONS AND BUSINESS CONSTRAINTS

8. ASSUMPTIONS AND BUSINESS CONSTRAINTS

- For FY-2013, the PMO will be fully resourced with the Program Manager and 11 positions (FTE budget [$nnK]).
- For FY-2013, the PMO will be resourced with contract funding ($nnK).
- For FY-2013, the PMO will be authorized to set-up the Project Review Process (CIOC).

8.1 ORGANIZATIONAL STRUCTURE, FUNCTIONS, AND SERVICES

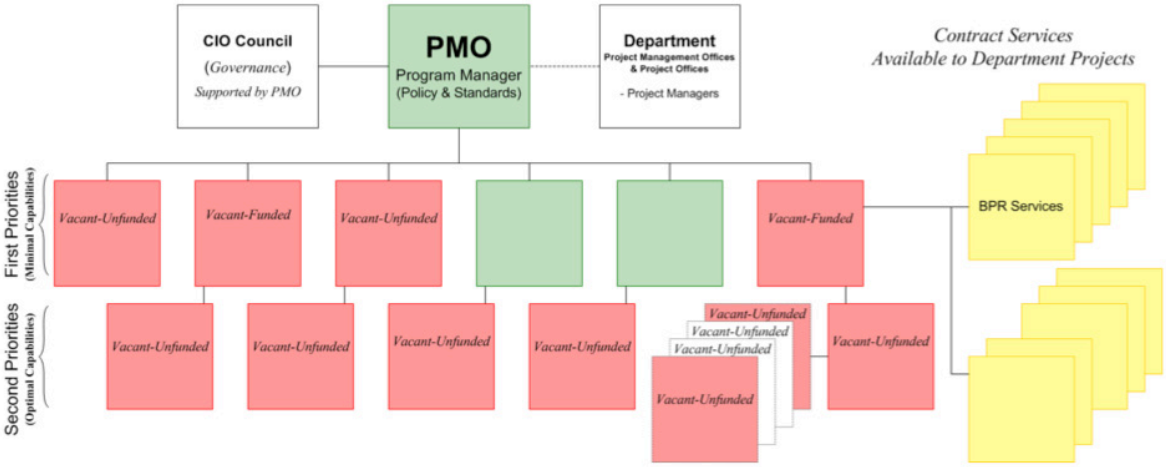


Figure 6: PMO's Target Structure (Positions, Services, Functions, and Grades)

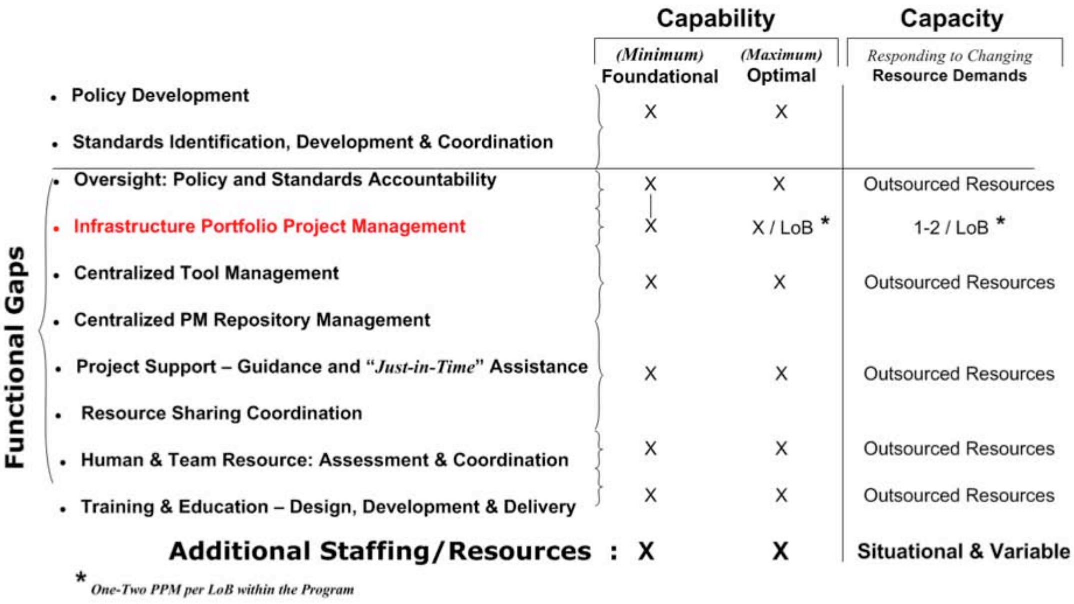
Legend: (Green: FTE filled; Red: FTE vacancy)

The PMO's internal organizational structure is represented by Figure 6 above. (For a detailed descriptions of services, see "Appendix E: Additional InformationAppendix E: Additional Information.") Note: To adjust to varying project management demands, the PMO is organized to collaboratively leverage available Departmental Project Manager resources (PMO = red and Departmental = white) and leverages contract support when needed via the reimbursable contract service (PMPs=yellow) set up by the PMO. In summary, these positions manage, coordinate, or perform the PMO services, listed as:

- Project management policy
- Best practice standards
- Oversight—project performance accountability
- Central tool management
- Central PM artifact repository management
- Portfolio project management/inter-project coordination
- Workforce assessment—practitioners and teams
- Training and education—curriculum identification, design and development, and delivery
- Project support—just-in-time assistance
- Resource (Project Manager) coordination

Externally, the PMO will administratively support the Project Review at the CIOC. The PMO will execute decisions regarding oversight, guidance, and assistance. The PMO will organize and support projects for the oversight reviews. After the fact, the PMO will perform the administrative and documentation follow-up activities, manage integrated baseline reviews, support project initiation and planning phases. Additionally, the PMO has a coordination role with the Department PMOs. Regarding projects, the PMO has oversight, support, and guidance roles.

PMO Maturity Strategy. The PMO's maturity strategy involves further developing the best practice capabilities and capacity to assist all projects. In Figure 7, the capability column shows the staffing levels for foundational (minimum) and optimal (fully developed/maximum) functionality. To perform all services, there is a minimum staffing level necessary to get to the foundational level. To get to the fully developed state, a moderate increase in staffing will take the PMO to the optimal capability level. Staffing beyond this point offers only minor increases in capabilities.



Functional Gaps	Capability *(Minimum)* Foundational	Capability *(Maximum)* Optimal	Capacity *Responding to Changing* Resource Demands
• Policy Development • Standards Identification, Development & Coordination	X	X	
• Oversight: Policy and Standards Accountability	X	X	Outsourced Resources
• Infrastructure Portfolio Project Management	X	X / LoB *	1-2 / LoB *
• Centralized Tool Management • Centralized PM Repository Management	X	X	Outsourced Resources
• Project Support – Guidance and "*Just-in-Time*" Assistance • Resource Sharing Coordination	X	X	Outsourced Resources
• Human & Team Resource: Assessment & Coordination	X	X	Outsourced Resources
• Training & Education – Design, Development & Delivery	X	X	Outsourced Resources
Additional Staffing/Resources :	**X**	**X**	**Situational & Variable**

* *One-Two PPM per LoB within the Program*

Figure 7: PMO Personnel Requirements

8.2 FUNCTIONAL CAPABILITY AND RESPONDING TO CAPACITY DEMANDS

Discussion: Because of the potential for many concurrent and interdependent projects, capacity must be given attention. Capacity is like bandwidth on the network. The network must provide functions (services); it also must have bandwidth for efficient delivery of the services. The PMO's staffing will offer all the necessary functions (capabilities) based on the resources available. When the PMO becomes fully functional, the PMO needs the capacity to provide the **services on demand** to all projects in a scalable manner. As illustrated in the capacity column of Figure 7, this can be provided via outsourcing using indefinite delivery/indefinite quantity (IDIQ)-like contract vehicles.

To provide these types of services on-demand through contracting to meet oversight responsibilities, the PMO must have minimal government staffing to manage this program. The OIMT's PMO resourcing analysis conclusions align with Gartner's principal message of being "lean and mean." To minimally support the hundreds of major and non-major IT projects, the PMO requires nn minimal staffing that includes the Program Manager. To optimally support the hundreds of major and non-major IT projects, the PMO requires staffing of the twelve FTEs. At the high end of the spectrum, the PMO should not grow beyond an optimized staffing level. The strategy for providing needed capacity leverages the IDIQ-like contract vehicles that adjust to varying demands.

Figure 8 below shows the priority of project management functions. These functional priorities are related to vstaffing levels and the development of organizational maturity. The current staffing level of three focuses on policy and standards, better oversight, inter-project coordination, and PM tool support (refer to the red box in Figure 8).

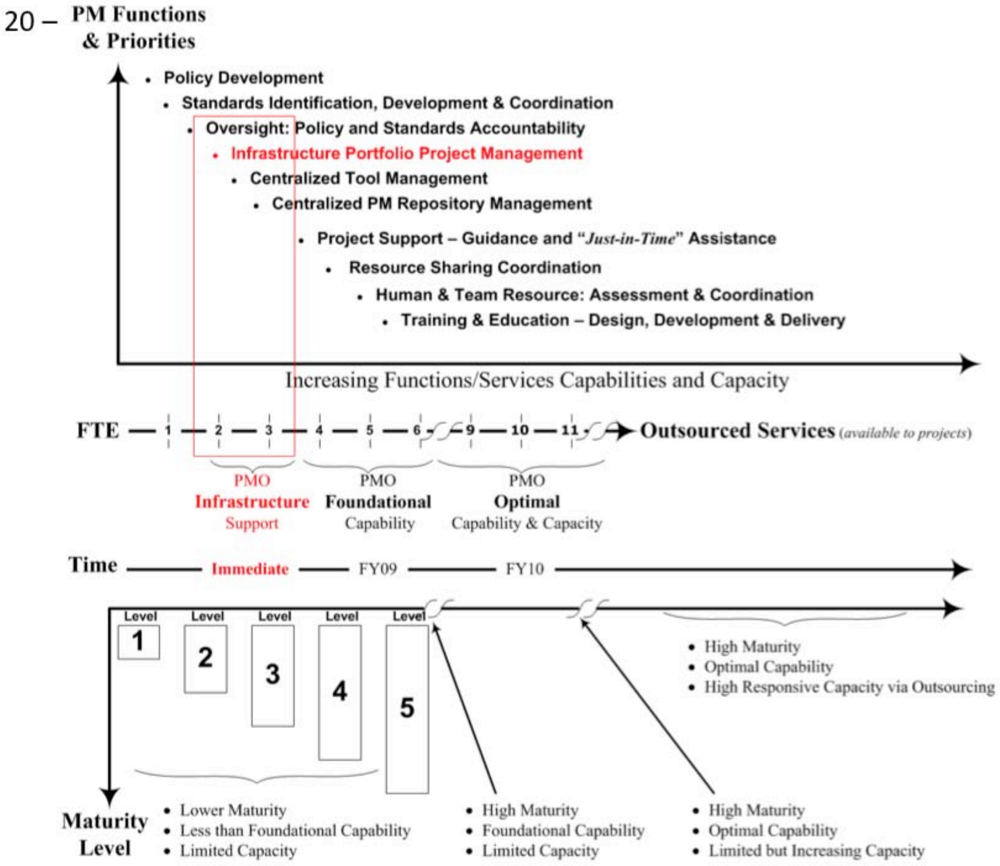

20 –
PM Functions & Priorities
Policy Development
Standards Identification, Development & Coordination
Oversight: Policy and Standards Accountability
Infrastructure Portfolio Project Management
Centralized Tool Management
Centralized PM Repository Management
Project Support – Guidance and "Just-in-Time" Assistance
Resource Sharing Coordination
Human & Team Resource: Assessment & Coordination
Training & Education – Design, Development & Delivery
Increasing Functions/Services Capabilities and Capacity
FTE
1
2
3
4
5
6
9
10
11
Outsourced Services (available to projects)
PMO Infrastructure Support
PMO Foundational Capability
PMO Optimal Capability & Capacity
Time
Immediate
FY09
FY10
Level 1
Level 2
Level 3
Level 4
Level 5
High Maturity
Optimal Capability
High Responsive Capacity via Outsourcing
Maturity Level
Lower Maturity
Less than Foundational Capability
Limited Capacity
High Maturity
Foundational Capability
Limited Capacity
High Maturity
Optimal Capability
Limited but Increasing Capacity

Figure 8: PMO Functional Priorities and Maturity Strategy

When able to perform these functions, the organization takes on more mature aspects of the Software Engineering Institute's Capability Maturity Model[3] (SEI-CMM). To perform all PMO basic functions, the foundational staffing level needs approximately nn additional FTEs. To perform all PMO functions (capabilities) and to be fully responsive to all projects, the optimal level needs approximately nn FTEs. Higher CMM maturity and high organizational performance result from developing all capabilities and developing capacity to deliver these capabilities. Again, a small increase in staffing will take the PMO from the foundational capability level to the optimized capability level. Staffing beyond the optimized point offers only minimal increases in capabilities. Beyond that point, increased performance is realized by developing greater just-as-needed capacity through IDIQ-like PM service contacts.

[3] CMMi: Capability Maturity Model (integrated) ranking, in this case, indicates the project planning and control processes maturity. CMM development was sponsored by the United State Air Force via the Software Engineering Institute (SEI) and detailed in Managing the Software Process, 1989.

8.3
PROJECT MANAGEMENT OFFICE FTES: POSITION STAFFING, PERCENTAGE OF TIME FOR ASSIGNMENT AND VACANCIES

Table 3: Project Management Office FTEs: Position Staffing, Percentage of Time for Assignment

Project Management Office - Service (Function)	Staffing	Percentage Time Assignment	Vacant FTEs
Portfolio Management	Vacancy	100%	1
Policies & Standards (Guidance) and Program Management	Vacancy	100%	1
Project Performance Accountability (Oversight)	Vacancy	100%	1
Project Planning Services (Assistance)	Vacancy	100%	1
Centralized Management Tools (Assistance)	Vacancy	100%	1
Project Records/Artifacts Management (Assistance)	Vacancy	100%	1
PM Workforce Assessment (Oversight)	Vacancy	100%	1
Professional Development (Guidance)	Vacancy	100%	1
Program Manager	Vacancy	100%	5
Project Manager	Vacancy	100%	7
Project Support (Assistance)	Vacancy	100%	4
Program Specialist - Acquisition	Vacancy	100%	1
Program Specialist - Risk	Vacancy	100%	1
Program Specialist - BPR	Vacancy	100%	1
Program Specialist - Communications	Vacancy	100%	1
Program Specialist – Change Management	Vacancy	100%	1
Program Specialist – Requirements	Vacancy	100%	
Program FTEs (supporting the optimal organization)	nn Planned		nn

9. RISK AND ISSUES

10. ROLES AND RESPONSIBILITIES

11. PROJECT MANAGEMENT

FTES—OPERATIONAL REQUIREMENTS

9. RISK AND ISSUES

A **risk** is an uncertain event or condition that, if it occurs, has a positive or negative effect on a Program's objectives, scope, cost, schedule and/or quality. An issue is a risk that has become a reality.

Table 4: Risks and Issues

Risk Register				
ID	Description	Probability 1 = low 5 = high	Impact 1 = low 5 = high	Mitigation Plan
	Issue: Under-resourcing Impact: delayed programs and personnel burnout	5	5	• Fill vacancies • Get additional support through contractors • Communicate and work with OIMT Budget Office, • Office of the Chief Information Officer (OCIO) Business Office and Human Resources to get approval to fill vacancies • Prioritize work • Manage workload expectations of senior OCIO management • Give staff flexibility to telework and extend deadlines where it is not possible to complete tasks
	Issue: Contracting delays for procurements Impact: Program delays and/or increase costs	5	5	• Start requisition process as early as possible and work closely with the State Procurement Office (SPO)
	Issue: Ability to get the cooperation and participation of program representatives in IT project 1. Policies 2. Practices 3. Decision-making Impact: Poor project performance	3	5	• Engage and communicate to better understand program interests • Provide value proposition (needs) so they see their interest in participation in the IT decisions • Use the policy and contract vehicle to establish objectives status and corrective actions

10. ROLES AND RESPONSIBILITIES

Table 4: Relationships and Responsibility Matrix

Relationships	Responsibilities
OIMT-PMO	• Project management policy • Standards—identification, development, and coordination • Oversight—project performance accountability • Central tool management • Central PM artifact repository management • Portfolio Project Management—inter-project coordination • Workforce assessment—practitioner and team evaluation • Training and education—identification, design and development, and delivery • Project support—guidance and just-as-needed and just-in-time assistance • Resource sharing coordination (For details, see "Appendix E: Additional Information.")
CIO (OIMT-PMO Sponsor)	• Authorizes PMO Program funding • Presents program results to major stakeholders and other executive bodies. • Facilitates resolution issues outside of the program • Signs and authorizes project management policy
Project Review Process (CIOC)	• Evaluates project performance results • Develops and drafts project guidance and recommendations • Resolves inter-project level issues outside of the program • Develops, reviews, and/or comments on drafts policy • Quality Assurance: validates project performance directly or via independent validation and verification (IV&V) and integrated baseline review (IBR) • Change Management: evaluates project change requests and develops/drafts change requests guidance and recommendations
Project Sponsors	• Authorize program/project funding • Present program results to major stakeholders and other executive bodies • Facilitate resolution issues outside of the Program

Relationships	Responsibilities
Contracting Officer	• Oversees contracts • Manages task order solicitation. • Supports contract administration. • Administers competitive procurements • Facilitates acquisitions)
OIMT Administrative Staff	• Support program fund actions • Support personnel actions
PMO Service Team Leader	• Provides leadership for Subject Matter Expertise (SME) • Actively participates in progress reviews to ensure critical program information is communicated to all stakeholder organizations • Facilitates resolution of program issues in stakeholder organizations • Defines acceptance criteria • Monitors and controls the work scope, quality, budget, risks, and schedule for the business stakeholders • Manages the day-to-day work of the business stakeholders • Leads, coordinates, and facilitates the business stakeholders' planning and execution of tasks and deliverables • Accountable for the success of the business stakeholders' tasks and deliverables • Ensures appropriately skilled program participants are available when needed • Facilitates resolution of issues and elevates risks
Program Manager	• Monitors and controls the scope, quality, budget, risks, and schedule • Manages the day-to-day work of the program • Defines and manages program risks • Leads, coordinates, and facilitates their team's planning and execution of tasks and deliverables • Accountable for the success of team tasks and deliverables • Ensures appropriately skilled program participants are available when needed • Prepares and presents program reports to appropriate levels of management • Facilitates resolution of issues and elevates risks • Manages acquisitions
Solution Architect	• Ensures all aspects of a solution are integrated, consistent, completes and correct • Facilitates analysis of change requests • Facilitates open communication between other Solution Architects to maintain complete and consistent architecture decisions

Relationships	Responsibilities
Stakeholders	• As the executives from each organization who are impacted by the program, stakeholders authorize their organization's resources required to successfully complete the program • Actively participate in progress reviews to ensure critical program information is communicated to stakeholder organizations • Facilitate resolution of program issues in stakeholder organizations • Define acceptance criteria
Team Leaders	• Monitor and control the scope, quality, budget, risks, and schedule for their area • Manage the day-to-day work of their area • Lead, coordinate, and facilitate their area's planning and execution of tasks and deliverables • Accountable for the success of their area's tasks and deliverables • Ensure appropriately skilled program participants are available when needed • Facilitate resolution of issues and elevate risks
All Program Participants	• Complete assigned tasks and deliverables based on agreed schedule • Act as SMEs for appropriate organizational function • Provide status updates including issues and risks • Provide actual hours worked per week by team • Attend all scheduled meetings • Be prepared to take some responsibility to educate others • Communicate openly and assertively • Respect opinions of others • Agree to work toward consensus • Commit to scope of the program

11. PROJECT MANAGEMENT FTES – OPERATIONAL REQUIREMENTS

Table 6: Project Management Office FTEs – Operational Requirements

Project Management Office - Service (Function)	Staffing	Tech Skills	Experience
Portfolio Management			
Policies & Standards (Guidance) and Program Management			
Project Performance Accountability (Oversight)			
Project Planning Services (Assistance)			
Centralized Management Tools (Assistance)			
Project Records/Artifacts Management (Assistance)			
PM Workforce Assessment (Oversight)			
Professional Development (Guidance)			
Program Management			
Project Management			
Project/Program Support (Assistance)			
Program Support - Acquisition			
Program Support - Risk			
Program Support - BPR			
Program Support - Communications			
Program Support – Change Management			
Program Support – Requirements			
Program FTEs (supporting the optimal organization)	nn Planned		nn

12. CONTRACT SERVICES REQUIREMENTS

13. DELIVERABLES

14. PROGRAM MANAGEMENT DELIVERABLES

15. PROGRAM/PROJECT CONTROL

12. CONTRACT SERVICES REQUIREMENTS

Table 7: Contractor Requirements

Role	Skills	Experience	Duration
CIOC Program and Project Review Services • Status: Not in place • Type: IDIQ • Funding: via the project's sponsoring office • Services: performs IBR to standards on project at the end of planning, before execution approval.	**Contractor** • Project Planning • Cost Estimating • Systems Engineering & Architecture **Government Manager** • Project Planning • Contacting	**Contractor** • Senior **Government Manager** • Senior	Ongoing/Operational
Project Management Planning Services (PMPS) • Status: Not in place • Type: IDIQ • Funding: via the project's sponsoring office • Services: performs Project Planning to standards on project.	**Contractor** • Project Planning • Cost Estimating • Systems Engineering & Architecture **Government Manager** • Project Planning • Contacting	**Contractor** • Senior **Government Manager** • Senior	Ongoing/Operational
Project Management Information System (PMIS) Support • Status: Not in place • Type: BPA-Support Services • Funding: Partial • Services: performs support services for the PM Management Tools (PMIS)	**Contractor** • MS-Project Server • SharePoint Services • System Operations • Project Management **Government Manager** • Project Planning • Contacting	**Contractor** • Senior **Government Manager** • Senior	Ongoing/Operational

Role	Skills	Experience	Duration
Business Process Management Professional Services • Status: Not in place • Type: BPM- Project Management and Support Services • Funding: Partial • Services: performs support services for the departments directly or via OIMT Program	**Contractor** • Project Planning • Business Process Methodologies (TOC, Lean, Six Sigma, iTLS) • Cost Estimating **Government Manager** • Project Planning • Contacting	**Contractor** • Senior **Government Manager** • Senior	Ongoing/Operational

13. DELIVERABLES

13.1 PROGRAM SERVICE DELIVERABLE

- Project management policy
- Standards—identification, development and coordination
- Oversight—project performance accountability
- Central tool management
- Central PM artifact repository management—management of project artifacts and archives
- Portfolio Project Management—inter-project coordination
- Workforce assessment—practitioner and team evaluation
- Training and education— curriculum identification, design and development, and delivery
- Project support—guidance and just-as-needed and just-in-time assistance
- Resource sharing coordination

13.2 PROGRAM DELIVERABLES

Table 8: Program Deliverables (Milestones)

Major 2013 Deliverables (Milestones)	
2013 Priority 1: Mature PMO	Mature the PMO with full capabilities to fully perform all PMO services and capacity to fully support all projects (as needed).
2013 Priority 2: Central Tool Management System	Mature the PMIS tool (Phase 2), including loading key projects and their project artifacts onto the PMIS, specifically charters and IRB authorizing records of decisions (RODs).
2013 Priority 3: Program and Project Review Process (CIOC)	Continue to mature the project's oversight, providing management and administrative support to the start-up of the Project Review at CIOC.
2013 Priority 4: Program and Project Planning	Expand the PMO's capabilities and capacity (grow and mature), providing guidance and assistance to priority projects.
2013 Priority 5: Program and Project Execution	Oversee or directly manage OIMT projects. When necessary, take management receivership of any project.

14. PROGRAM MANAGEMENT DELIVERABLES

- Weekly status reports
- Program reviews
- Departmental performance reporting

15. PROGRAM/PROJECT CONTROL

The items described in this section are required elements of project and program control.

15.1 ACTION ITEM LIST

Project-related action items will be maintained and monitored to ensure awareness of actions necessary for program success:

- PMIS development
- Project Review Board

15.2 ISSUE LOG

A list of program issues will be maintained and monitored to ensure awareness of actions necessary for the program's success:

- PMIS development
- Project Review Board

15.3 RISK REGISTER

A program risk register will be maintained and monitored to ensure awareness of actions necessary for program success:

- PMIS development
- Project Review Board

15.4 DELIVERABLE REVIEW AND APPROVAL

Deliverable reviews will be conducted for all program deliverables to ensure that they are complete, correct, and consistent. Program participants and stakeholders will be asked to participate in these reviews, which can be conducted via email or in person. Review comments will be documented in a Quality Assurance Review Comment Sheet. To sort documents by date, the file name for each QA Review Comment Sheet will be in the format of: YYYYMMDD QA Review Document Title. Each of the identified comments will be categorized by type, severity, and priority. The comments will be analyzed, and then incorporated by the author of the deliverable as appropriate. Comments not incorporated require an explanation back to the reviewer. The final deliverables will then be approved by the designated approvers. The completed Quality Assurance Review Comment Sheets and the approved deliverables will be stored in the OCIO CM Repository.

15.5 QUALITY ASSURANCE:

Quality Assurance activities will be performed to ensure quality control processes are defined and followed. As the program progresses, metrics will be provided on a weekly basis to identify the number of Quality Assurance reviews conducted, the number and priority of comments identified, and the number of approved deliverables completed. If it is found that the review and approval processes are not being performed, then the identified issues will be escalated to the Program Manager for corrective action. The goal of the monitoring effort is to provide visibility on the status of the quality tasks performed for the program.

The verification of program requirements, as documented in the Requirements Traceability Matrix (RTM), will be performed. The requirement verification methods include analysis, inspection, demonstration, or testing. The method by which the requirements will be verified will be documented in the test plan. The results of the verification activities will be documented in the RTM.

Privacy and Security. All program documents will be labeled For Official Use Only in the header and footer. All Certification and Accreditation (C&A) tasks and deliverables required before this program's solution can be implemented in production are part of this program.

APPENDIX A: PROGRAM SUMMARY DESCRIPTION

APPENDIX A: PROGRAM SUMMARY DESCRIPTION

Program Name	Program Management Office (PMO)
Description	The PMO promotes and delivers management excellence based on best practice standards that contribute to achieving the OIMT's missions. The result is that the State of Hawai`i projects achieve success and meet their respective performance goals that contribute to achieving the OIMT's missions. General goals: 1. Outcome Goals: projects achieve success, contributing to OIMT's missions. 2. Performance Goals: the PMO support projects achieve their performance, cost, and schedule goals. 3. Organizational Goals: the PMO provides services and effective support to project and project practitioners' leadership to meet their goals. PMO FY-2012 Goals (aligned to the above general goals): 1. Provide better project oversight and assistance though standardized tools and structure. 2. Initiate the PMIS) tool (Phase 1). 3. Provide guidance and assistance to priority projects; provide planning services to projects. PMO FY-2013 Goals (aligned to the above general goals): 1. Continue to mature the project's oversight capability though expansion of the program. 2. Continue to mature the program and projects oversight, providing management and administrative support to the start-up of the Project Review at CIOC. 3. Mature the Project PMIS tool (Phase 2), including loading key projects and their project artifacts onto the PMIS, specifically charters and authorizing RODs. 4. Expand the PMO's capabilities and capacity (grow and mature), providing guidance and assistance to priority projects; provide planning services to projects. 5. Expand PMO's capabilities and capacities (grow and mature), providing project execution management to priority projects; provide planning services to projects.
Business Areas Impacted	All OIMT mission and mission support offices.
Period of Performance	Ongoing
Performing Unit	Office of the CIO-PMO
Sponsors	Sonny Bhagowalia
Program Manager	Nicholas Harrigan

APPENDIX B: PROGRAM SCHEDULE

APPENDIX B: PROGRAM SCHEDULE

FY-2012 Priority	Planned Completion Date
2012 Priority 1: Mature the PMO Mature the PMO with full capabilities to fully perform all PMO services and capacity to fully support all projects (as needed).	
2012 Priority 2: Central Tool Management (Guidance and Assistance) Mature the PMIS tool (Phase 2), including loading key projects and their project artifacts onto the PMIS, specifically charters and IRB authorizing RODs.	
2012 Priority 4: Project Review Board (PRB) (Oversight) Continue to mature the projects oversight, providing management and administrative support to the start-up of the Project Review at CIOC.	
2012 Priority 5: Project Planning (Assistance) Expand PMO's capabilities and capacity (grow and mature), providing guidance and assistance to priority projects.	
2012 Priority 6: Project Execution (Assistance) Oversee or directly manage OIMT projects. When necessary, take management receivership of any project. Projects include OIMT projects.	

APPENDIX C: PROGRAM FY-2012 COST ANALYSIS (SUMMARY)

APPENDIX C: PROGRAM FY-2012 COST ANALYSIS (SUMMARY)

FY-2012 Spend Plan for 2012 (Dollars)	
Object Class	**FY-2012 Planned Obligations**
11. Personnel Compensation	
12. Personnel Benefits	
13. Benefits to Former Employees	
Sub-total, Comp and Benefits	
21. Travel and Train	
22. Transportation of Things	
23. Communications	
23.a. Rent	
24. Printing	
25. Other Services	
26. Supplies	
31. Equipment	
93.a. Indirect	
Sub-total, Other	
Total	

Note: the funding and gap analysis is as follows:

2012 Priority 1: Mature the Project Management Office Mature the Project Management Office with full capabilities to fully perform all PMO services and capacity to fully support all projects (as needed). ***Priority 1:** Funding represents the overall analysis. The funding information below represents aspects of the overall analysis.		

APPENDIX D: PROJECT MANAGEMENT SERVICE

APPENDIX D: PROJECT MANAGEMENT SERVICE

E.1 **Policy:** Manage, develop, and coordinate Federal and State of Hawai`i PM Policy.

Within the PMO, the Program Manager is responsible for understanding project management policy, regulation, directives and guidance; and coordinates their appropriate implementation into State of Hawai`i policies, directives, and guidance. This includes project management policy, regulation and guidance. This function supports the PMO's oversight and all other functional responsibilities regarding human resources, practice standards, and professional tools. It is inherently the PMO's responsibility; this provides one set of directives, standards and guidance for all State of Hawai`i Bureau and Office PMOs and Project Offices. Leveraging economy of scale, this prevents each project from developing policies.

E.2 **Standards Identification, Development and Coordination:** Manage, develop and coordinate project management standards recognized by the Federal government and the State of Hawai`i.

Within the PMO, the Program Manager is responsible for understanding project management standards; and coordinates the appropriate translation of these directives into State of Hawai`i policies, directives, and guidance. This includes project management standards that include to Project Management Body of Knowledge (PMBOK). This function supports the PMO's oversight, training development, and training delivery responsibilities. This provides one set of directives, standards, and guidance for all State of Hawai`i Bureau and Office PMOs and Project Offices. If performed at the project level, this would create inconsistent practices and reporting of planning and performance.

E.3 **Oversight: Policy and Standards Accountability:** Manage and coordinate State of Hawai`i project oversight activities to assure adherence to policy and standards; monitor and track performance.

The PMO is responsible for evaluating project planning quality and due diligence; and provide continuous monitoring and tracking of project performance. At the project planning stage, this includes managing and coordinating of the independent IBR. At the completion of execution/development, this includes the post implementation review (PIR). Throughout the project this includes performance reporting to the State of Hawai`i's portfolio management and governance structures. This function supports the policy and standards adherence responsibilities regarding human resources, practice standards, and professional tools. This provides consistent and standardized project oversight that meets State of Hawai`i requirements.

E.4 **Central Tools Management:** Manage and coordinate State of Hawai`i enterprise project management tools.

The PMO is responsible for planning and managing common enterprise tools needed by all project offices. The managing of and training for one PMIS provides a cost effective shared resource that supports a statewide portfolio repository. Central tools management function/service strategy includes the PMIS, cost estimating tools, and team assessment tools. It will manage and coordinate the collection of project performance information and project artifacts. This function supports the PMO's central PM repository management responsibility. Leveraging economy of scale, this provides central tool management for project planning, monitoring, and tracking and accounting. This is prohibitively expensive for many projects to set up and manage.

E.5 **Central PM Repository Management:** Manage and coordinate the collection of project performance information and project artifacts.

By managing and coordinating the collection of project performance information and artifacts, the PMO is responsible to support the reporting the State of Hawai`i's portfolio performance, maintaining project records for agency accountability, and lessons learned. This includes periodic EVM information reporting, risk management, estimating and other planning artifact management responsibilities. This function supports the PMO's oversight and lessons learned responsibilities required by an IBR. Leveraging economy of scale, this provides artifact management used for project accountability and lessons learned. This would be prohibitively expensive for all projects to set up and manage.

E.6 **Portfolio Project Management (PfM):** Manage and coordinate the inter-project management and coordination.

The PMO's portfolio project management performs very important project initiation and inter-project coordination services with a line of business (LOB), including:

- Project initiation phase analysis and support
- Project charting assistance
- Project and inter-project portfolio resource planning
- Acquisition planning and strategy development
- Project and inter-project portfolio execution tracking and oversight
- Portfolio PM repository coordination

This function supports the PMO's project oversight, repository management responsibilities, HR assessment and development functions, performs inter-project coordination and dependency identification, and critical project initiation activities. Not performed at the project level, PPM provides the important project initiation and inter-project coordination within a LOB

E.7 **Human and Team Resource Assessment:** Manage and coordinate the project manager competency and team maturity assessment process.

The PMO performs the capability assessment of practitioners and project team required by best practices. This function supports the PMO's project support, training planning, and training delivery responsibilities. Not consistently performed at the project level, the practitioner and team assessment are better managed and more cost effectively performed at the enterprise level.

E.8 **Training and Education – Planning, Design, and Development:** Manage and coordinate the development of the competency delivery process for practitioners and teams.

The PMO performs planning and design requirements of curriculum to be delivered based on competencies required by best practice standards. This function supports the PMO's project support and training delivery coordination responsibilities. Leveraging economy of scale, this provides standardized and consistent quality training and education planning; design and development that are not performed at the project level.

E.9 **Training and Education – Delivery and Delivery Coordination:** Manage and coordinate the training and education delivery process for practitioners and teams.

The PMO coordinates the curriculum delivery of PM competencies required by best practice standards. Currently, the PMO co-manages the delivery via outsourced contract administration. This function supports the PMO's project support and leverages economy of scale, providing standardized and consistent quality training and education delivery that is not performed at the project level.

E.10 **Project Support - Guidance and Just-in-time/Just-as-needed Assistance:** Provides special skillsets that projects require for successful performance.

The PMO must provide and coordinate just-in-time and just-as-needed special skillsets for projects such as cost and schedule estimating, EVM assistance, and risk management expertise. This function supports resource-sharing coordination. Leveraging economy of scale, this provides standardized and consistent quality and a high level of planning due diligence expertise that is needed for short periods and not cost effectively developed at the project level.

E.11 **Resource Sharing Coordination:** Working with projects, helps projects plan and balance resources. It maximizes all of the organizations' usage of resources.

For mature organizations, the PMO coordinates the movement of project managers and other specialty resources to maximize the whole organization's resource demands. This function supports project support activities, helps the training and education functions, and assists the PPM function. This function is level 4-5 of the CMM maturity levels. This is the PM function that has great value to the organization by increasing performance and reducing costs.

APPENDIX E: ADDITIONAL INFORMATION

APPENDIX E: ADDITIONAL INFORMATION

Project Management Planning Standard: The PMO-developed project management planning standard provides better guidance to projects teams and prepares them for the required IBR. The Project Management Integrated Planning Standard is explicit guidance for developing a realistic, quality, mature project plan. The planning standard includes: 1) artifact standards (addressing what's in the plan), 2) artifact quality standards, and 3) the planning process standards. The Project Management Planning Standard is the basis for State of Hawai`i's IBR Program, IBR Services, the PMPS, and the OIMT Project Management Professional Development curriculum.

Integrated Life Cycle (ILC) Framework: The Integrated Life Cycle Standards describe the State of Hawai`i's required life cycle processes, their artifacts, and when and how decisions are to be made (governance). The State of Hawai`i's ILC standard components address the three phases of DME planning and development and the operation and maintenance (O&M) steady state. The three phases apply to all of the information management (IM) disciplines including CIPC, Project Management, Records Management, and Privacy.

Project Management Services: The PMO has set up two contract vehicles to assist projects, the PMPS and IBR Services. These contract services are complimentary to the PMO's responsibilities and goals of providing projects guidance, oversight, and assistance.

Project Management (PM) Curriculum Enhancement and Alignment: The PMO enhanced and aligned State of Hawai`i's PM curriculum. The enhancements incorporated State of Hawai`i's Project Management Planning Standard and the ILC guidance into the PM curriculum. The enhanced curriculum offers a more relevant course design, providing students with clear connection between best practice techniques to State of Hawai`i's project planning standards and policy. The restructured curriculum will offer a combination of required project management courses and courses for both Program and Project Managers.

Program Management Office (PMO) Operations: Within the boundaries of resources, the PMO has actively worked with State of Hawai`i's IT projects to facilitate their success, meeting State of Hawai`i's business goals. Existing and new projects have benefited via the PMO's guidance, assistance, and consultation. Many of these projects had significant issues, being considered for discontinuance (red-lining). The PMO provided appropriate consultation and just-in-time support to these projects, correcting issues and turning projects from distress into successes.

IT HUMAN CAPITAL MANAGEMENT STRATEGIC PLAN

TABLE OF CONTENTS

1.0 EXECUTIVE SUMMARY....4

1.1 Background – The Value Chain and Value Proposition....5

1.2 A Clear Case for Change and Transformation....6

1.3 New Day Vision: New Hope – New Ideas – New Way of Doing Business and IT....6

2.0 INTRODUCTION....7

2.1 Purpose....8

2.2 Scope....8

2.3 Document Overview....8

2.4 Associated Documents....8

3.0 BACKGROUND....9

3.1 Current As-Is Environment....10

3.2 Strategy for Implementing the Vision (Best Practices and Industry Standards)....10

3.2.1 CIO Leadership Strategy....10

3.2.2 Implementation Strategy....11

3.2.3 IT/IRM and Business Transformation Strategy....12

4.0 PROPOSED FUTURE INFORMATION TECHNOLOGY ORGANIZATION....13

4.1 Mission and Vision of the Department of Information Technology (DoIT)....14

4.2 Guiding Principles....14

4.3 Roadmap to Consolidation....14

5.0 ORGANIZATIONAL OVERVIEW....16

5.1 Functional Design....17

5.2 Roles, Responsibility, Accountability, and Authority....21

5.2.1 DoIT Checks and Balances....21

6.0 ORGANIZATIONAL CHANGE MANAGEMENT....23

6.1 Overcoming Challenges with Active Change Management....24

6.1.1 Organizational Change Management....25

7.0 HUMAN RESOURCE CONSIDERATIONS....31

7.1 Reclassification Considerations....32

7.1.1 Why This Effort is Different....32

7.1.2 Current Reclassification Strategy Definition....32

7.1.3 Challenges/Problems....33

7.1.4 Recommendations....33

7.1.5 Benefits....33

7.2 Recruitment Strategy....33
7.2.1 Approach....33
7.2.2 Recruitment Plan Strategies....34
7.2.3 Establish a Recruiting Culture....34
7.3 Professional Development....35
7.3.1 Overview and Approach....35
7.3.2 Training Plan Strategies:....35
7.3.3 Training Needs Analysis....36

8.0 IMPLEMENTATION STRATEGY....37
8.1 Immediate Strategies and Timeframes (The First Six Months)....38
8.2 Short-term Strategies and Timeframes (Six Months–One Year)....38
8.3 Medium-term Strategies and Timeframes (Two-Three Years)....39
8.4 Long-term Strategies and Timeframes (Three-Five Years)....40

9.0 FUNDING CONSIDERATIONS....41

10.0 CONCLUSION....41

LIST OF FIGURES

Figure 1: Hawai'i's Lines of Business....5
Figure 2: Performance Improvement Life Cycle....11
Figure 3: IT/IRM and Business Transformation Strategy....12
Figure 4: Roadmap to Consolidation (Three Phases)....14
Figure 5: Timeframe for Consolidation and Centralization Steps....15
Figure 6: State of Hawai'i IT Reorganization Functional Design and Technology Life Cycle....17
Figure 7: DoIT Structure....21
Figure 8: Active Change Management....24
Figure 9: The Cycle of Change....25
Figure 10: Eight Stages of Change Management....26
Figure 11: Implementation Strategies and Timeframes....38

1.0 EXECUTIVE SUMMARY

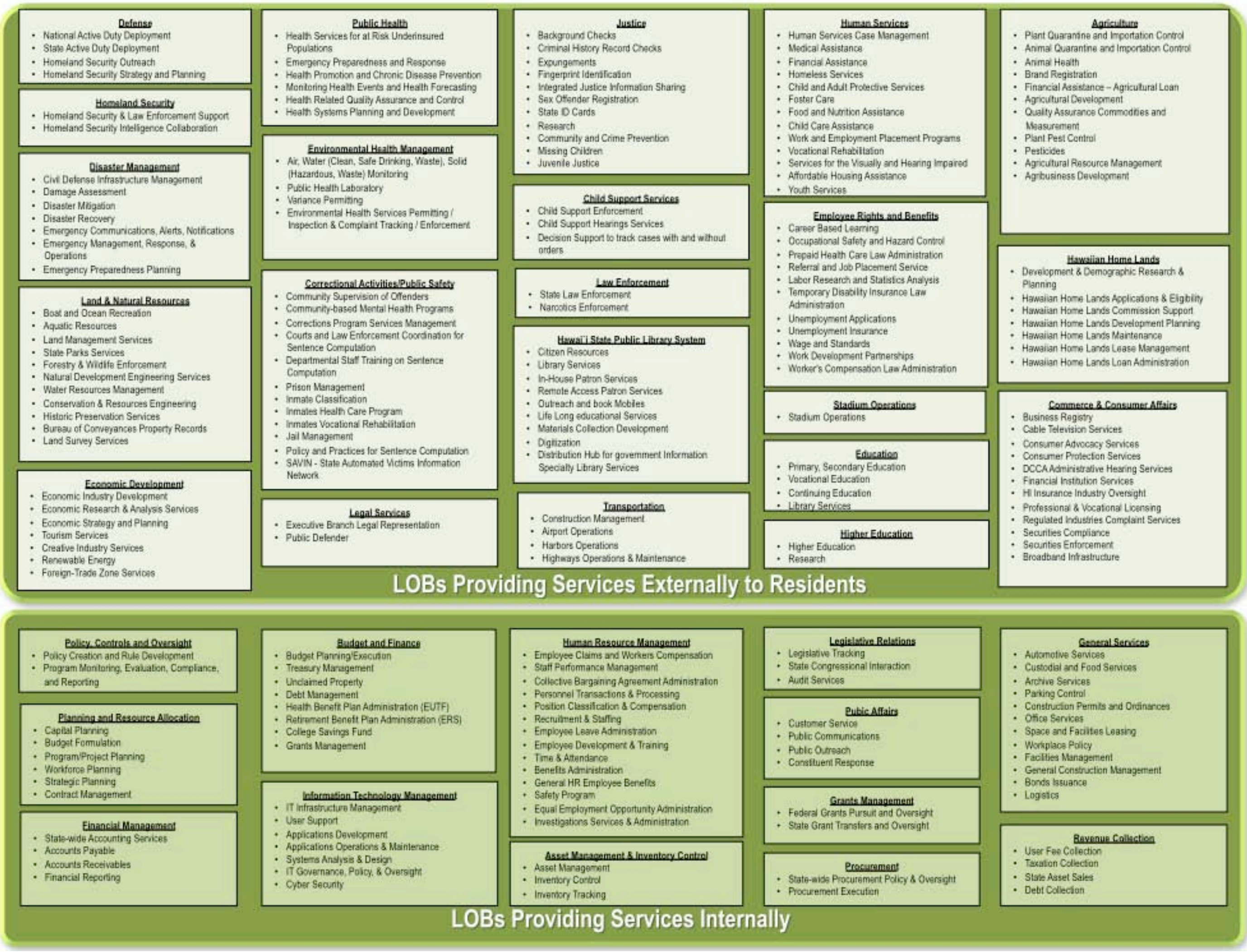
1.0 EXECUTIVE SUMMARY

1.1 BACKGROUND – THE VALUE CHAIN AND VALUE PROPOSITION

The business and Information Technology (IT) environment provides context for the size, scope, and complexity of the transformation challenges and opportunities for the State of Hawai'i. The Executive branch of Government of the State of Hawai'i is a large $11 billion dollar business enterprise with 18 departments and 41,000 employees serving 1.4 million residents/citizens with 204 services across 34 lines of business (LOBs). The concomitant IT organization is a $157 million dollar (1.5%) enterprise with no central IT Department and 746 IT staff fragmented across 18 organizations that support over 700 legacy systems and applications and one LOB (six functions). Not surprisingly, Hawai'i is mired in ineffective and inefficient paper-based, manual business processes with old technology that does not promote interoperability, reliability, security, privacy, and maintainability. Therefore, Hawai'i is not positioned to capitalize on the promise of the 21st century's information age.

> **"Information technology can expect to improve business processes about 10%. However, redesigning a process and then adding technology can improve the process up to 90%."**
>
> – Bill Gates, *Business @ the Speed of Thought, 1999*

The State of Hawai'i's Value Chain, shown in Figure 1 below, provides the State with an actionable framework for redefining the IT organization. There are 204 services/business functions across 34 LOBs in the portfolio that meet the State's goals. These outputs provide the real value to the organization. The value chain helps to identify opportunities for streamlining business processes, integrating technology, and realizing cost savings. The value proposition is simple: standardize the common shared services that can be used by all, and then optimize the mission-unique functions to serve citizens more effectively and efficiently.



Defense
- National Active Duty Deployment
- State Active Duty Deployment
- Homeland Security Outreach
- Homeland Security Strategy and Planning

Homeland Security
- Homeland Security & Law Enforcement Support
- Homeland Security Intelligence Collaboration

Disaster Management
- Civil Defense Infrastructure Management
- Damage Assessment
- Disaster Mitigation
- Disaster Recovery
- Emergency Communications, Alerts, Notifications
- Emergency Management, Response, & Operations
- Emergency Preparedness Planning

Land & Natural Resources
- Boat and Ocean Recreation
- Aquatic Resources
- Land Management Services
- State Parks Services
- Forestry & Wildlife Enforcement
- Natural Development Engineering Services
- Water Resources Management
- Conservation & Resources Engineering
- Historic Preservation Services
- Bureau of Conveyances Property Records
- Land Survey Services

Economic Development
- Economic Industry Development
- Economic Research & Analysis Services
- Economic Strategy and Planning
- Tourism Services
- Creative Industry Services
- Renewable Energy
- Foreign-Trade Zone Services

Public Health
- Health Services for at Risk Underinsured Populations
- Emergency Preparedness and Response
- Health Promotion and Chronic Disease Prevention
- Monitoring Health Events and Health Forecasting
- Health Related Quality Assurance and Control
- Health Systems Planning and Development

Environmental Health Management
- Air, Water (Clean, Safe Drinking, Waste), Solid (Hazardous, Waste) Monitoring
- Public Health Laboratory
- Variance Permitting
- Environmental Health Services Permitting / Inspection & Complaint Tracking / Enforcement

Correctional Activities/Public Safety
- Community Supervision of Offenders
- Community-based Mental Health Programs
- Corrections Program Services Management
- Courts and Law Enforcement Coordination for Sentence Computation
- Departmental Staff Training on Sentence Computation
- Prison Management
- Inmate Classification
- Inmates Health Care Program
- Inmates Vocational Rehabilitation
- Jail Management
- Policy and Practices for Sentence Computation
- SAVIN - State Automated Victims Information Network

Legal Services
- Executive Branch Legal Representation
- Public Defender

Justice
- Background Checks
- Criminal History Record Checks
- Expungements
- Fingerprint Identification
- Integrated Justice Information Sharing
- Sex Offender Registration
- State ID Cards
- Research
- Community and Crime Prevention
- Missing Children
- Juvenile Justice

Child Support Services
- Child Support Enforcement
- Child Support Hearings Services
- Decision Support to track cases with and without orders

Law Enforcement
- State Law Enforcement
- Narcotics Enforcement

Hawai`i State Public Library System
- Citizen Resources
- Library Services
- In-House Patron Services
- Remote Access Patron Services
- Outreach and book Mobiles
- Life Long educational Services
- Materials Collection Development
- Digitization
- Distribution Hub for government Information Specialty Library Services

Transportation
- Construction Management
- Airport Operations
- Harbors Operations
- Highways Operations & Maintenance

Human Services
- Human Services Case Management
- Medical Assistance
- Financial Assistance
- Homeless Services
- Child and Adult Protective Services
- Foster Care
- Food and Nutrition Assistance
- Child Care Assistance
- Work and Employment Placement Programs
- Vocational Rehabilitation
- Services for the Visually and Hearing Impaired
- Affordable Housing Assistance
- Youth Services

Employee Rights and Benefits
- Career Based Learning
- Occupational Safety and Hazard Control
- Prepaid Health Care Law Administration
- Referral and Job Placement Service
- Labor Research and Statistics Analysis
- Temporary Disability Insurance Law Administration
- Unemployment Applications
- Unemployment Insurance
- Wage and Standards
- Work Development Partnerships
- Worker's Compensation Law Administration

Stadium Operations
- Stadium Operations

Education
- Primary, Secondary Education
- Vocational Education
- Continuing Education
- Library Services

Higher Education
- Higher Education
- Research

Agriculture
- Plant Quarantine and Importation Control
- Animal Quarantine and Importation Control
- Animal Health
- Brand Registration
- Financial Assistance – Agricultural Loan
- Agricultural Development
- Quality Assurance Commodities and Measurement
- Plant Pest Control
- Pesticides
- Agricultural Resource Management
- Agribusiness Development

Hawaiian Home Lands
- Development & Demographic Research & Planning
- Hawaiian Home Lands Applications & Eligibility
- Hawaiian Home Lands Commission Support
- Hawaiian Home Lands Development Planning
- Hawaiian Home Lands Maintenance
- Hawaiian Home Lands Lease Management
- Hawaiian Home Lands Loan Administration

Commerce & Consumer Affairs
- Business Registry
- Cable Television Services
- Consumer Advocacy Services
- Consumer Protection Services
- DCCA Administrative Hearing Services
- Financial Institution Services
- HI Insurance Industry Oversight
- Professional & Vocational Licensing
- Regulated Industries Complaint Services
- Securities Compliance
- Securities Enforcement
- Broadband Infrastructure

LOBs Providing Services Externally to Residents

Policy, Controls and Oversight
- Policy Creation and Rule Development
- Program Monitoring, Evaluation, Compliance, and Reporting

Planning and Resource Allocation
- Capital Planning
- Budget Formulation
- Program/Project Planning
- Workforce Planning
- Strategic Planning
- Contract Management

Financial Management
- State-wide Accounting Services
- Accounts Payable
- Accounts Receivables
- Financial Reporting

Budget and Finance
- Budget Planning/Execution
- Treasury Management
- Unclaimed Property
- Debt Management
- Health Benefit Plan Administration (EUTF)
- Retirement Benefit Plan Administration (ERS)
- College Savings Fund
- Grants Management

Information Technology Management
- IT Infrastructure Management
- User Support
- Applications Development
- Applications Operations & Maintenance
- Systems Analysis & Design
- IT Governance, Policy, & Oversight
- Cyber Security

Human Resource Management
- Employee Claims and Workers Compensation
- Staff Performance Management
- Collective Bargaining Agreement Administration
- Personnel Transactions & Processing
- Position Classification & Compensation
- Recruitment & Staffing
- Employee Leave Administration
- Employee Development & Training
- Time & Attendance
- Benefits Administration
- General HR Employee Benefits
- Safety Program
- Equal Employment Opportunity Administration
- Investigations Services & Administration

Asset Management & Inventory Control
- Asset Management
- Inventory Control
- Inventory Tracking

Legislative Relations
- Legislative Tracking
- State Congressional Interaction
- Audit Services

Pubic Affairs
- Customer Service
- Public Communications
- Public Outreach
- Constituent Response

Grants Management
- Federal Grants Pursuit and Oversight
- State Grant Transfers and Oversight

Procurement
- State-wide Procurement Policy & Oversight
- Procurement Execution

General Services
- Automotive Services
- Custodial and Food Services
- Archive Services
- Parking Control
- Construction Permits and Ordinances
- Office Services
- Space and Facilities Leasing
- Workplace Policy
- Facilities Management
- General Construction Management
- Bonds Issuance
- Logistics

Revenue Collection
- User Fee Collection
- Taxation Collection
- State Asset Sales
- Debt Collection

LOBs Providing Services Internally

Figure 1: Hawai'i's Lines of Business

1.2 A CLEAR CASE FOR CHANGE AND TRANSFORMATION

In September 2011, the state completed and released the first-ever comprehensive assessment of its IT assets, policies, and procedures in a baseline report. This was completed over a period of four months (after the new CIO was in place). To complete the report, over 200 individuals from 18 departments, offices, and attached agencies were interviewed, and more than 1,500 pages of notes and background material were cataloged. The baseline report identified 204 business functions and services delivered by State government employees in 18 departments and over 700 IT applications currently in use. The report identified widespread symptoms of Information Technology/Information Resource Management (IT/IRM) challenges including: inefficient manual interfaces; minimal enterprise integration and sharing; narrowly focused federally funded solutions; limited use of IT/IRM to enable mission service delivery; the condition of aging legacy systems (20+ years old); the proliferation of all types of IT/IRM products and services; and little business process coordination or information sharing across departments (and programs). The symptoms are driven by three root causes: 1) no coordinating authority for managing information resources and technology across the State; 2) lack of cross-cutting business process re-engineering (BPR); and 3) deep cuts in resources and budget reductions in the State over the past decade (up to 50%).

The 20 key recommendations and findings in the baseline report provided the basis for the priorities, architecture, and projects required for change. Four key themes emerged:

- Enterprise focus for projects
- Establish enterprise governance
- Re-engineer business processes
- Strengthen technical infrastructure

The need for change/transformation was echoed in reports by the auditor: *Audit of the State of Hawai'i's Information Technology: Who's in Charge?* (2009), *Report of the Task Force on Reinventing Government* (January 2010), State of Hawai'i Information Technology Transition Document (February 2011), and the *Baseline Assessment* (September 2011).

1.3 NEW DAY VISION: NEW HOPE – NEW IDEAS – NEW WAY OF DOING BUSINESS AND IT

The Governor has envisioned a new day in Hawai'i with a *New Day Plan* that is committed to three waves of change that comprise a winning strategy for Hawai'i: growing a sustainable economy, investing in people, and transforming government.

> **"Automating a mess yields an automated mess."**
>
> - *Reengineering the Corporation*
> by Michael Hammer & James Champy (1993)

There is also a new sense of urgency in Hawai'i—leapfrog to the front with a *Business and IT Transformation Plan* that seeks to reorganize government while striving for world-class excellence with Aloha. The plan is to do a comprehensive make-over of business and IT in several phases over several years.

This effort will:

- Operationalize the New Day Vision into an actionable, measurable plan
- Help State agencies publicize and manage key activities
- Demonstrate State agencies' responsiveness to State legislators and to the congressional delegation in Washington, D.C.
- Result in one cohesive statewide, long-range vision that drives the business and IT improvements
- Educate the public about State agency unity and progress in transforming government

2.0 INTRODUCTION

2.0 INTRODUCTION

2.1 PURPOSE

The *State of Hawai'i IT Human Capital Management Strategic Plan* establishes the guidelines and principles that will define the roadmap to establish a unified and progressive IT organization for the State of Hawai'i. The Plan defines the stages that will be taken to implement IT leadership and create and build on a foundation of strategic and thoughtful steps that combine the goals of government and the community. The Plan is not just about technology—the goals, objectives, and performance measures to be established will guide the use of information services in support of the State of Hawai'i's diverse missions and business objectives. This plan sets the strategy for implementing the vision and describes the recommended next phases to establish an information-enabled enterprise that benefits all the citizens, stakeholders, and employees of the State of Hawai'i.

The purpose of this plan is to present the future state of the State of Hawai'i's IT organization and how it can best leverage IT to assist agencies in the effective, efficient, and convenient delivery of programs and services to the residents and businesses of the State. As the implementation phases roll out, the Plan is expected to evolve and adjust based on discovery and through coordination with the other strategies such as the *Enterprise Architecture (EA) Sequencing Plan.*

2.2 SCOPE

The *State of Hawai'i IT Human Capital Management Strategic Plan* has been developed to ensure that the necessary information services are appropriately planned, invested in, and implemented based on a future information service environment that must be secure, well-managed, and delivered by a highly skilled and trained workforce.

To define this Plan, first the As-Is state of IT in the State of Hawai'i was examined. Before new technologies can be implemented, it makes sense to re-examine and analyze the processes in use. Some of these processes were developed before the current IT capabilities were available and before the State of Hawai'i experienced its current growth and diversification. Care will be taken throughout the system reorganization efforts to incorporate process improvements and assure that system support and development is done in a way that achieves efficiency and promotion of business goals. This transformation effort has a set of objectives and performance metrics that will be used to assess the success of the transformation and the continuity of the reorganization effort going forward: functional organization, human capital management, implementation strategy, and funding considerations.

2.3 DOCUMENT OVERVIEW

The *State of Hawai'i IT Human Capital Management Strategic Plan* describes the strategy, decisions, and executable roadmaps that will be addressed in the next phase of this initiative.

The first part of this document is a review of the current environment and the strategic goals to be used to define the new environment. Several phases will be implemented to build the foundation for the ultimate functional design and organizational structure that is described along with the checks and balances that will be put in place to ensure its integrity and efficiency.

The next part of the document covers human resource considerations, especially the highly researched and defined reclassification strategy. The reclassification plan is built on the past efforts of two initiatives to address IT in the State of Hawai'i. Those efforts also defined the importance of recruitment strategy. The results are also leveraged in addressing staff recruitment and professional development plans that will optimize the steps taken to develop a world-class IT department. All of these items, as well as business and EA strategies, are utilized in the definition of the timelines and considerations for implementation of the plan.

The intended audience for this document is not limited. It is the goal of those involved with the State of Hawai'i IT transformation initiative to be transparent and welcoming to all contributors and stakeholders.

2.4 ASSOCIATED DOCUMENTS

- *State of Hawai'i Business Transformation Strategy and IT/IRM Strategic Plan,* 2012
- *Baseline of Information Management and Technology and Comprehensive View of State Services* (referred to as the Final Report), prepared by SAIC
- *Federal Segment Architecture Methodology* (FSAM)

3.0 BACKGROUND

3.0 BACKGROUND

3.1 CURRENT AS-IS ENVIRONMENT

The current IT environment is characterized by widely distributed and duplicated resources, non-integrated systems, non-standardized enterprise systems (e.g., email, purchasing, etc.), and the lack of vision and leadership. There are 18 compartmentalized departments with siloed IT efforts and limited centralized IT functions. Fundamental objectives and service levels are undefined. Talented resources are hard to obtain and retain. As a result, costs, efficiencies, and internal and external customer service have suffered.

The 2009 Audit Report describes the State's IT environment in these terms:

- No clearly defined roles, duties, and responsibilities for IT leadership
- A focus that is more operational rather than strategic
- Concentrates on the maintenance of the State's data center and computer networking, leaving departments without guidance and direction
- Does not maintain up-to-date technology standards
- Does not enforce and monitor compliance with technology standards
- Has not addressed nor provided guidance for critical processes such as disaster recovery
- Does not offer relevant services and support to effectively assist departments in carrying out their missions
- Does not ensure that IT investments are cost effective, optimally utilized, adequately planned for future growth, or have the operational flexibility to easily adapt to changing requirements

3.2 STRATEGY FOR IMPLEMENTING THE VISION (BEST PRACTICES AND INDUSTRY STANDARDS)

It was agreed that a strategy and implementation plan would be created utilizing best practices and industry standards. CIOs from other states who executed similar consolidation efforts were contacted for their recommendations and guiding principle solutions.

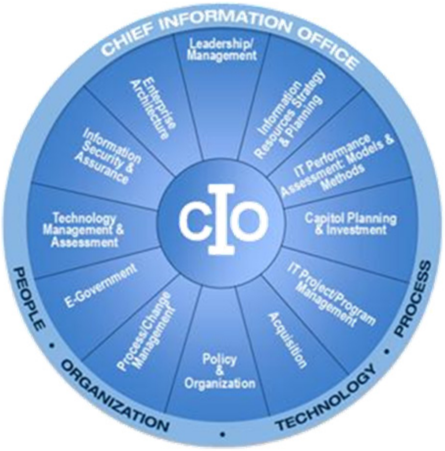
Key concepts identified to guide the initiative included the following:

- CIO leadership strategy
- Implementation strategy
- IT/IRM and business transformation strategy

3.2.1 CIO LEADERSHIP STRATEGY

The CIO will provide IT/IRM leadership through the following priorities:

- Develop, implement, and manage IT/IRM governance.
- Establish and enforce policies and standards.
- Create architectural requirements.
- Provide statewide IT/IRM investment oversight.


CHIEF INFORMATION OFFICE
Leadership/ Management
Information Resources Strategy & Planning
IT Performance Assessment: Models & Methods
Capitol Planning & Investment
IT Project/Program Management
Acquisition
Policy & Organization
Process/Change Management
E-Government
Technology Management & Assessment
Information Security & Assurance
Enterprise Architecture
CIO
PEOPLE • ORGANIZATION • TECHNOLOGY • PROCESS

3.2.2 IMPLEMENTATION STRATEGY

The initiative will follow a widely accepted and proven Performance Improvement Life Cycle (Figure 2) that the U.S. Federal Government Office of Management and Budget (OMB) utilizes to allow Federal agencies to assess, report, and advance their enterprise architecture activity and maturity. While originally identified for EA management, the ideals and approach of this process have been adopted and incorporated into every aspect of technology and functionality as a best practice for assessing, designing, and implementing change.

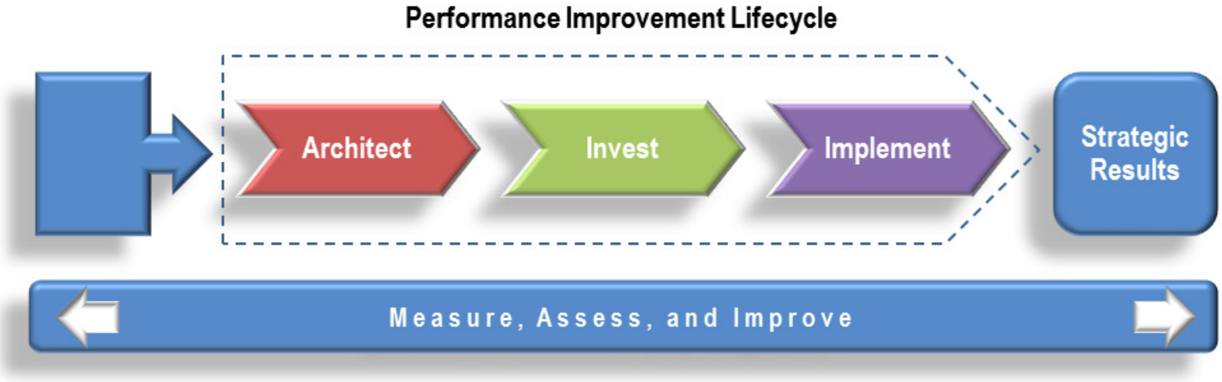

Performance Improvement Lifecycle
Architect
Invest
Implement
Strategic Results
Measure, Assess, and Improve

Figure 2: Performance Improvement Life Cycle

Each phase of the life cycle is comprised of integrated processes that, together, transform the defined top-down strategic goals and bottom-up system needs into a logical series of work products designed to achieve strategic results. The Performance Improvement Life Cycle is proven to provide the foundation for sound information and IT management practices, end-to-end governance of IT investments, and alignment of IT investments with an agency's strategic goals.

Phase	Description
Architect	Define current (baseline) and future (target) states, and plan to transition from the current to the future state, with a focus on strategy, performance improvements and IT investments.
Invest	Performance improvement opportunities identified during the Architect process are addressed through portfolio investment and tactical solutions. This step defines the implementation and funding strategy for individual initiatives that are part of the overall Plan.
Implement	Projects are executed and tracked throughout the system development life cycle (SDLC). Achievement of the program/ project plan within acceptable variance for schedule and budget is measured and reported through Earned Value Management (EVM) process. Performance is measured to determine how well the implemented solutions achieve the desired outputs and mission outcomes, and provide feedback to all invested parties.

3.2.3 IT/IRM AND BUSINESS TRANSFORMATION STRATEGY

The strategy for improving and transforming IT/IRM for the State of Hawai'i will focus on business transformation while incorporating the guiding principles surrounding human resource capital management. Business Transformation is a change management strategy that aligns three separate initiatives: people, process, and technology.

Figure 3 identifies how these initiatives are brought together in the process. CIOs build effective IT/IRM through transforming resources and management practices.

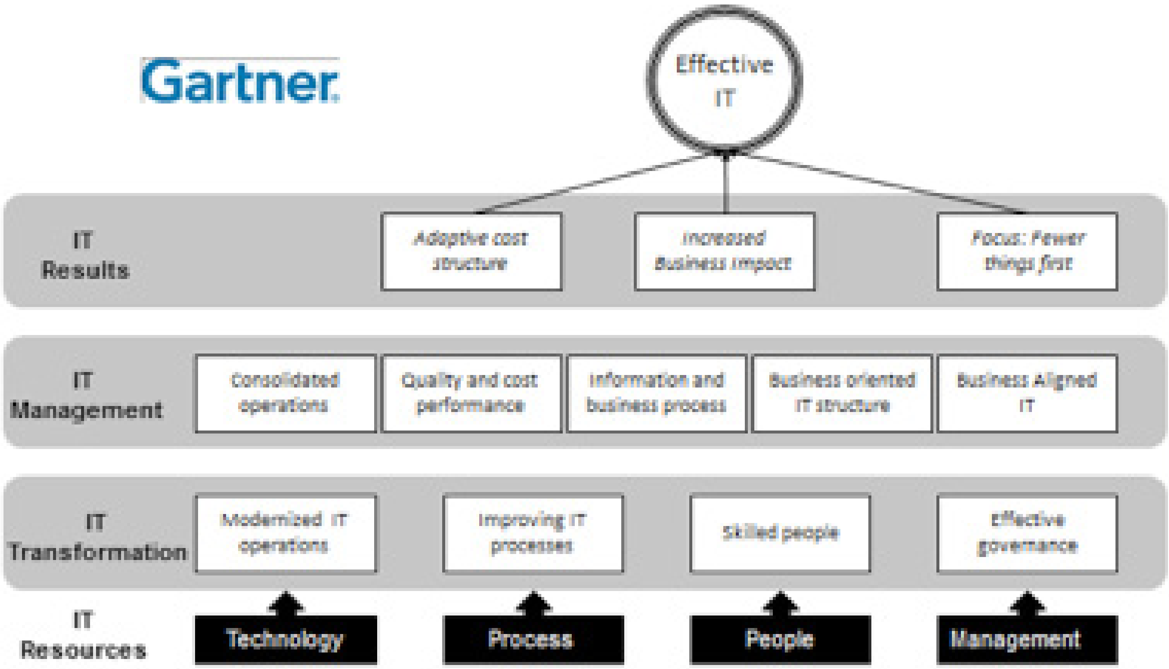
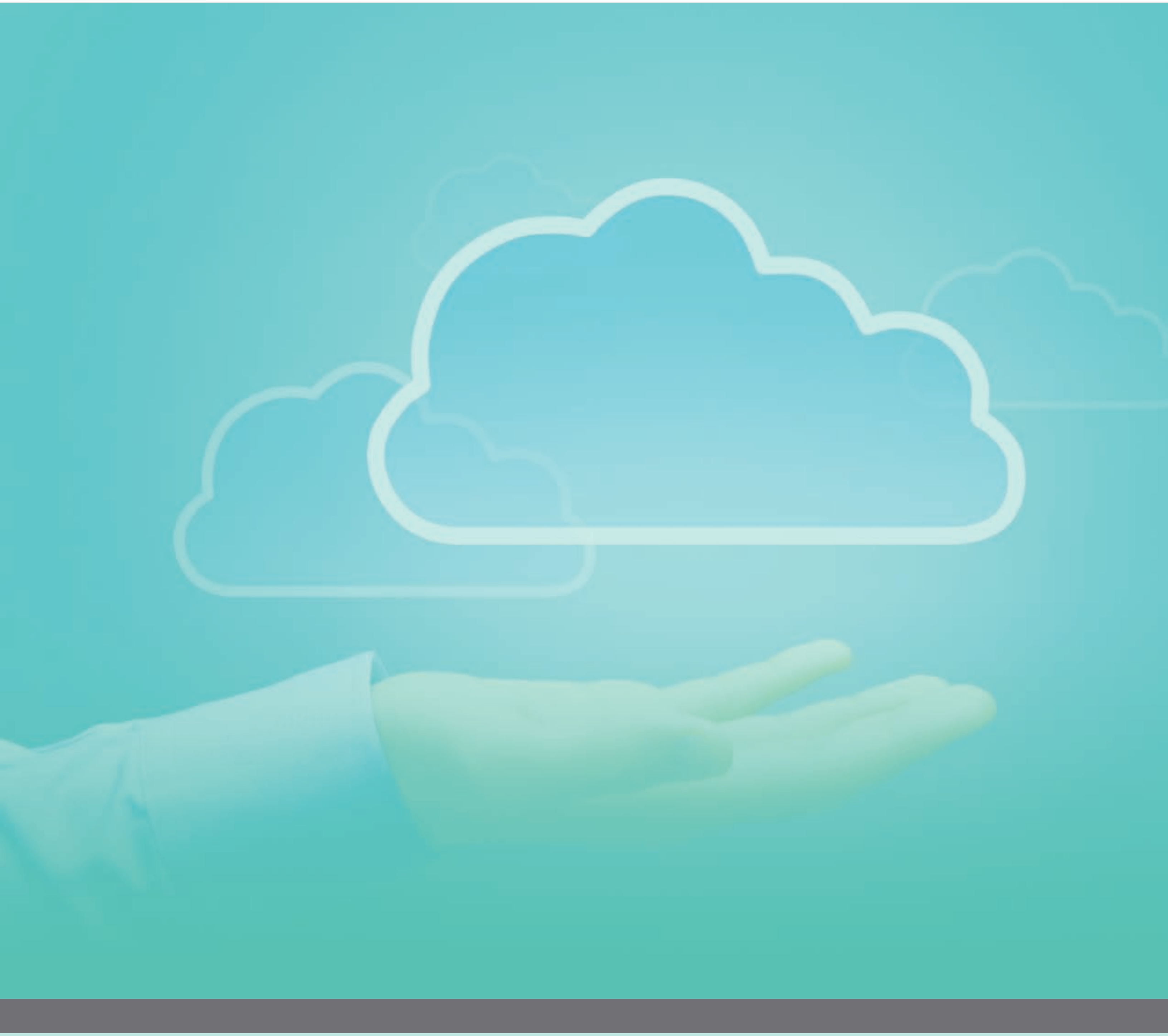


Figure 3 – Business and IT/IRM Transformation Strategy



4.0

PROPOSED FUTURE INFORMATION TECHNOLOGY ORGANIZATION

4.0 PROPOSED FUTURE INFORMATION TECHNOLOGY ORGANIZATION

A new, consolidated IT organization will be designed to address the current technology management challenges faced by the State of Hawaiʻi by:

- Centralizing maintenance of the State's data center and computer networking incorporating LOB applications
- Defining and maintaining up-to-date technology standards
- Enforcing and monitoring compliance with technology standards
- Establishing and providing guidance for critical processes such as data backups and disaster recovery
- Offering relevant services and the creation of enterprise solutions necessary to support and effectively assist departments in carrying out their missions
- Establishing a customer service environment and technological expertise that instills department managers' confidence in the Department of IT's (DoIT's) ability to provide support for their applications
- Ensuring that IT investments are cost effective, optimally utilized, adequately planned for future growth, and have the operational flexibility to easily adapt to changing requirements

4.1 MISSION AND VISION OF THE DEPARTMENT OF INFORMATION TECHNOLOGY (DOIT)

The DoIT mission: To assist agencies in the effective, efficient, and convenient delivery of programs and services to the public through business transformation and IT modernization.

The DoIT vision is a State where:

- The public engages with an open and transparent government.
- State employees, citizens, and businesses have convenient and secure access to reliable information.
- Government processes are streamlined, integrated, and implemented to meet the public's service expectations.
- IT and information capabilities align and support business needs, strategies, and outcomes.
- Innovation and continuous improvement are fostered.

4.2 GUIDING PRINCIPLES

The initiative's guiding principles are clear and well defined:

- People first – *Kuleana:*
  - Each job and role is valued.
  - Everyone is accountable; everyone is responsible.
  - Change management will be essential.
- Collaborative, open, and transparent – *Laulima:*
  - Teamwork is achieved across all levels of staff among departments and between branches of government.
  - Central oversight is accomplished with local presence and agility.
- Effective and efficient – *Kūlia i ka Nuʻu* (strive for the summit):
  - The organization is built to last and adaptive to change.
  - Best practice frameworks are followed.
  - There is a phased implementation approach.

4.3 ROADMAP TO CONSOLIDATION

The remainder of this document lays out the strategies and implementation timeline for instituting a new, consolidated IT organization. A high-level view of the strategic roadmap is described in this section. Several phases will create the progression and interim structure that are the necessary foundation for building the new, unified organization. Definition of these phases includes the thoughtful consideration of impact on stakeholders and identification of realistic task durations. The ability to correctly identify all affected personnel and organizations was key to defining the appropriate timeline. The goal is an effective implementation without a negative interruption to people, processes, and technology. A three-phased approach was designed (see Figure 4 below).

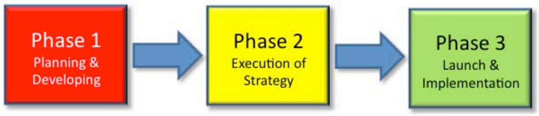


Figure 4 – Roadmap to Consolidation (Three Phases)

Phase 1—Planning and Developing; setting the groundwork:

- Assembling a key team of IT resources
- Identifying requirements
- Planning and strategizing courses of action
- Defining the technology framework
- Verifying strategies
- Obtaining approvals and sign-offs

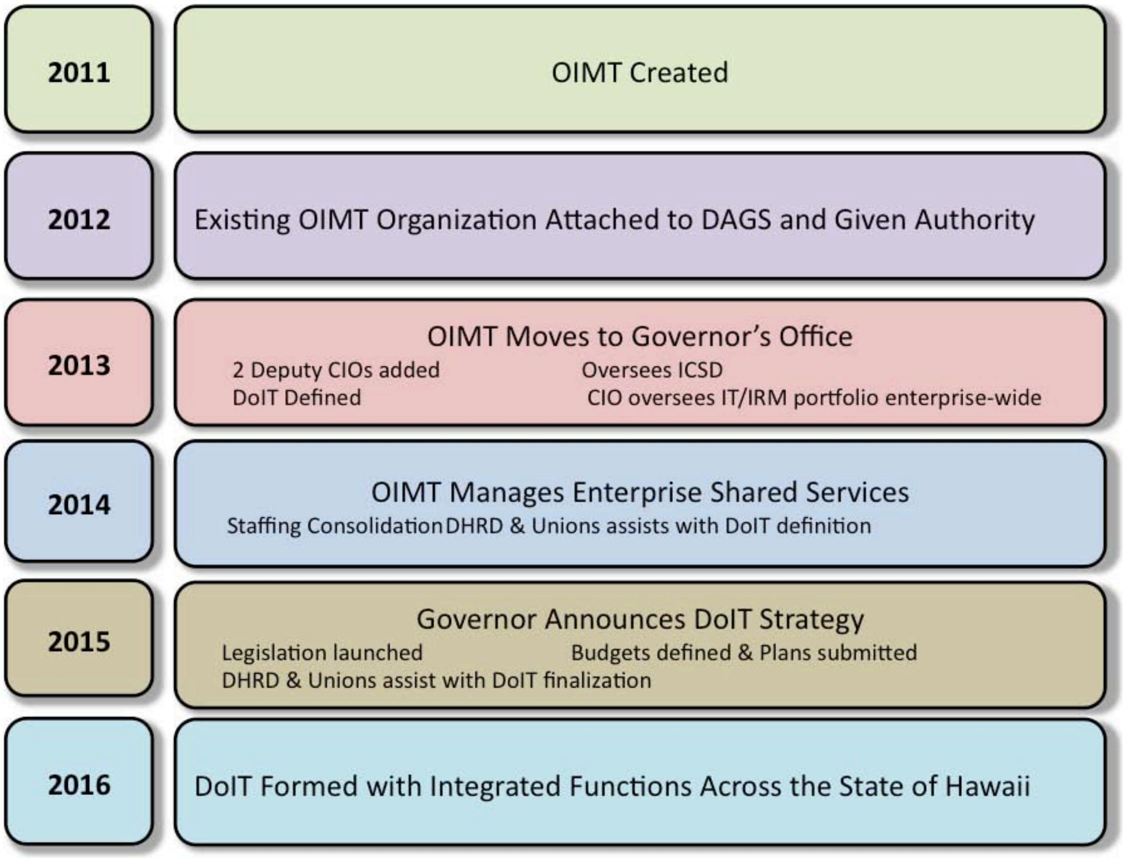
Phase 2—Execution of Strategy; laying the foundation:

- Key positions filled
- Unification of efforts for existing and new IT resources
- Efforts cornerstoned and staged from ICSD
- Required legislation launched
- Teams assembled to work on key initiatives with the Department of Human Resources Development (DHRD), DNF, and the unions
- Funding procured
- Budget established
- Technology framework launched
- Program Management established
- Customer service structure in place
- Staffing finalized
- Detailed close-out steps and processes identified and are as complete as possible

Phase 3—Launch and Implementation; finalizing the structure:

- Approval of legislation
- Completion of close-out steps and processes
- Establishment of new, consolidated DoIT

These phases and their schedule have been defined to create the most effective path toward establishing a consolidated, progressive IT Department, the State of Hawai'i DoIT. The complete journey of the initiative and the timeframes of the key steps that have, and will, be taken are shown in Figure 5 below.



2011 OIMT Created

2012 Existing OIMT Organization Attached to DAGS and Given Authority

2013 OIMT Moves to Governor's Office
2 Deputy CIOs added
DoIT Defined
Oversees ICSD
CIO oversees IT/IRM portfolio enterprise-wide

2014 OIMT Manages Enterprise Shared Services
Staffing Consolidation DHRD & Unions assists with DoIT definition

2015 Governor Announces DoIT Strategy
Legislation launched
Budgets defined & Plans submitted
DHRD & Unions assist with DoIT finalization

2016 DoIT Formed with Integrated Functions Across the State of Hawaii

Figure 5: Timeframe for Consolidation and Centralization Steps

The details for execution of this vision of consolidated IT and centralized IRM are described on the following pages.

5.0 ORGANIZATIONAL OVERVIEW

5.0 ORGANIZATIONAL OVERVIEW

In this section, the organizational approach and strategy for defining the new DoIT organization is established. Two key areas are addressed:

- Functional design
- Roles, responsibility, accountability, and authority

This overview will be the blueprint for the next phases of this initiative, and the best roll-out methods for achieving the guiding principles surrounding human resource capital management will be used to direct the details of the implementation. The organizational design must align with the three interconnected and focused goals: people, process, and technology.

5.1 FUNCTIONAL DESIGN

The first building block of the IT Human Capital Management Strategic Plan is to establish the functional design that would best meet the culture, environment, and goals of the State. The consolidation of IT departments of several states were referenced and analyzed in order to follow best practices and incorporate lessons learned. Several models were proposed and modified in the course of this exercise, always keeping the guiding principles in mind during the decision process. The results of these deliberations are illustrated in Figure 6.

DEPARTMENT OF INFORMATION TECHNOLOGY (DoIT)

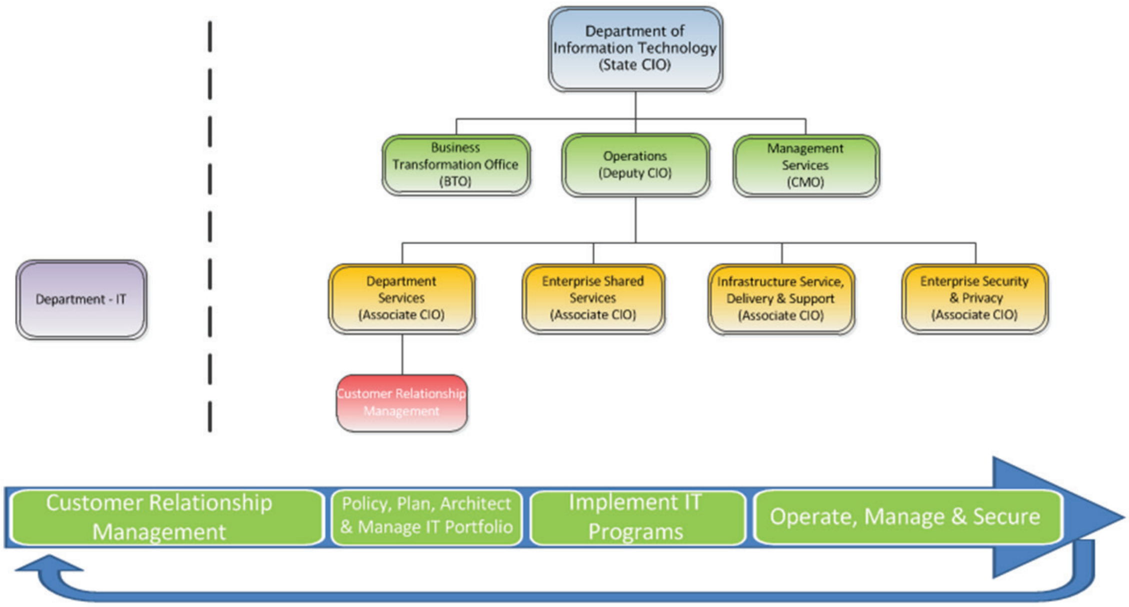

Department of Information Technology (State CIO)
Business Transformation Office (BTO)
Operations (Deputy CIO)
Management Services (CMO)
Department - IT
Department Services (Associate CIO)
Enterprise Shared Services (Associate CIO)
Infrastructure Service, Delivery & Support (Associate CIO)
Enterprise Security & Privacy (Associate CIO)
Customer Relationship Management
Customer Relationship Management
Policy, Plan, Architect & Manage IT Portfolio
Implement IT Programs
Operate, Manage & Secure

Figure 6: State of Hawai'i IT Reorganization Functional Design and Technology Life Cycle

The functional design was created based on the Life Cycle Development Phases; it also emphasizes customer service. The philosophy of support and delivery resulted in maintaining LOB IT resources within the departments, but designing a customer relationship function with the IT Department to support the departmental resources in their daily responsibilities and support the departments in their overall IT requirements and enterprise system needs.

Three key leadership areas within the new department address:

- Business transformation
- Operations
- Management services

Department/Office	Description
Department IT	• Supports and develops mission-unique applications will remain within the departments. • Includes planning, life cycle strategies, business analysis, documentation, training responsibilities, and any other unique technical support that may be required
Department of Information Technology (State CIO)	The DoIT, led by the CIO, is responsible for overseeing the IT/IRM plans that will govern IT for the State of Hawaiʻi. The CIO will oversee information technology governance via the Executive Leadership Council, CIO Council, and the IT Steering Committee.
Business Transformation Office (BTO)	The BTO, led by the Business Transformation Officer, will lead and advance departments in business operations and technological processes. Business and Process Analysis: The mapping and analysis of existing business processes to identify opportunities for improvement either through functional reengineering, application of automated tools, or software solutions.
Enterprise Architecture (EA)	• Develop and maintain an EA roadmap for the State of Hawaiʻi. • Develop and implement processes to review and ensure that projects and initiatives are aligned to and comply with the enterprise architecture requirements. Open Data Standards: The support and facilitation of the interoperability and data exchange among different software, products and services. Systems Integration: Develop, implement, and support the software that is used to connect and enable communication between software systems and components.
Enterprise Program Management Office (PMO)	Design, implement, and measure performance of Program Management Methodology, Tools and Reporting. IT Policy, Procedures, and Standards: Define and implement the rules and framework to be followed enterprise-wide (COBIT, ITIL, SDLC, and PMP). IT Performance Management Framework: Design, implement and publish performance reporting (Dashboards and Metrics)
Program Management Office (PMO)	• Develop and implement Project Management processes and manage compliance to them • Monitor the project portfolio to maximize performance and track interdependencies (Development, Modernization, and Enhancement Projects [DME]) Business Process Improvement: The mapping and analysis of existing business processes to identify opportunities for improvement either through functional reengineering, application of automated tools, or software solutions.
Portfolio Management	This group will be responsible for: • IT budget and capital planning • IT procurement/acquisitions services • IT asset management • IT/IRM tactical planning • Call for IT/IRM projects (project implementation selection) • EA planning and execution

Department/Office	Description
Management Services (CMO)	The Management Services Office, led by the Chief Management Officer, will establish, monitor, and enforce guidelines for compliance, change management, business services, budget, and acquisitions. This office is also responsible for management of communications, IT personnel, and DoIT administration.
Compliance Management	The definition, implementation, and enforcement of processes to ensure compliance to established operational guidelines, requirements and/or legislative stipulations.
Organizational Change Management	• Defines and executes change control processes to govern projects, initiatives, and implementations for the purpose of change management, effective change roll out, and to minimize disruption to IT services or business processes • Processes define the identification of change factors, analysis, prioritization, authorization, implementation plan design, risk identification, testing, documentation, and roll out—all in a managed and structured delivery
Business Services Office	Responsible for DoIT's fiscal and budget management, DoIT acquisition; and Business Continuity (development and implementation of processes to protect the IT environment, ensure delivery of established IT service level agreements, and protect business continuity).
Personnel and Administration	• Execute departmental administration responsibilities • Develop and implement personnel/IT training (user, applications, IT, professional development)
Communications/ Legislative Relations	Responsible for legislative relations, communications and outreach, public information/Freedom of Information Act (FOIA), and grant writing.
Operations (Deputy CIO)	The Operations Office, led by the Deputy CIO, will be responsible for the development, implementation and management of the operational areas in the IT Department. These include: • Department Services • Enterprise Shared Services • Infrastructure Service, Delivery, and Support • Enterprise Security and Privacy
Department Services (Associate CIO)	The Department Services Office, led by an Associate CIO, will manage the IT relationship with all of the State's departments. The office is also responsible for the overall management of the DoIT portfolio.
Customer Relationship Management	The DoIT's LOB representatives will be designated to support the departments' IT and enterprise application requirements and needs. They will work to define the customer view and identify what IT can do to meet and improve business performance. Service Level Agreements (SLAs) will be established, monitored, and managed to assure customer satisfaction. DoIT LOB representatives will share information and communicate to ensure that cross-jurisdictional requirements between departments' LOBs are communicated and addressed appropriately.

Department/Office	Description
Enterprise Shared Services (Associate CIO)	The Enterprise Shared Services Office, led by an Associate CIO, will manage enterprise applications and the development and implementation of applications for the rest of the State's departments.
Enterprise Applications	• Research, development, testing, implementation, evaluation, and management of enterprise applications (e.g., ERP, geographic information system [GIS], Collaboration, and others) and the solutions resulting from management of the Technology Refresh Plan (e.g., upgrades, migrations, new technology) • Electronic records management and execution of business intelligence and analytics
Departmental Application Support	Department application development and implementation.
Infrastructure Service, Delivery and Support (Associate CIO)	The Infrastructure Service, Delivery and Support Office, led by an Associate CIO, will manage and support the technologies of the State of Hawai'i.
Server and System Management	Storage Management, System Administration, Database Administration, Departmental Application Support, Enterprise Application Support
End User Computing Management	Support of laptops, desktops, mobile and smart phones.
Data Center Management	Facilities Management, data backups, and disaster recovery
Service Management	Service/Help Desk, user administration, network operations center
Telecommunications Management	Networking (e.g., telecommunications, ISP, TIC), voice and video, land mobile radio, wireless
Enterprise Security and Privacy (Associate CIO)	The Enterprise Security and Privacy Office, led by the Associate CIO, will define, develop, implement, manage, and monitor the policies and procedures surrounding technological security for the State of Hawai'i, as well as establish, monitor, and enforce guidelines.
Security Operations	Security policy and procedures, security standards, infrastructure security, applications security, security compliance
Cyber Security Controls	e-Discovery (electronic format information requested for litigation), continuous monitoring, cyber security operations center, information assurance (security and accessibility)
Identity and Access Management	Develop, implement, and enforce identity and credential access management following industry best practices.

5.2 ROLES, RESPONSIBILITY, ACCOUNTABILITY, AND AUTHORITY

5.2.1 DOIT CHECKS AND BALANCES

Checks and balances must be considered in any organizational design, but this is even more important for the DoIT. DoIT is responsible for the health and advancement of the data, key business systems, and support technology that are required to keep the State of Hawai'i departments running and progressing. A description of the governance and structure that will be put in place is described below and illustrated in Figure 7.

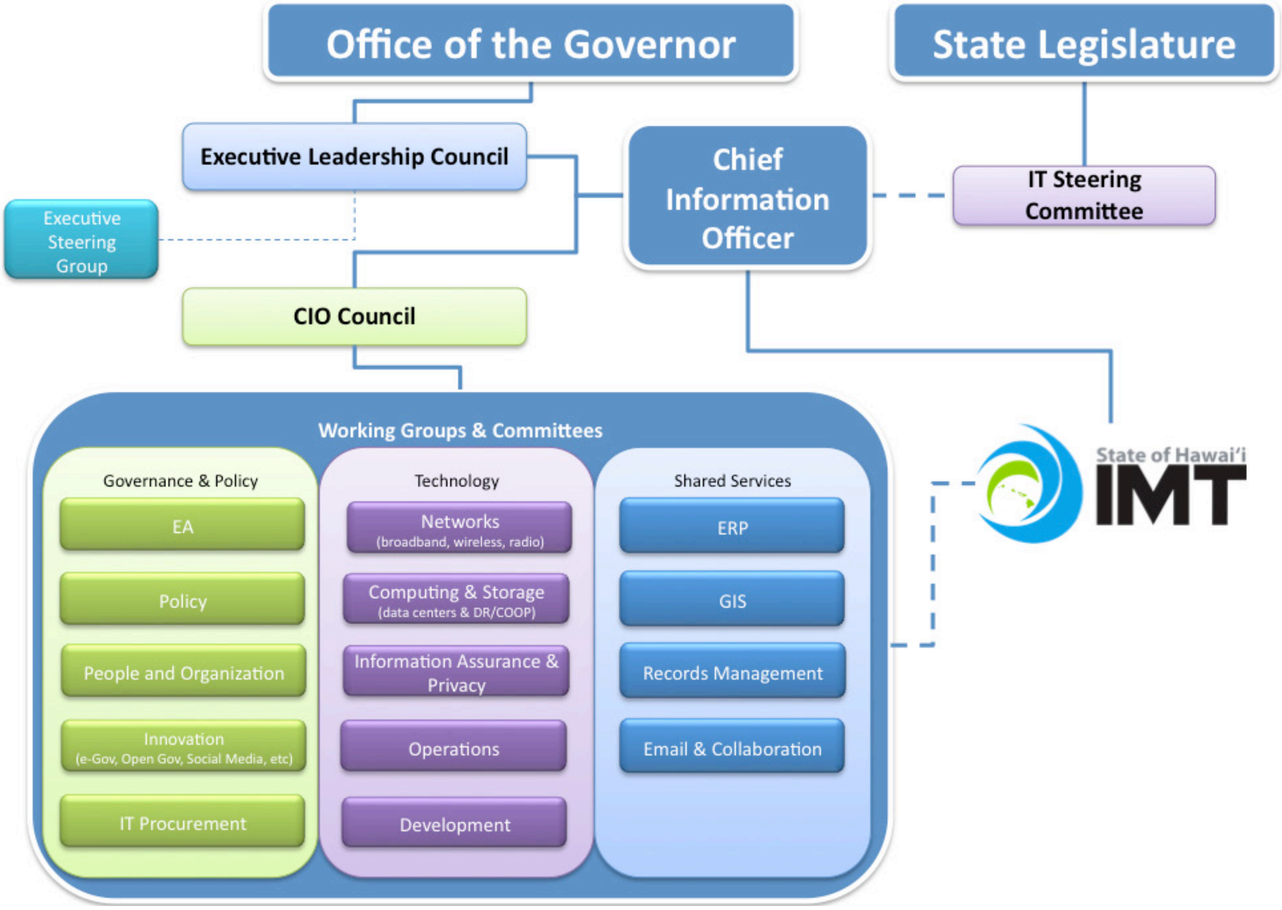


Figure 7: DoIT Structure

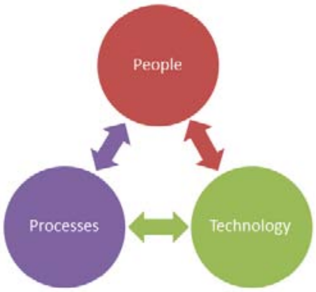
Role	Responsibility
IT Steering Committee	Assist the CIO in developing the State's IT standards and policies
Executive Leadership Council	Implement a governance process to review and rank project requests and IT investments to determine which are best suited to meet the State of Hawai'i's needs. Oversight of the short-term and long-term business plans and budgets of all departments in State of Hawai'i government.
CIO Council	Composed of Department CIOs that are responsible for the selection, control, and evaluation of IT investments. They will advise the CIO on critical IT matters, assess IT initiatives in the budget review process, and conduct post-implementation reviews of completed projects to benefit from lessons learned.
Chief Information Officer (CIO)	• Oversees all IT functions • Develops and executes short- and long-term IT strategic plans • Develops and executes short- and long-term IRM strategic plans • Prepares annual IT budget • Participates in the Executive Leadership Council (ELC) • Leads the CIO Council (CIOC) • Chairs the IT Steering Committee
Deputy CIO	• Establishes and enforces the Enterprise PMO methodology and tools, and reports and manages the PMO • Manages the selection, control, and evaluation of IT investments • Develops, maintains, and facilitates implementation of a sound and integrated IT architecture • Assesses, improves and implements IRM processes • Ensures that projects and initiatives are managed in an efficient and cost-effective manner • Ensure the integrity, availability, and confidentiality of DoIT systems and their data • Assesses technical personnel and ensures that a robust workforce of well-qualified IT professionals is maintained
Business Transformation Officer	• Responsible for business process improvement and reengineering • Establishes and enforces Enterprise PMO methodology, tools, and reporting • Ensures compliance to EA policies • Establishes and enforces IT policy, procedures, and standards including COBIT (framework for IT management governance), ITIL (aligns IT services with business needs), the System Development Life Cycle [SDLC] processes, and the Project Management Plan [PMP]) • Defines and produces dashboards and metrics to measure the performance of DoIT • Ensures the efficient integration of enterprise systems
Chief Management Officer	• Oversees administration of the DoIT • Establishes, oversees, and ensures compliance with processes and standards that verify and validate that requirements and specifications are met for services and systems • Defines and manages Business Continuity policies • Defines and monitors organizational Change Management

6.0 ORGANIZATIONAL CHANGE MANAGEMENT

6.0 ORGANIZATIONAL CHANGE MANAGEMENT

The consolidation of IT resources will bring into play several very important endeavors related to the driving component of this initiative—people. Considerations include:

- Organizational change management—promoting reassurance and inclusion
- Reclassification—implementing freedom and fluidity of process
- Professional development—arming for success
- Recruitment strategy—search for missing pieces



These areas address people and process, two of the three keys to IT excellence shown in the diagram.

This widely accepted paradigm stresses that each of these areas must be addressed when targeting organizational improvement. While the strategies and direction of technological improvements is a big part of this initiative, the targeted first steps surround the functional organization of IT staff, the processes surrounding their advancement, and the opportunities that will be made available to them.

6.1 OVERCOMING CHALLENGES WITH ACTIVE CHANGE MANAGEMENT

The majority of challenges that are faced are not related to technology or process. Rather, the most important and critical challenges are based on the human impact of change. The transformation will have very tangible effects for many people. To ensure that the uncertain and uncomfortable nature of change does not derail the project, a rigorous change management approach will be developed (illustrated in Figure 8 below). Adopting a proactive approach to helping people transition allows for quicker identification of roadblocks, fosters widespread support, and builds the momentum needed to drive the realization of the vision.

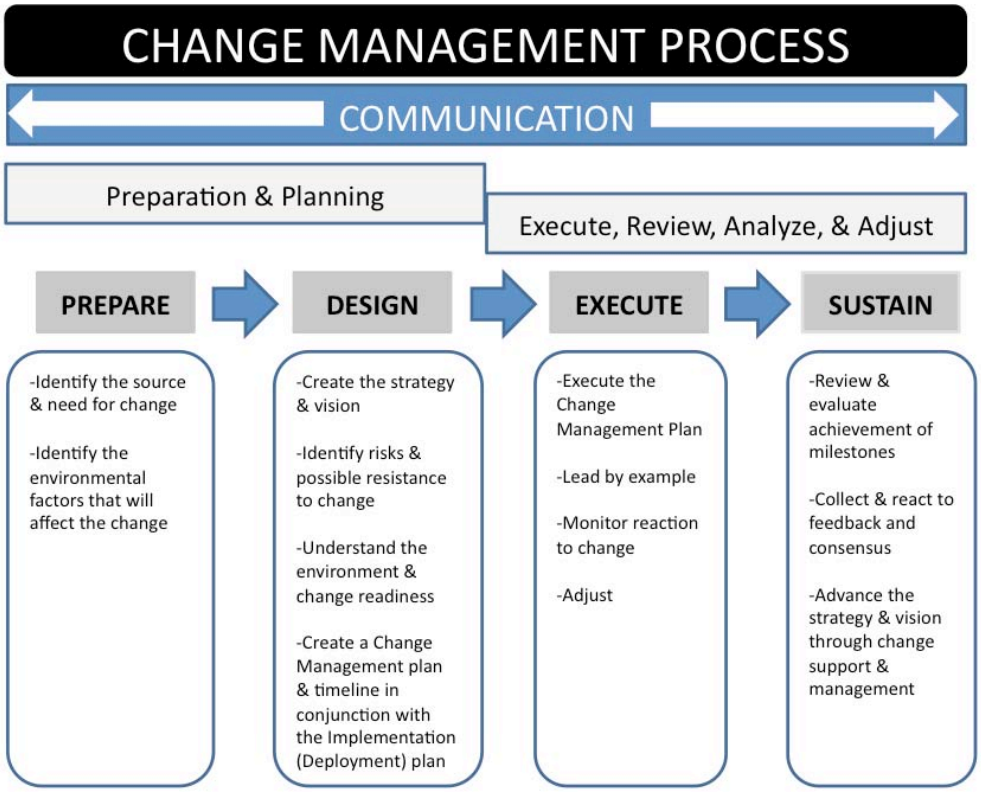

CHANGE MANAGEMENT PROCESS
COMMUNICATION
Preparation & Planning
Execute, Review, Analyze, & Adjust
PREPARE
DESIGN
EXECUTE
SUSTAIN
-Identify the source & need for change
-Identify the environmental factors that will affect the change
-Create the strategy & vision
-Identify risks & possible resistance to change
-Understand the environment & change readiness
-Create a Change Management plan & timeline in conjunction with the Implementation (Deployment) plan
-Execute the Change Management Plan
-Lead by example
-Monitor reaction to change
-Adjust
-Review & evaluate achievement of milestones
-Collect & react to feedback and consensus
-Advance the strategy & vision through change support & management

Figure 8: Active Change Management

6.1.1 ORGANIZATIONAL CHANGE MANAGEMENT

Organizational Change Management (OCM) encompasses all activities aimed at helping an organization successfully accept and adopt new technologies, strategies, and ways to serve its customers. Effective change management enables the transformation of strategy, processes, technology, and people to enhance performance and ensure continuous improvement in an ever-changing environment. A comprehensive and structured approach to organizational change management is critical to the success of any project that will bring about significant change.

6.1.1.1 THE CYCLE OF CHANGE

Change is never-ending. It is unavoidable, continuous, and challenging. However, each generation of change has a clear beginning and end, much like the beginning and end of a technology generation. The diagram in Figure 9 simplifies the complexities of change by dividing a change generation into four phases.

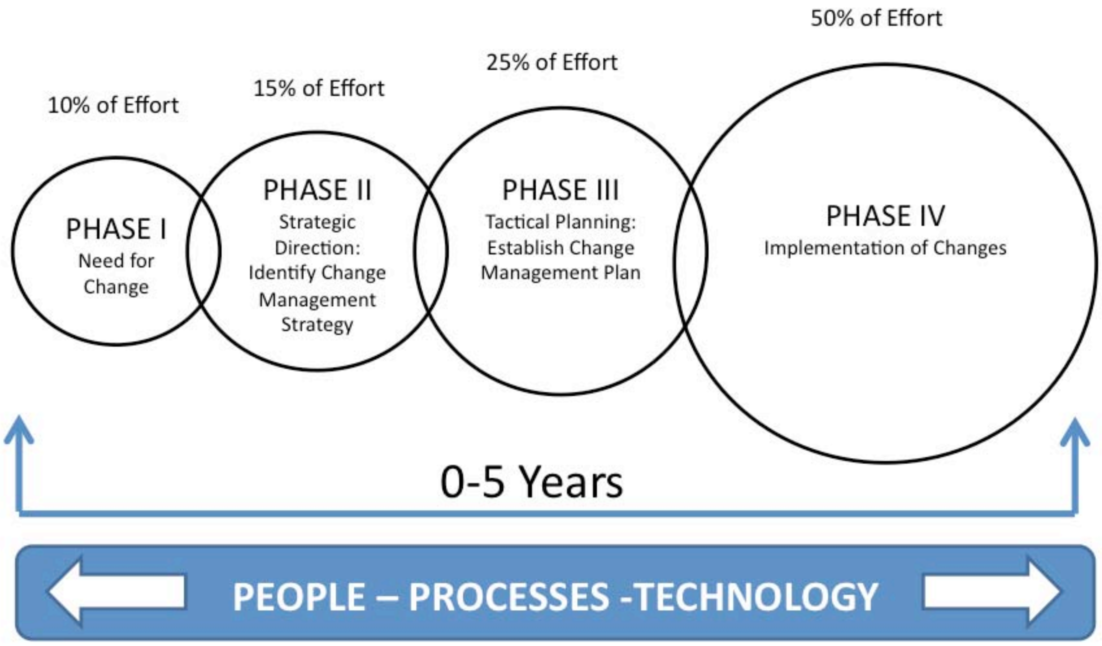

10% of Effort
15% of Effort
25% of Effort
50% of Effort
PHASE I
Need for Change
PHASE II
Strategic Direction: Identify Change Management Strategy
PHASE III
Tactical Planning: Establish Change Management Plan
PHASE IV
Implementation of Changes
0-5 Years
PEOPLE – PROCESSES -TECHNOLOGY

Figure 9: The Cycle of Change

Phase I: Need For Change. Change begins when a vision for how things could be better is identified. While Phase I is about 10% of the effort of a change initiative, relationships formed during this phase are crucial to the ultimate success of the project. In Phase I, the goal is changing the underlying belief systems that determine current performance and block performance improvements.
In this phase, the emphasis is working to convince others that change is necessary.

Phase II: Strategic Direction: Strategy for Change. Once everyone believes that change is necessary, they usually ask, "How will we make the change?" The answer is that the organization needs an enterprise-wide strategy for change, and each organizational segment needs a subordinate strategy that is tailored to its unique operations and congruous with the enterprise strategy. Developing an enterprise-wide strategy for change with supporting agency/program strategies is about 15% of the duration of a typical change management cycle.

Phase III: Tactical Planning—Coordinating the Change Management Plan with the Implementation (Deployment) Plan. This phase involves coordinating the steps that will be taken as the definition of the Change Management Plan moves forward, and how that plan will be coordinated with the Implementation (Deployment) Plan that is being defined during this phase. Defining the details will be expected to take 25% of the change management cycle.

Phase IV: Implementation of Change. The bulk of the time and expense, about 50%, of a change management initiative lies in implementation. Most significant organizational changes will impact business processes, technologies, and the workforce simultaneously. From vision to implementation, the change cycle for this initiative will have the same duration as the expected implementation cycle, a full-scale implementation of five years.

6.1.1.2 THE CHANGE MANAGEMENT PROCESS

John Kotter's book entitled *Leading Change* divides the process of change into the eight stages illustrated in Figure 10.

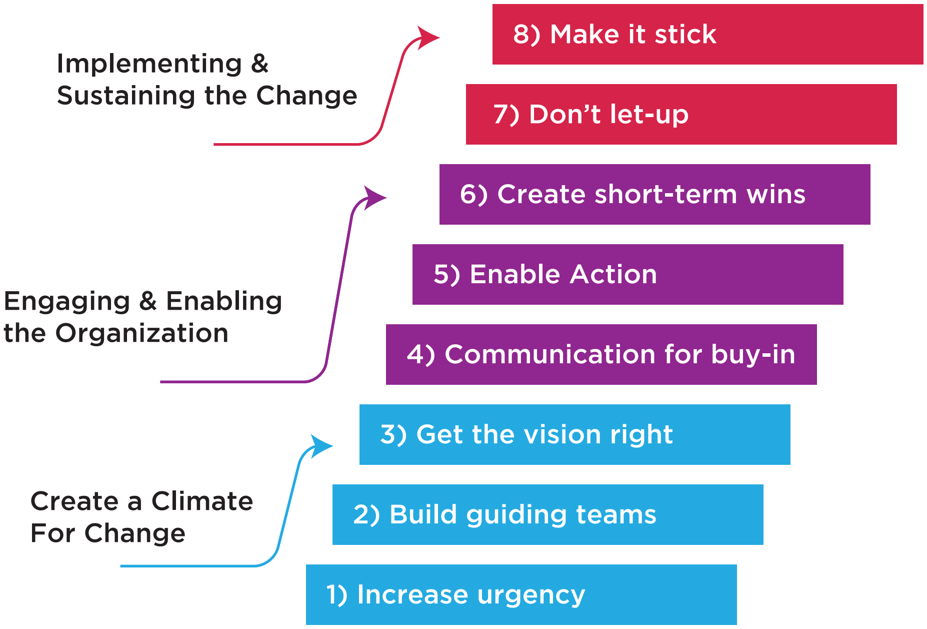

Implementing & Sustaining the Change
8) Make it stick
7) Don't let-up
6) Create short-term wins
Engaging & Enabling the Organization
5) Enable Action
4) Communication for buy-in
3) Get the vision right
Create a Climate For Change
2) Build guiding teams
1) Increase urgency

Figure 10: Eight Stages of Change Management

These stages have been adapted to meet the State of Hawai'i's culture and the goals of the initiative. As the figure shows, the process of change begins when the need for change is identified, and the change is completed when it becomes a habit that is "anchored in the culture." Successive stages of the change process cannot begin until the status of the preceding stage is at least yellow.

The importance of proceeding through the steps in order cannot be understated. Many organizations feel the need to show results, to get past the planning stages and into action. However, unless the case for change has been thoroughly made and an enterprise-wide sense of urgency exists, Kotter stresses that the action will tend to be confined to the small group of true believers. The rest of the organization will resist the change, either due to complacency, perceived self-interest, or cynicism. Rushing ahead without laying the proper foundation for success is a sure-fire plan for failure.

Enterprise change adds a new dimension to the eight stages of change. Specifically, it is typical for the organizational element who originally established the sense of urgency for change to be a few stages ahead of other organizational elements with respect to the change process.

Stage 1: Establish a Sense of Urgency
Proposed actions:

1. Identify and communicate the value of the change, as well as the consequences of avoiding the change. This has been done via the *Auditors Report* and the SAIC report. Press releases and industry communications have been issued.
2. Increase the visibility of the initiative. This has been done via:
   - Website postings: intranet and internet
   - Press releases
   - Industry communications
3. Constant communications. Information will continue to be issued as the initiative progresses to encourage understanding and involvement and give the State of Hawai'i as a whole a reason to care about it. Performance metrics will be instituted, publically published, and delivered to the leadership to make the extensive inefficiencies of the current situation more real and the solution more tangible.

Stage 2 – Create the Guiding Principles and Leadership
Potential actions:

1. Determine the best strategy to establish trust in the initiative leadership and goals. The initiatives, goals, and guiding principles have been established based on the input and guidance of all areas of the State of Hawai'i and outside contributors. These have been published, followed, and maintained:
   - People first
   - Collaborative, open, and transparent processes
   - Effective and efficient strategies, implementation and management based on proven best practices and industry standards
2. Define a common goal. What should be accomplished needs to be established. The critical aspect is that everyone agrees on the goal. Even if no consensus arises as to the process or the method, at least the various organizations are not working at cross purposes. The common goal must also be defined as specifically as possible.

The common goal has been established through two previous, but cut short, initiatives and the consensus that this initiative must succeed and must address the problems that have been commonly recognized.

3. Take visible actions and make sacrifices. The end result of change will always involve the termination of certain investments against the wishes of their supporters. Sacrifices will have to be made in terms of money and control. In order to create unity across the various departments and agencies, it must be established early on that all the sacrifices will not be either in vain nor administered unfairly. To establish trust and win consensus, every stakeholder needs to show that they are willing to bear some of the cost themselves. By voluntarily and publicly ceding some degree of self interest in pursuit of the greater good, the leaders will demonstrate to each other and to their own people that they are serious about the changes, and are willing to do what is necessary to make them real.

Stage 3 – Develop a Vision and Strategy

Potential actions:

1. Develop vision to be compelling picture of future performance. Start at the end and work backward. What does the goal look like? What is it we hope to achieve? Again, the goal needs to be as specific as possible and can evolve over time. The key is that the processes established are just that–processes that are the means by which we move the organization from the as-is state to the to-be state; they are not the goal in and of themselves. Whatever the decision is, it should be ambitious, but also realistic and achievable, and it then must be a constant refrain from the leadership of how the State of Hawai‘i intends to do business from this point forward. This action has been fulfilled via this report.

2. To foster broad debate, distribute the draft vision statement widely. While the leadership makes the decisions and sets the policy, there are many smart people throughout State government who can contribute greatly to defining the future state. A static and unchanging goal is almost no better than no goal at all. Once the initial vision has been established, it must be publicized, and feedback should be welcomed. Changes in circumstances, technology, and mission priorities will necessitate occasional re-visioning. By incorporating feedback into the new vision, not only will the stakeholders feel a greater sense of ownership in the process, but the objectives of the process will be stronger. This action has been fulfilled via this report.

3. Devise strategy that can be applied throughout the organization. One leadership tenet that holds especially true in this case is “Tell your people what to do, not how to do it.” Even when the goals of all the different organizations and stakeholders within the State of Hawai‘i are aligned, the processes by which those goals are achieved can vary greatly. Personnel, culture, mission, and resources all play into the best way to accomplish a goal, and no one-size-fits-all approach will be successful everywhere. As long as the desired results are clear and consistent, the ways and means employed to achieve those ends should be flexible.

   This action has been fulfilled via the strict adherence to the guiding principles of this initiative as the strategies of this report have been identified.

4. Rework the vision and strategy to be clear, concise, and compelling. Finally, the output of this phase is a document. The vision (where we are going) and strategy (how we are getting there) should be written down and distributed. Agreeing on a common vision means little if it cannot be published and referenced. Ultimately, the guiding principles and leadership will have developed a statement that clearly, concisely, and convincingly spells out what needs to be accomplished, and the plan for achieving those goals.

   This action has been fulfilled via this report. It is recognized that the process will continue to evolve as it moves forward.

Stage 4 – Communicate the Change Vision

Once the vision is established, there are a number of ways to communicate it.

Potential actions:

1. Publish the vision/strategy prominently on the organizational website.

2. Take the vision/strategy on road shows throughout the organization. Nothing makes an impression quite like a personal appearance. Site visits to the stakeholders’ home bases by leadership is an important part of the communication strategy. Not only does a personal visit demonstrate the importance of the topic to the leadership, it is much more likely to be listened to than a passive web posting. Finally, proclaiming the vision in person allows the leadership to answer questions and address concerns in the field immediately, helping to foster understanding and buy-in.

3. Explain inconsistencies between vision and current actions. Few plans are ever executed without complications. However, when unique circumstances or emergent priority shifts cause the execution to deviate from the plan, there is a high potential for people to become disillusioned with the plan itself. If our leaders are not following their own guidance, why should we? It is critical that inconsistencies be explained in order to preserve morale and commitment to the goal.

4. Address nay-sayers and their reservations. In any organization, and with any change, there are bound to be those who resist. Sometimes these people can be persuaded to get on board for the big win, but other times they are not looking to be a part of the solution. Regardless of the cause for their resistance, their concerns need to be treated as valid, as indeed they often are. It is sometimes the case that the most recalcitrant obstructionist has a valid point that the true believers had not thought of. To encourage fence-sitters to believe and trust leadership rather than fall in league with the malcontents, even those few who refuse to adapt must be treated fairly and their concerns addressed.

Stage 5 – Empower broad-based action

Once the vision has been established and communicated, it is time to let the people do their job. It is now leadership's role to facilitate, rather than direct, their actions. Certain steps can be taken to enable the process and reinforce the behaviors that contribute to the goals of the organization.

Potential actions:

1. Remove obstacles perceived by many to impede progress. No strategy, no matter how well planned, can anticipate all potential roadblocks. Also, certain obstacles can appear which had not existed before. It is important that once the momentum for change has been painstakingly built, it is maintained. It is here that leadership must actively find ways to remove or alleviate the obstacles and burdens that impede progress toward the goal or risk losing the support of the people who are needed execute the plan.

2. Align HR practices (e.g., hiring and promoting) with the vision. When people change their normal way of doing business, they expect to see some benefit. Likewise, when they see others who have not adapted, yet suffer no repercussions, they begin to doubt the organization's commitment to its stated goals. Awards and promotions, or the lack thereof, can provide both the carrot and the stick to help drive the behavior that engenders success.

3. Align processes and training programs with the vision. No major change will be taken seriously if it is not reflected in the day-to-day experience of those involved. We cannot expect our goal to be successful if those it affects are left to figure it out for themselves, or if they can routinely ignore it. Anyone involved in the IT consolidation initiative should be trained and involved in the changes.

4. Address supervisors who resist the required changes. There are few things more frustrating than trying to follow a higher-level policy when one's immediate supervisor does not support it. In order for our goal to become engrained in the culture, it must be as firmly established as security clearances and dress codes. Resistors are entitled to their own opinion, but their actions must be in alignment with the organization.

Stage 6 – Create short-term wins

Success breeds more success. Short-term wins not only move us closer to the desired goal, they are also useful as a motivating tool. Identify and publicly proclaim these wins to show that the process is working, and more successes will follow.

Potential actions:

1. Identify and plan specific short-term wins (i.e., six months). Some successes will come naturally, others unexpectedly. However, there are some interim goals that can be planned in advance, striven toward, and achieved. Setting short-term goals makes problems more achievable, and achieving those goals gives participants a sense of accomplishment that makes the next goal more attainable.

   Examples of early wins and demonstration of competence were identified in the *State of Hawai'i Business and IT-IRM Transformation Strategic Plan (Version 2)* and proposed through a series of smaller projects executed during the planning phase. These projects fell into four categories:

   - Triage projects are required immediately to fix unrecoverable, high-impact failures in critical systems that are currently at a high probability of failing.

   - Pilot projects are required near-term involving high-impact, low-cost enhancements to the existing system that radically improve employee productivity, are synergistic with long-term EA, and can demonstrate future vision now.

   - BPR projects are focused on defining, measuring and reengineering business processes for more efficiency and automating with IT/IRM as required.

   - Major initiatives are large IT/IRM projects that are flagship initiatives for the State, represent key administration priorities (either already underway or launching prior to July 2013 implementation), and need management/governance according to the strategic plan.

2. Assign managers responsibility to achieve short-term wins. While short-term wins may be natural or even unexpected, they are rarely accidental. They are the result of a determined effort by a finite set of people. Identify the managers whose roles put them in a position where they are capable of achieving success, then make it clear that success is expected. The likelihood of success is much greater when it becomes personal: "my job" instead of "everybody's job."

3. Publicize, celebrate, and reward short-term wins. Even for those not directly involved in the win, seeing that success is recognized and rewarded provides motivation for their own effort. For those who are directly involved, public recognition makes the hard work and sacrifice worth it, and will encourage continued success.

4. Provide evidence that sacrifices are linked directly to the wins. As discussed earlier, change can upset the status quo in terms of money and control, and sacrifices of one, the other, or both will be required by everyone. Show a direct link between the money that was taken away from such-and-such system and given to IT procurement, or training, or whatever the departments need to underline the importance of the effort and the benefit being derived from it.

Stage 7 – Consolidate gains and produce more change

After a certain level of success has been achieved, keeping the momentum going is the next challenge before complacency sets in. The success must be expanded, the bar raised higher, and the impetus that produced the original achievement maintained.

Potential actions:

1. Involve a larger number of organizational segments in change. Very often, it is only specific segments of the organization that have led the way in establishing change. Once a track record has been established and lessons have been learned, the next logical step is to reach back to the lagging segments and bring them into the fold. They will have seen that the sacrifices of the trailblazers have been rewarded and that their initial reluctance was unfounded. The specter of uncertainty will also be greatly diminished by this point, and their original objections or concerns will have been largely addressed.

2. Continue to generate and publicize short-term wins frequently. Final success rarely comes in one fell swoop, but rather in many small victories. In order to maintain the sense of urgency and keep interest high, the practice of recognizing these victories is even more important than before so that attention remains focused on the goal. Continue to make a point of celebrating success.

3. Delegate management roles to low organizational levels. What was once a new initiative, requiring high levels of direct involvement of the upper echelons of leadership, is now becoming standard practice. The big problems have largely been solved, and all that remains is execution. The top levels can afford to shift some (but not all) of their attention to new problems, and allow the routine decisions to be made at lower and lower levels. This is in itself a success; the new process is now routine. It also serves as yet another means to provide a sense of ownership and accountability, both of which will yield even more success going forward.

4. Eliminate unnecessary process interdependencies. Lean engineering principles tell us that any process can be improved and streamlined almost indefinitely. Certain process steps that were necessary early in the change process will be able to be eliminated, bottlenecks relieved, and redundancies reduced. Continually refining the process also demonstrates that what matters is the result of the process, not the process itself. Furthermore, by removing unnecessary or now-irrelevant interdependencies between process steps or organizations, the process becomes more flexible, can be applied more widely, and requires fewer resources.

Stage 8 – Anchor new approaches in the culture

Now that we have achieved the goals we set out to accomplish, we must not allow the organization to forget what was accomplished and revert to the status quo. The changes we initiated so long ago are now a part of the normal course of business. To ensure that we do not backslide, there are some steps we can take.

Potential actions:

1. Graft new practices onto valuable aspects of the old culture. Although we instituted major transformational change, there are many aspects of the old culture that should be maintained. Where it is possible and appropriate, it is time to fold the new processes into the old so that our transformational effort becomes an almost invisible part of everyday life.

2. Evolve ineffective, old cultures. Organizations must continually evolve to adapt to new circumstances. While valuable parts of the pre-existing culture should be preserved and adapted, the parts that no longer serve the mission need to be eliminated.

3. Interview new hires from perspective of the vision and strategy. Does this potential hire agree with the goals of the organization, and will he or she act in a way that promotes the success of the organization? By ensuring a good cultural fit at the outset, and communicating the priorities and goals of the organization up front, leadership can help to ensure that the hard-won culture shift becomes permanent.

3. Incorporate vision and strategy into succession planning. Personnel changes in leadership positions are a fact of life in the State of Hawaiʻi, and most change initiatives are intended to outlast their original sponsor. Often, the "new sheriff in town" has his or her own priorities and goals to achieve that may or may not agree with those of the predecessor. In many respects, this is a welcome change and serves to re-invigorate a stagnant culture. However, not everything can change, and the years of work that went into establishing the new paradigm should not be discarded lightly. The outgoing leader should take steps to ensure that the new one agrees with the most important goals and will continue to support them alongside the new initiatives that will surely follow. This also means that the vision and strategy must be defined with the future in mind, and cannot be a narrow or personal definition suited only to the current powers that be.

6.1.1.3 CURRENT STATUS OF THE EIGHT STAGES

The table below outlines the current status of the eight stages of the Change Management process.

Stage	Stage Title	Status	Assessment
1	Establish a sense of urgency	Green	The current level of urgency driving the initiative is supported and participated in by all levels of the State of Hawai'i. Specifically, the Legislature, department leaders, OIMT members, the CIO, and representatives from multiple departments on the People and Organization Working Group are all engaged.
2	Create the guiding principles and leadership	Green	The Leadership Team, the People and Organization Working Group, a core OIMT staff, and the CIO have been assembled, established, and engaged.
3	Develop a Vision and Strategy	Green	This report represents the development of the vision and strategy of this initiative.
4	Communicate the change vision	Green	Besides the issuance of this report, its strategies and goals will be also communicated via other means.
5	Empower broad-based action	Green	Detailed steps and participants will be defined in the next stage (the Tactical Planning stage) of the initiative's three stages of Strategic Direction Towards Implementation (Strategic Direction – Tactical Planning – Implementation).
6	Create short-term wins	Green	Part of the Tactical Solution planning will incorporate short-term wins.
7	Consolidate gains and produce more change	Green	This will be a natural progression of the implementation and change management plans.
8	Anchor new approaches in the culture	Green	Going forward, this will be a process of implementation and management.

7.0 HUMAN RESOURCE CONSIDERATIONS

7.0 HUMAN RESOURCE CONSIDERATIONS

The strategies outlined for human resource considerations were developed based on the valuable work done in two previous IT reorganization efforts undertaken in 2000 and 2004. This work is highlighted and utilized as the foundation of the strategy in the "Reclassification Considerations" section. The sections that follow on "Recruitment Strategy" and "Professional Development" are based on this foundation.

7.1 RECLASSIFICATION CONSIDERATIONS

When defining the functional design of the new DoIT, care was taken to make sure that it would incorporate:

- Best practices
- A vision for growth and advancement
- An efficient, agile, and responsive IT environment
- All of the parameters established via the To-Be requirements studies

It was determined that a best-of-the-best structure was the goal, and the focus would be on functionality and not on the current organization or positions. Based on the extensive work done in previous reorganization efforts, reclassification requirements were identified as a key component necessary to create a nimble IT organization that can be attractive to a talented and committed workforce.

An important first step was leveraging the previous efforts for reclassification of IT positions. The first was undertaken in 2000, and a second was launched in 2004. In both of these initiatives, the goal was to identify the proper strategy that would lead to retention of existing employees as well as successful new employee recruitment. The issues identified and strategies for resolution have changed little since these first efforts; unfortunately, they did not have the administration support, fiscal climate, or political environment to enable them to move forward. It is the work, results, and recommendations of these prior initiatives that will be the foundation that this initiative will build on.

7.1.1 WHY THIS EFFORT IS DIFFERENT

In the face of the historic attempts at IT reorganization, it must be pointed out why this initiative is different and how it has been designed for success:

From the SAIC report:

- Strong gubernatorial and Legislative support and critical prioritization with the passage of Act 200 and Act 84 (HRS 27-43)
- Identification and hiring of the State's first CIO
- Establishment of OIMT
- Department and IT leaderships' overwhelming recognition of the need to enhance IT solutions to conduct the business of the State and service the citizens more effectively and efficiently
- Creation of an *IT Strategic Plan*
- Establishment of an IT Steering Committee to support the CIO and IT governance activities
- Mandated annual briefings to the Legislature regarding the status of IT and progress against the *IT Strategic Plan*

These actions provide evidence that the State is now ready to take the next steps in addressing IT needs and opportunities with both commitment and focus.

7.1.2 CURRENT RECLASSIFICATION STRATEGY DEFINITION

The strategy for the current reorganization is to leverage the work delivered from the second IT reclassification initiative (incorporating the best of the first initiative) and the lessons learned from a very successful broadbanding effort at the University of Hawai'i. The University had encountered the same issues that the State of Hawai'i IT has continued to face.

The initiative will include close cooperation between the developing Department of Technology, the DHRD, and the Hawai'i Government Employees Association (HGEA) to finalize a flexible and attractive IT recruiting, hiring, and retention strategy. A summary of this strategy and approach is below.

7.1.3 CHALLENGES/PROBLEMS

Multiple departments and stakeholders identified several IT staffing challenges through surveys and discussions conducted by the reclassification initiatives that preceded this effort:

- Difficult to recruit and retain good employees with the desired competencies
- Pay not competitive with private sector
- Good performance is not recognized or rewarded
- Certifications are not recognized, rewarded, or encouraged
- Classification challenges:
  - Takes too long (classification specs become outdated because work in the occupation changes frequently)
  - Inflexible and restrictive traditional position classifications
  - Inability to add value for IT expertise that requires a broad spectrum of responsibilities; in particular, for those statewide systems that have cross-jurisdictional responsibilities and requirements

  - Constant updating of or the need to update class specifications as means to address overall compensation (total reward program)

  - IT positions are only one of several classes of positions in their professional series, and other professional classes must be considered.

- Restrictions in granting higher pay levels

- Funding challenges

- Challenges in the State of Hawai'i environment, including human resource turnaround time for IT recruitment announcements and screening

7.1.4 RECOMMENDATIONS

The following recommendations outline the strategy proposed for a successful reclassification effort:

- Modernize the IT classification system:
  - Simplify the classification tiers, including broadband.
  - Update classification and job descriptions.

- Design a successful recruiting process:
  - Incorporate the Professional Recruiting Office (PRO). PRO is a pilot project created by DHRD to complete the entire recruitment process, from application to hire, in a few days.
  - Launch a creative marketing campaign.
  - Recruit by resume:
    - Investigate using the NEOGOV system.
    - Take care to identify the necessary supplemental questions needed to determine if minimum requirements are met. Resumes are often too brief and lacking in specific job information to make a fair and consistent determination of eligibility/ineligibility. The lack of complete information in a resume can lead to disparate treatment and inefficient hiring decisions.
  - Re-engineer and simplify the screening and selection process.
  - Introduce waivers from minimum qualifications.
    - Federal and State law guidelines must be followed.
  - Hire and recruit above minimum wage levels.
    - The current flexible hiring rate pilot project for certain IT positions should be expanded.
  - Pay for performance based on compensable factors.
  - Encourage obtainment of recognized certifications and reward them.

- Implement a funding strategy.

7.1.5 BENEFITS

- Improves recruitment and selection

- Simplifies and expedites classification

- Ability to reward professional growth and exceptional employee performance attracts individuals who are motivated:
  - Promotes employee excellence
  - Saves money and provides an incentive to complete projects that result in savings for the State
  - Creates efficiencies and encourages the performance of additional responsibilities
  - Promotes excellence in employee performance and boosts morale

- Tangible demonstration of the Administration's philosophy to:
  - Motivate State workers to perform at a high level
  - Reward and recognize them for their ideas and contributions to the organization

- Empowers managers and provides them with a tool to manage operations

- Employees have opportunities for career track options:
  - Enables flexibility to move from band to band (vertical mobility) and across bands (lateral mobility)

7.2 RECRUITMENT STRATEGY

7.2.1 APPROACH

Recruiting qualified IT employees can be a challenge for many reasons:

- Skilled resources are in high demand.

- Candidates without ties to the State of Hawai'i may not consider it a long-term destination.

- It can be difficult to validate a candidate's credentials in such a fast-paced field.

- Commitment to guiding principles and cultural fit can rule out candidates.

An effective approach to recruitment can help the State of Hawai'i successfully compete for limited technical employee resources. To maximize its competitive advantage, the State must choose the recruiting method that produces the best pool of candidates quickly and cost effectively for each position to be filled.

With a typical hiring cycle taking several weeks to complete, all efforts must be made to recruit in an expedited manner. Not counting the prep work going into position advertisement, once an open position is published, it can take six to eight weeks to notify and screen applicants, and a week or more to conduct interviews and make a decision regarding a job offer. After the decision is made, the selected candidate should be expected to give a two-week notice to his or her previous employer, and the first week of employment is often consumed with on-boarding activities such as new hire orientation, benefits overviews, training, and getting acclimated to the new position. This process can leave vital positions vacant for months.

7.2.2 RECRUITMENT PLAN STRATEGIES

- Identify the roles and/or positions to be filled.

- To accurately determine recruitment needs, clearly define all requirements for job openings:
  - To discourage all but the best applicants from applying, include specific employee requirements in the position's description.

- Assign salary and organizational placement to the positions based on industry research and internal guidelines:
  - Establish a starting salary within the predetermined range.
  - The cost of the position must consider professional growth, certification maintenance, the impact of future raises, and compensation.

- Determine sources of funds for the cost of the recruitment process and the cost of supporting the new position:
  - This must be addressed before the recruitment process begins.
  - Budget definition will drive the recruitment plan decisions.

- Determine key position requirements and avoid candidates that do not fulfill them.

- Identify recruitment sources:
  - Hiring from within
  - DHRD recruitment
  - Employee referral program
  - Professional organizations
  - Alumni associations
  - Graduate placement programs
  - Armed forces (dependents)
  - Media (e.g., newspaper, radio, television)
  - Trade magazines
  - Websites
  - Internet job sites
  - Social media outlets

- Select the appropriate recruitment sources for each position:
  - Considerations include the cost of the recruitment channel, convenience, speed, workforce demographics and trends, appropriateness for position, and the target audience.
  - Identify the target population/audience for the position.
  - Avoid under-recruitment (no viable candidate pool is generated) or over-recruitment (flood of applications).

- Determine and launch recruitment efforts.

- Establish guidelines for testing and validation of credentials:
  - Interviews will include the Technical Lead.
  - To verify the candidate can troubleshoot, diagnose, and repair as needed, conduct a hands-on test.
  - Verify past work experience.

- Determine how candidates and resumes will be reviewed and establish timelines for each of the following:
  - Who will the resume/application be submitted to?
  - Who will review the application?
  - Who will verify the credentials of the candidate?
  - Who will the interview the candidate?
  - How will interviews be conducted:
    - In person and/or by phone
    - Provide candidates an opportunity to learn more about the position, the environment and the culture (avoid acceptance without knowing about aspects that might affect long-term job satisfaction, or refusal without knowing about some of the job's attractive attributes).
    - Interview new hires from perspective of the vision and strategy:
      - Does this potential hire agree with the goals of the organization, and will he or she act in a way that promotes the success of the organization?
      - By ensuring a good cultural fit at the outset, and communicating the priorities and goals of the organization up front, leadership can help to ensure that the hard-won culture shift becomes permanent.
  - Who will create and deliver job offers to selected candidates?
- Preserve recruitment lessons learned—remain competitive as an employer:
  - Continually evaluate the process of attracting, obtaining, and retaining talented IT employees.
  - Factors to consider when defining recruitment goals and the strategies:
    - Evaluate current and future workforce needs.
    - Understand the Department's strengths and weaknesses.
    - Establish strategies for achieving and maintaining diversity in the workplace.
    - Gather and analyze feedback from new and transitioning employees.

7.2.3 ESTABLISH A RECRUITING CULTURE

It is important for hiring managers to remember the human aspect of this process. Although defining roles and screening applicants can be a tedious task, mistreating potential employees can be a detriment to the reputation of the State as an employer. Before any job openings are posted or any resumes are considered, the following must be determined and adhered to:

- Determine the candidate submission deadline:
  - In fairness, applications submitted beyond the deadline will not be considered for the job opening unless no other candidates meet the qualifications of the posting.
  - Applications submitted after the deadline may be kept on file for future openings.

- Determine the interview deadline:
  - Interviews for qualified candidates must be scheduled quickly.
  - It is poor business practice to cancel or reschedule interviews, and doing so can be detrimental to the reputation of the State as an employer.

- Determine the final selection deadline:
  - Hiring managers must adhere to the final selection deadline.
  - Prolonging a vacancy can cause undue burden on existing employees and allow job seekers time to be recruited by another source, causing the State to miss opportunities to hire the most qualified candidates.

- Final decision and employment offer:
  - The individuals who are designated to make the final decision in the hiring process must be available to authorize the employment offer by the established deadline.
- Determine the start date (and end date [if contract employee]):
  - The employment offer must include a start date and any prerequisites required of the future employee.
  - An end date must be included for all contract employees.

Establishing communication expectations to and from potential employees can ease some of the frustration of the screening and hiring process. It can also help promote confidence in the hiring process for both the applicant and hiring department.

7.3 PROFESSIONAL DEVELOPMENT

7.3.1 OVERVIEW AND APPROACH

During the reorganization it will be expected that multiple employees will be found to have redundant skillsets, while other areas of expertise are left unfilled. A skillset void can also be created by moving an employee off a particular team or by changing the employee's role within the organization. The voids can be addressed by either hiring a new employee or training an existing one. There are three key reasons why training is the preferred solution:

- It is less expensive to train good employees than find new ones.
- Employees will benefit from training both personally and professionally.
- Effective training of existing staff is essential to developing and retaining a qualified workforce.

To maintain productivity and employee morale, all skillset voids will be addressed quickly. Combining the appropriate technical resources into one centralized department will bring together a wealth of knowledge and experience. This should be leveraged as a source of training and sharing of knowledge between IT staff. Intradepartmental training is a great opportunity for existing employees to gain new skills at little cost to the State.

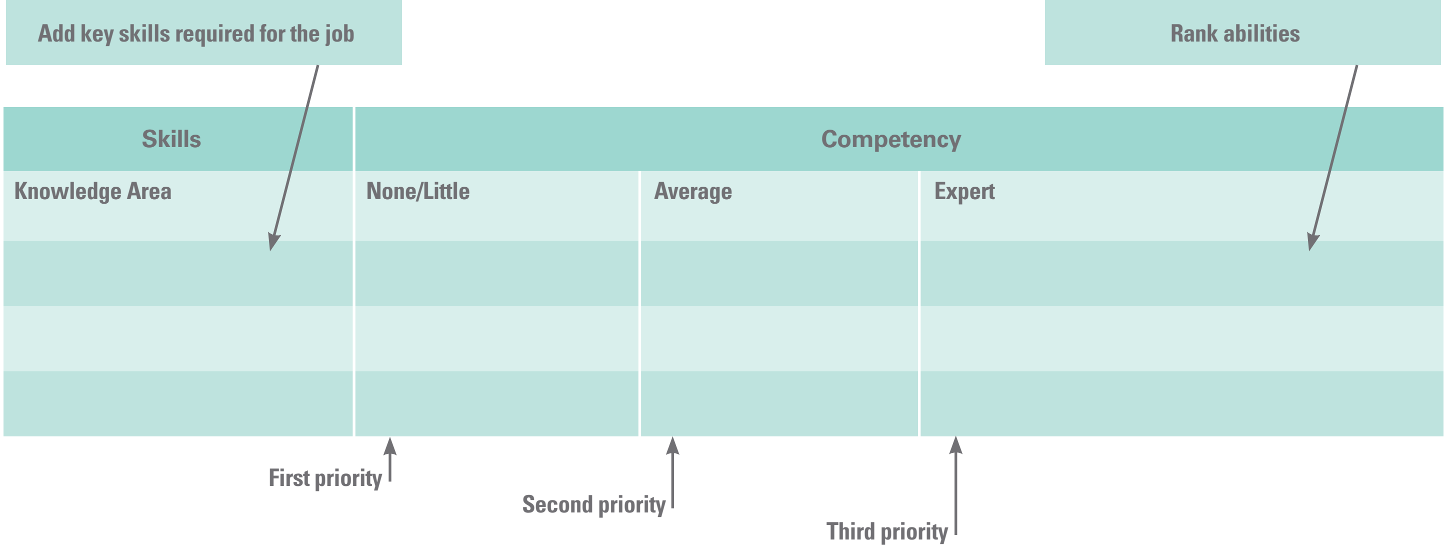
When outside training resources must be utilized, there are several to choose from: online training, software-based training, classroom, and private companies.

7.3.2 TRAINING PLAN STRATEGIES:

- Identify required skillsets—existing and future:
  - Identify and document competencies/skills required for each job description.
  - Maintain a current inventory of skills.
  - Address overall career development issues as well as skill-specific training issues.
- Perform a skillset gap analysis—existing and missing:
  - Day-to-day: support, development, and management
  - Strategic growth: identify implementation timelines and allocation commitments in such areas as technology innovation.
- Conduct a training needs analysis:
  - Align IT training needs with business goals.
  - Use self-directed tools, such as individual development plans, to give employees responsibility in assessing their development needs.
  - Ensure that management training is included (e.g., leadership and project management).
  - Identify and prioritize cross-training and begin to incorporate it. (Identify the most critical specialties and niche areas of expertise; having a single person that is trained or qualified for a needed skill is a risk).
- Select training sources:
  - Consider cost, availability, duration, success rates, and compatibility with the resources to be trained
  - Intradepartmental training opportunities (resources within the department train other department resources)
  - Internet
  - Classroom
- Create a training timeline:
  - Involve critical stakeholders, such as top management, business unit managers, subject matter experts, human capital staff, and end users in planning IT training.
  - Prioritize training.
- Launch training:
  - Use a single portal to give staff and managers access to training and career development information.

7.3.3 TRAINING NEEDS ANALYSIS

As shown below, identification of training needs will be done by assessing current skillsets to determine gaps and any single points of failure, and also to establish the order in which training should be conducted.



Add key skills required for the job

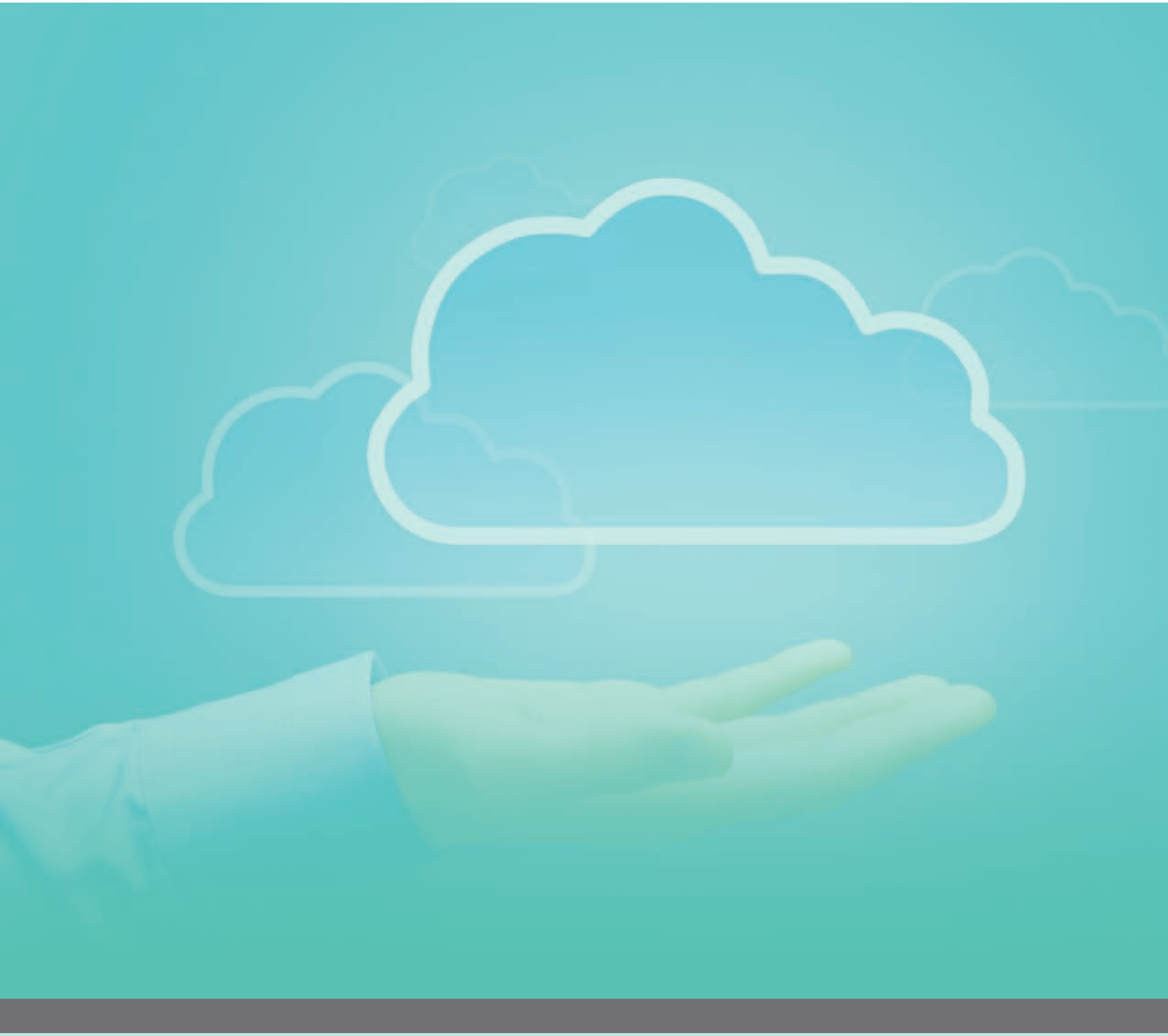
Rank abilities

Skills	Competency		
Knowledge Area	None/Little	Average	Expert

First priority

Second priority

Third priority



8.0 IMPLEMENTATION STRATEGY

8.0 IMPLEMENTATION STRATEGY

The *Implementation Plan* was developed based on:

- Legislative and legal requirements and their lead times
- Departmental processes and lead times
- State of Hawaiʻi culture
- As-Is and To-Be functional designs
- Incorporation of short-term wins
- Lessons learned from reorganizations conducted in other states

Based on the acceptance of the strategies outlined in this document, the implementation steps would be defined in the timeframes in Figure 11.

Implementation Strategies and Timeframes				
	0 to 6 months	**6 months to 1 year**	**2 to 3 years**	**3 to 5 years**
Immediate: Create the Department of Information Technology	🟩			
Short Term: Establish & Implement DoIT Organization, People, Processes & Technologies		🟩		
Medium Term: Create & Implement the Model			🟩	
Long Term: Maturing the Model				🟩

Figure 11: Implementation Strategies and Timeframes

8.1 IMMEDIATE STRATEGIES AND TIMEFRAMES (THE FIRST SIX MONTHS)

Begin the consolidation process:

- Submit the *IT Strategic Plan.*
- Develop a recruitment strategy to address how existing IT professionals at departments will be transitioned to DoIT in terms of the LOB concept and reporting structure.
- Continue Governance via the ELC, CIOC, and IT Steering Committee.
- Establish Organizational Change Management.

8.2 SHORT-TERM STRATEGIES AND TIMEFRAMES (SIX MONTHS—ONE YEAR)

Define strategies and tactical plans for establishing and implementing the consolidated organization, people, processes, and technologies:

- Begin the tactical planning process:
  - Business Transformation Office (BTO)
  - Operations
  - Management Services
  - Department Services
  - Enterprise Shared Services
  - Infrastructure Service, Delivery, and Support
  - Enterprise Security and Privacy

- Create a Program Management Office (PMO) and Development, Modernization, and Enhancement (DME) projects.

- Begin to implement enterprise solutions:
  - Enterprise Resource Planning (ERP)
  - email consolidation ✓**Quick Win**
  - Tax modernization
  - Help Desk
  - Expand use of ICSD Internet Board ✓**Quick Win**

- Begin to implement infrastructure solutions:
- Data center (e.g., NOC, CSOC, Help Desk)
  - Adaptive computing environment
  - Networking ✓**Quick Win**
  - Mobile, wireless, and radio
  - Shared services applications (rapid application prototyping)
  - GIS

- Establish fiscal/budget management.

- Develop enterprise architecture (EA).

- Establish business transformation initiatives (two or three):
  - Contract vehicle, agency business transformation, and tracking

- Create portfolio management:
  - Establish IT/IRM tactical planning.
  - Implement a call for IT/IRM projects.

8.3 MEDIUM-TERM STRATEGIES AND TIMEFRAMES (TWO-THREE YEARS)

Create and implement the model:

- Hire key executives:
  - Business Transformation Office (BTO)
  - Operations (Deputy CIO)
  - Management Services (CMO)
  - Department Services
  - Enterprise Shared Services
  - Infrastructure Service, Delivery, and Support
  - Enterprise Security and Privacy

- Before ICSD can be folded into OIMT/DoIT, revise the statute to authorize OIMT/DoIT to employ civil service employees.

- Create a Customer Relationship Model (CRM):
  - Service Level Agreements (SLAs)

- Create a security policy and procedures.

- Create an IT policy, procedures, and standards (COBIT, ITIL, SDLC, and PMP).

- Create an IT performance management framework (dashboards and metrics).

- Implement Compliance Management.

- Establish Disaster Recovery.

- Create Enterprise Program Management (office, methodology, tools, and reporting).

- Establish electronic records management.

- Consolidate network resources (facilities, budget, and people).

- Data center:
  - Establishment of Data Center 2
  - Consolidation of Data Center 2 resources (NOC, CSOC, and Help Desk; and facilities, budget, and people)

- Adaptive computing environment:
  - Implement next generation solution
  - Consolidation of adaptive environment resources (facilities, budget, and people)

- Network:
  - Implement next generation solution
  - Consolidation of network resources (facilities, budget, and people)

- Mobile, wireless, and radio:
  - Implement next generation solution
  - Consolidation of mobile, wireless, and radio resources (facilities, budget, and people)

- Shared Services applications:
  - Departmental legacy application retirement/consolidation/modernization (150)
  - Implement next generation solution
  - Consolidation of Shared Services applications resources (facilities, budget, and people)

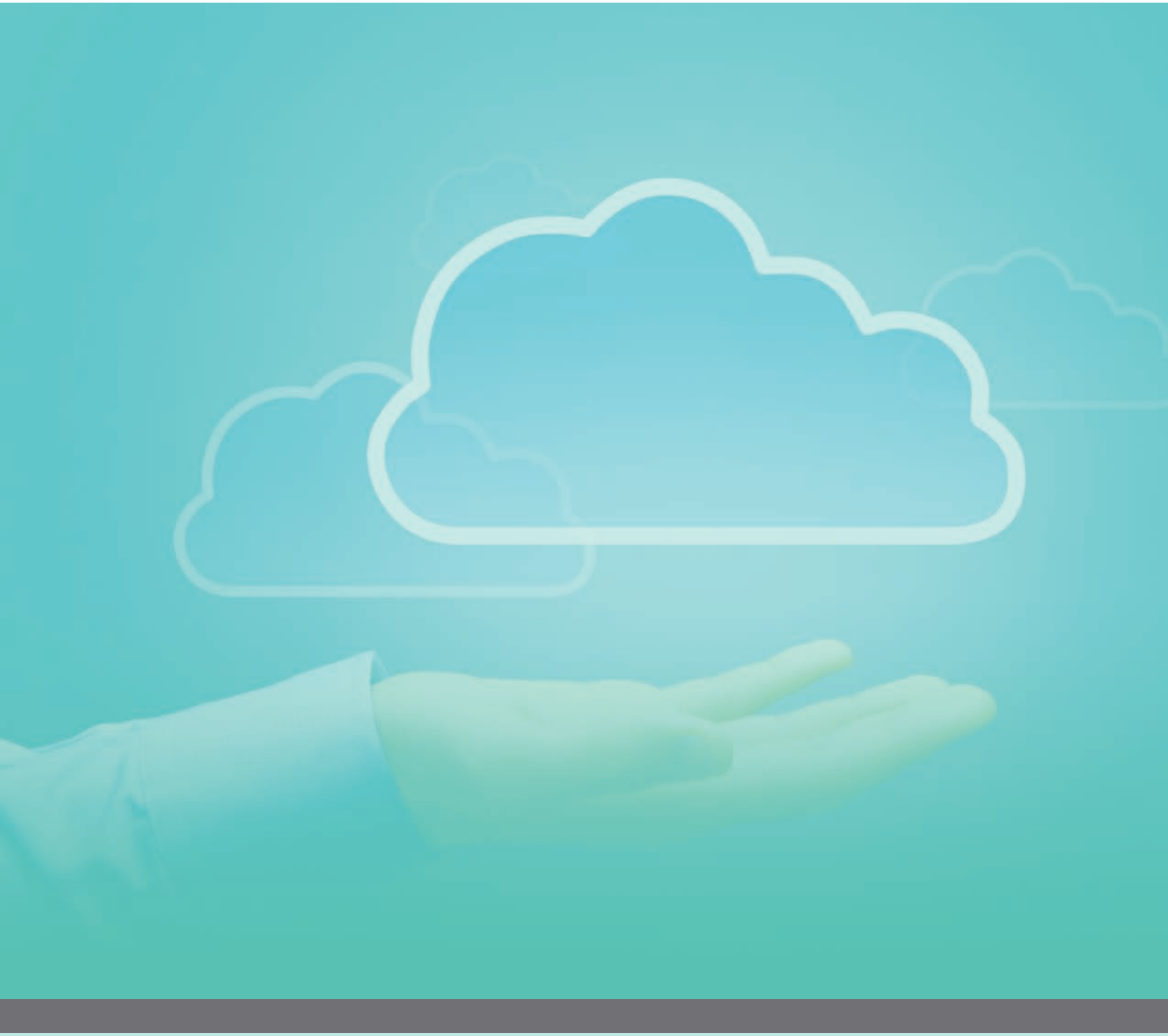
- GIS:
  - Implement next generation solution
  - Consolidation of GIS resources (facilities, budget, and people)

- Establish business transformation initiatives (six)

8.4 LONG-TERM STRATEGIES AND TIMEFRAMES (THREE-FIVE YEARS)

Maturing the model:

- Create the department (Legislative statute).
- Integrate ICSD and all of the new, consolidated initiatives into DoIT.
- Create open data standards.
- Applications:
  - Support application development.
  - Incorporate department legacy application retirement/consolidation/modernization (300).
- Establish identity and credential access management.
- Implement research, development, testing and evaluation.
- Establish business transformation initiatives (12).
- Data Center:
  - Establishment of Data Centers 3-5
  - Consolidation of Data Centers 3-5 resources (NOC, CSOC, Help Desk; facilities, budget, and people)
- Adaptive computing environment:
  - Implement next generation solution
- Network:
  - Implement next generation solution
- Mobile, wireless, and radio:
  - Implement next generation solution
- Shared Services applications:
  - Implement next generation solution
- GIS:
  - Implement next generation solution



9.0 FUNDING CONSIDERATIONS

10.0 CONCLUSION

9.0 FUNDING CONSIDERATIONS

The initiative cannot be implemented without appropriate funding. The funding and budget plans must be designed in an open, collaborative manner that will manage expectations and also allow for the correct timeframes needed to generate and fulfill each funding strategy.

Key funding considerations for the new IT Department:

- Personnel/staffing:
  - Executive management positions
  - Supporting roles
- Professional development/training
- Program initiatives
- Organizational Management program
- Technology and Infrastructure
- Administrative expenditures:
  - Facilities/office space
  - Miscellaneous
- Collective bargaining

10.0 CONCLUSION

The State of Hawaiʻi IT Human Capital Management Strategic Plan was developed through the efforts and input of current and past State of Hawaiʻi stakeholders. Concern was expressed at all levels that, despite the dollars allocated to IT and IT-related activities, the State was not maximizing its use of technology and was not benefitting from IT in terms of productivity improvements, cost savings, effectiveness, or efficiencies to the extent that other state governments, private industry, and the Federal government experience. The inefficiencies and potential risks affecting the business missions of the State of Hawaiʻi clearly identified the criticality of moving forward and establishing a focused, progressive, effective, and agile DoIT.

This Plan has outlined the key areas for reorganizational success and the direction that the next phases will take to further define and implement them. An effective technology platform will launch rewards in all areas of State of Hawaiʻi business that will result in the ultimate goal: better service for the citizens and businesses of the State of Hawaiʻi.

IT ACQUISITION STRATEGIC PLAN

TABLE OF CONTENTS

EXECUTIVE SUMMARY....5

Background....6

Methodology....6

Recommendations....6

Implementation....6

1.0 INTRODUCTION....7

1.1 Purpose....8

1.2 Scope....8

1.2.1 People....9

1.2.2 Policy....9

1.2.3 Process....9

1.2.4 Technology....9

1.2.5 Methodology....9

1.3 Document Overview....9

1.4 Associated Documents....9

2.0 BACKGROUND....10

2.1 IT Acquisition Life Cycle....11

2.1.2 Prioritize....11

2.1.3 Plan....11

2.1.4 Procure....11

2.1.5 Manage....12

2.1.6 Optimize....12

2.2 Current State....12

2.2.1 People....12

2.2.2 Policy....14

2.2.3 Process....16

2.2.4 Technology....17

3.0 BEST PRACTICES....18

3.1 Best Practices....19

3.2 Peer State Review....19

3.2.1 Oregon....20

Roles....20

Policy....20

People....20

Technology....21

3.2.2 Texas....21

Roles....21

Policy 22
People 22
Technology 23
3.2.3 Virginia 23
Roles 23
Policy 24
People 24
Technology 24
3.3 Peer State Comparison 25

4.0 TARGET FUTURE STATE 26

4.1 Call to Action 27
Initiative #1: Establish mechanisms to allow all public entities to benefit from the collective volume of the State 27
Project 1.1: Pilot Optimized Cooperative Purchasing Program for IT Acquisition 27
Project 1.2: Optimize the rule for cross entity contract use 27
Project 1.3: Establish an IT Acquisition Coordinating Committee 28
Initiative #2: Streamline and optimize the State acquisition process 28
Project 2.1: Create a Dedicated Purchasing/Sourcing Group at OIMT 28
Project 2.2: Create a Dedicated IT procurement support group at SPO 28
Project 2.3: Develop an IT Acquisition and Contract Management Guide 28
Project 2.4: Review and update acquisition templates 29
Project 2.5: Automate the creation and processing of Purchase Orders 29
Project 2.6: Review and optimize contract review processes 29
Project 2.7: Prioritize as a foundational project the modernization of state financial and procurement systems 30
Initiative #3: Maximize state purchasing power through a comprehensive IT contract portfolio 30
Project 3.1: Develop and execute on a two year sourcing plan to establish a comprehensive statewide IT contract portfolio 31
Project 3.3: Establish performance measures for state IT contract portfolio and vendors 31
Initiative #4: Establish acquisition review practices that reinforce IT priorities, enterprise architecture and governance 32
Project 4.1: Develop and implement a formal IT strategic planning process that incorporates IT acquisition planning 32
Project 4.2: Develop and implement a Planned Acquisition Schedules process 32
Project 4.3: Develop and implement policy related to CIO review of IT acquisitions 33
Initiative #5: Identify, prioritize and execute on shared service initiatives that create the foundation for success for Hawaii in the decades to come 33
Project 5.1: Develop and execute on a two year sourcing plan to establis a shared services portfolio under the CIO 33

5.0 IMPLEMENTATION STRATEGY 34
5.1 Immediate Strategies and Timeframes (The First Six Months) 35
5.2 Short-term Strategies and Timeframes (Six Months–One Year) 35
5.3 Long-term Strategies and Timeframes (One-Three Years) 35
6.0 FUNDING CONSIDERATIONS 37
7.0 CONCLUSION 37
APPENDIX A: CIO/CPO COORDINATION FACTORS MEMO 39
APPENDIX B: CIO/SPO AGREEMENT 41

LIST OF FIGURES

Figure 1: Key Variables of Acquisition 8
Figure 2: IT Acquisition Life Cycle 11
Figure 3: State Acquisition Organizational Structure 13
Figure 4: Texas Planning, Reporting, and Budgeting Framework 21
Figure 5: eProcurement Maturity Model 30
Figure 6: Reducing Acquisition Effort 30
Figure 7: Transactional vs. Transformational Acquisition 31

LIST OF TABLES

Table 1: Current and Future State Summaries by Architectural Layer 19
Table 2: Peer State Comparison 25

EXECUTIVE SUMMARY

EXECUTIVE SUMMARY

BACKGROUND

The IT Acquisition Strategic Plan identifies discreet and actionable steps to be taken by the State to immediately begin to optimize the management of IT services and programs, including the planning and acquisition process for the State. The ultimate goal is to deliver on the policy direction of state leadership – act to modernize the state technology infrastructure and make Hawaii a model for the nation. The plan identifies an appropriate IT acquisition life cycle model to best meet long term needs of the State for IT acquisitions, one that works in concert with overall state acquisition practices of the State.

METHODOLOGY

The IT Acquisition Strategic Plan has been developed to ensure that four key variables – people, processes, policies and technology – as related to the acquisition of IT goods and services are aligned to provide for an effective and efficient acquisition life cycle model that drives value and outcomes in state technology acquisition initiatives.

To develop the plan, a series of review efforts captured the current state of IT acquisitions for Hawaii. With the current state identified, industry and government best practices, along with the current practices of other states as relates to IT acquisition were examined. Leveraging this work, a set of holistic recommendations were developed to close the gap, culminating in the following plan that provides a prioritized matrix of initiatives and discreet, actionable projects.

RECOMMENDATIONS

For Hawaii to transform and modernize as envisioned by state leadership, there must be a call to action to all levels of government across the islands to come together to implement the following key initiatives:

1. Establish mechanisms to allow all public entities to benefit from the collective volume of the State
2. Optimize the State acquisition process
3. Maximize state purchasing power through a comprehensive IT contract portfolio
4. Establish acquisition review practices that reinforce enterprise architecture and governance
5. Identify, prioritize and execute on shared service initiatives that create the foundation of success for Hawaii in the decades to come

The plan provides an overview of each initiative and a set of discrete, actionable projects to meet the goal of each initiative. The overarching target outcome of these initiatives and projects is to make IT acquisitions put resources to work in a way that is faster, better and cheaper; achieving any one of these outcomes is good, two of them would be great, and all three of them would move Hawaii to first tier in the nation, and that is the goal of this plan.

IMPLEMENTATION

To move the state from the current "As Is" state to the envisioned future state model for IT acquisition, the plan compiles and sequences the recommended projects providing a timetable for implementation of the projects associated with the key initiatives.

1.0 INTRODUCTION

1.0 INTRODUCTION

1.1 PURPOSE

The IT Acquisition Strategic Plan identifies discreet and actionable steps to be taken to address short-term gaps necessary to streamline and optimize the IT acquisition process for the State, and identifies an appropriate IT acquisition life cycle model to best meet long term needs of the State for IT acquisitions. This plan seeks to work within the existing acquisition framework of the State to transform IT acquisition practices wherever practical, and to work in concert with the State Procurement Office in areas of mutual responsibility.

State leadership has stated with high clarity through creation of the CIO office, and legislative directives, the need for expedited implementation of business reengineering and foundational technology initiatives, and specifically establishes intent for an expedited procurement approval process for IT projects that are funded for fiscal year (FY) 2013 as outlined in Act 222.

The purpose of the plan is to establish the strategy regarding the future state of IT acquisition for the State of Hawaii, the operational impact of that strategy, and establish intended outcomes to maximize the outcomes from public funds dedicated to moving the state forward.

1.2 SCOPE

The IT Acquisition Strategic Plan has been developed to ensure that four key variables – people, processes, policies and technology – as related to the acquisition of IT goods and services are appropriately aligned to provide for an effective and efficient acquisition life cycle model that drives the greatest value for IT acquisitions for the State.

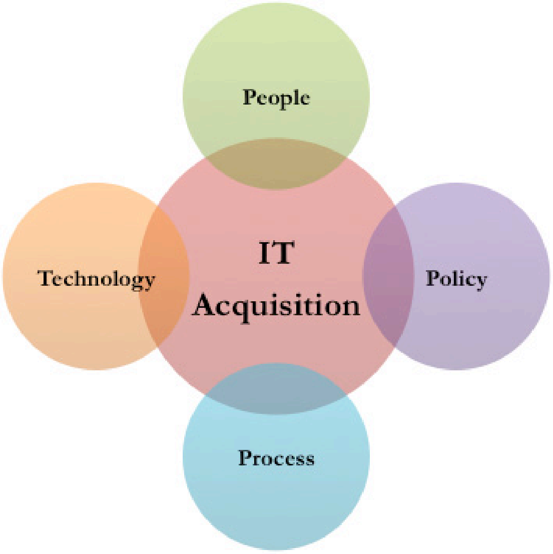


Figure 1: Key Variables of Acquisition

1.2.1 PEOPLE

The roles, organizational structure, and authority of individuals that impact the state function of IT acquisition.

1.2.2 POLICY

The formal policy directing the function of IT acquisition, which is comprised of legislative and statutory direction, formal executive branch direction from the Governor, administrative policy, and other documented requirements that extend administrative policy such as policy circulars, directives and memos.

1.2.3 PROCESS

The prescribed sequence of interdependent activities performed by people to operationalize policy in the function of IT acquisition.

1.2.4 TECHNOLOGY

The use of automated tools and systems to enforce policy and optimize the efficiency of people in their efforts to complete process activities related to IT acquisition.

1.2.5 METHODOLOGY

In order to develop an accurate "As Is" state of IT acquisitions, current policies, procedures, process documentation, and statute related to the IT acquisition process were reviewed. In addition, numerous interviews were held with management and staff at OIMT and the State Procurement Office (SPO), along with members of the IT Acquisition Work Group and other state agency and local government stakeholders. Lastly, the technical infrastructure in place to support the IT acquisition function was assessed.

To support plan development , review of best practices relevant to the current state for Hawaii were examined, along with the current practices of other states as relates to IT acquisition. From this review, an initial target future state model for the State was developed along with initial recommendations. These recommendations and the initial target future state model were presented to many of the same stakeholders from the current state phase of work for comment and feedback.

Lastly, the gap between the current state and the target future state was assessed to identify discreet actionable projects that would help the State to move from the current state to the target future state. This effort culminated in this plan and provides a prioritized matrix of initiatives, and associated projects, to be implemented by the state, including descriptions, policy considerations and possible technology requirements for each initiative.

1.3 DOCUMENT OVERVIEW

The IT Acquisition Strategic Plan describes the outcomes from the work described above, with emphasis on a prioritized matrix of initiatives, and associated projects, to be implemented by the state, including descriptions, cost estimates, associated cost savings and/or process efficiencies, policy considerations and possible technology requirements for each initiative.

1.4 ASSOCIATED DOCUMENTS

- *State of Hawai`i Business and IT/IRM Transformation Plan, September, 2012*
- *Baseline of Information Management and Technology and Comprehensive View of State Services (known hereafter as the "Final Report") prepared by SAIC and State of Hawai'i, September, 2011*

2.0 BACKGROUND

2.0 BACKGROUND

2.1 IT ACQUISITION LIFE CYCLE

For the purposes of this document, the concept of the Acquisition Life Cycle is defined as a process that connects business need with fair and effective methods to acquire goods and services needed to fulfill those needs. Initial stages build best practices to prioritize, plan, and procure goods and services. Vendors and projects are managed to deliver outcomes and meet scope commitments. Individual contracts and the overall contract portfolio are optimized through performance assessments that inform future acquisitions. Figure 2 provides a visual overview of the IT Acquisition Life Cycle and key functions performed in each phase.

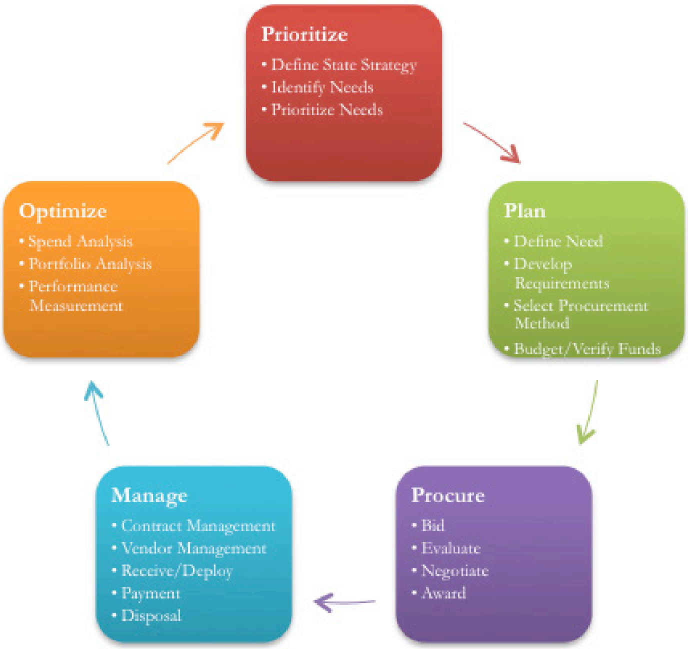


Figure 2: IT Acquisition Life Cycle

2.1.2 PRIORITIZE

The Prioritize phase is a process of establishing broadly applicable strategy and reviewing individual needs to determine alignment with the priorities of the state. From this phase agencies seek to identify priorities for legislative review and approval and eventual inclusion in the state budget, and post appropriation work in coordination with the state CIO to regarding overall timing and sequence of initiatives.

2.1.3 PLAN

The Plan phase is a process of defining the specific need and the appropriate fulfillment method for provisioning the goods or services needed. This phase includes review of state shared services and shared infrastructure alternatives, both existing and scheduled. If necessary for the acquisition method chosen, entities will develop requirements for the goods or services during this phase. The phase also typically encompasses the completion of purchasing processes, such as requisitioning, budget verification and gathering of required approvals, necessary to acquire the goods or services.

2.1.4 PROCURE

The Procure phase is the process of acquiring the needed goods or services through an open, competitive process. To complete this phase entities, working in conjunction with the central procurement authority, will develop a solicitation document, release the document, receive vendor responses, evaluate those responses and complete discussions and or demonstrations necessary to award a contract. Careful attention should be placed in this phase to develop risk mitigation strategies that are appropriate for the services to be procured.

2.1.5 MANAGE

The Manage phase is a process of monitoring and tracking contracts and the associated vendors to be certain requirements and contract terms and conditions are being met, risk mitigation strategies are being reviewed and reconciled, assets management, vendor invoices are correct, and payments to vendors are being made in a timely manner.

2.1.6 OPTIMIZE

The Optimize phase is a process of reviewing outcomes of individual contracted initiatives to assess vendor performance, return for the State and overall determine lessons learned. In addition to individual contract performance reviews, in the optimize phase the overall contract portfolio should be consistently reviewed on a spend category basis to ensure that the state has an appropriately managed contract portfolio in place, to ensure an efficient and competitive process of IT acquisition, with the best possible pricing, product availability, and favorable terms and conditions.

2.2 CURRENT STATE

The following provides a synopsis of relevant factors regarding people, policy, process and technology in regards to the current state of IT acquisition for Hawaii.

2.2.1 PEOPLE

The roles and responsibilities regarding overall State procurement iThe roles and responsibilities regarding overall state procurement is established via Chapter 103D of the Hawaii Revised Statutes (HRS), referred to as The Hawaii Public Procurement Code (HPPC), Part II defines the procurement organization for the State. At the highest level is the Procurement Policy Board, a seven member board that is made up of following members:

- Comptroller;
- A County Employee with significant high-level procurement experience; and,
- 5 members appointed by the Governor.

The Board has the statutory authority and responsibility to adopt rules, consistent with the HPPC, governing the procurement, management, control, and disposal of any and all goods, services, and construction. The Board also has the power to audit and monitor the implementation of its rules and the requirements of the HPPC, but is not able to exercise authority over the award or administration of any particular contract, or over any associated dispute, claim, or litigation.

The HPPC also establishes the State Procurement Office (SPO) and tasks the entity with assisting and advising state governmental entities in matters related to procurement, including the development of:

- A statewide procurement orientation and training program;
- A procurement manual for all state procurement officials; and,
- A procurement guide for vendors wishing to do business with the State.

The statute directs that the administrator of that entity, appointed by the Governor and housed at the Department of Accounting and General Services (DAGS), shall also act as the Chief Procurement Officer (CPO) for the executive branch agencies.

The final layer of the procurement organization for the State is the Chief Procurement Officer (CPO). As defined in the HPPC, Hawaii has broadly delegated authority for procurement to 21 CPO's at all levels of government.

Figure 3 provides an overview of the state acquisition organizational structure. Each orange shaded box represents a statutorily identified CPO for the State.

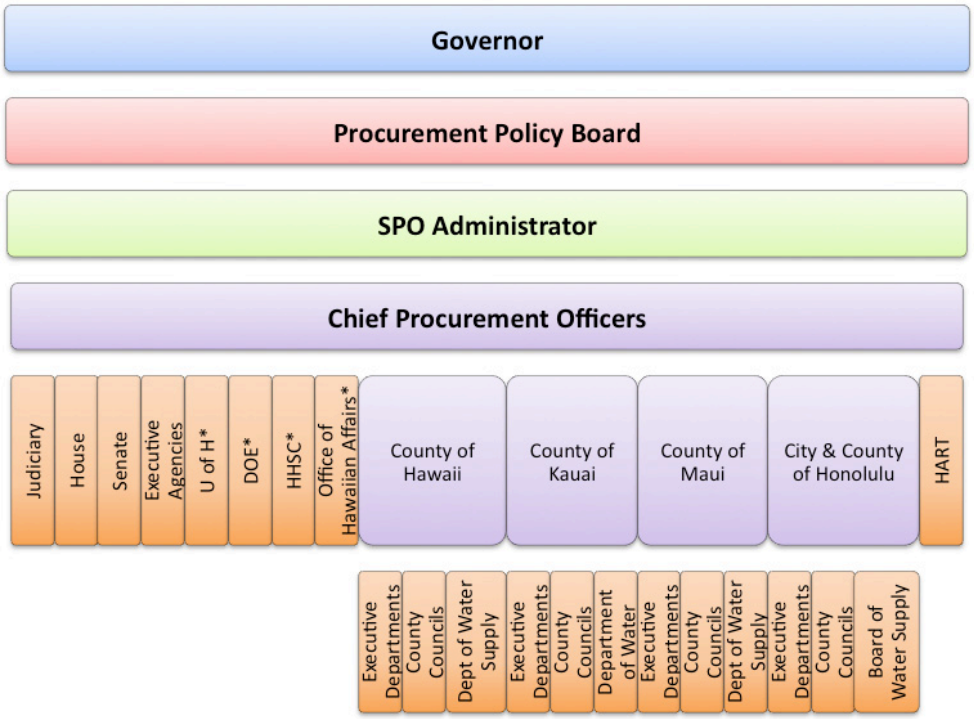


Figure 3: State Acquisition Organizational Structure

*Outside direct purview of the State CIO, who oversees the Executive Branch IT/IRM Only (Act 200)

In 2008, the State faced a significant budget shortfall, and as a consequence of the ensuing cuts in the state budget, the SPO had a significant reduction in force, leading to discontinuance of several projects and staff resources. This reduction led to the SPO restructuring various procurement services, delegating projects and services it was handling on behalf of the executive branch agencies to the executive branch agency administrators, a major shift in acquisition policy and process for the State. The SPO role was refocused to act primarily as a monitoring and oversight entity, with a focus on providing applicable training, while enforcing the ethics and integrity of the procurement process.

The executive branch agency administrators, to whom the procurement responsibilities were delegated, were by and large not prepared to receive it, and did not have the appropriate staff or infrastructure to support the function. Under direction of Department Directors, this led to further delegation of the procurement authority by agency administrators to lower level managers, supervisors and staff in each entity. While there are exceptions within executive branch agencies, in almost all stakeholder interviews it was consistently reported that procurement authority resides with line staff personnel, and is one of many other duties they are required to perform as part of the daily work.

The procurement function is definitely professionalized within SPO and DOE with consistent standards compared to other states. Despite resource cuts and de-centralization of acquisition functions over time, SPO has done a good job in trying to establish and manage a professional IT Acquisition environment with an “equity in process” framework with established-but-rigid acquisition practices.

However, the function of acquisition within the 18 Departments and attached agencies in Hawaii is not professionalized (i.e. career IT acquisition professionals) is a manner consistently found in most other states. The procurement function is not provided centrally as an administrative function of the agency. There is no specified job classification or career path for procurement professionals in agencies.

The SPO has developed and provides training on the procurement process, the training is extensive, can overwhelm line staff tasked with the duty, and is heavily focused on the Procure phase of the Acquisition Life Cycle. Due to a focus that does not extend into planning activities described in the Acquisition Cycle, the training does not address the requisite knowledge necessary to navigate the entirety of processes required to complete acquisitions.

2.2.2 POLICY

Official acquisition policy for the State of Hawaii is broadly dispersed in numerous sources. As an example, the following are the identified sources of policy related to acquisition of goods and services for the State:

- The HPPC (HRS Chapter 103D);
- Hawaii Administrative Rules (HAR), Chapters 3-120 to 3-132;
- Procurement Circulars (87) issued by the Administrator of the SPO to transmit policies, procedures, directions, and instructions;
- Procurement Directives (9) issued by the Procurement Policy Board to transmit the Hawaii Administrative Rules and policies; and,
- Comptroller's Memos (9) issues by the Department of Accounting and General Services.

Due to resource shortages and the highly delegated nature of the procurement function, and the early implementation steps toward a cooperative contracting program, there is a great deal of effort involved in creating multi-entity contracting efforts, and in some cases conflicting policy regarding the establishment of broadly available statewide contracts for use by all state entities. The administrator of the SPO, as CPO for the executive branch agencies, may establish contracts required for the executive branch, and in some cases based on initial participant scope, other entities in the state. While today in Hawaii these are referred to as "statewide" contracts, this definition is inconsistent with how the term is used in other States. Additional governmental entities, including other state governmental entities and any level of political subdivision within the state, must enter into an individual agreement with SPO on each individual Contract.

Cooperative contracting is directed by statute (HPPC, Part VIII). Cooperative contracting is defined as a, "procurement conducted by a public or external procurement unit with one or more public procurement units, external procurement units, or nonprofit private procurement units." SPO issued a MOA to each CPO jurisdiction to amend the current process seeking individual CPAs, providing essentially a 'blanket approval' to use any optional contracts issued by SPO. This recently established process by SPO allows for each CPO jurisdiction to be party to go forward with term contracts through a memorandum of understanding, changing the prior process of requiring each entity to sign an agreement for each individual sourcing event. This is a very positive step.

Aside from the new memorandum of understanding process described above, entities not included in the initial solicitation document are not allowed to utilize the contract.

In this model the lead entity, which can be the SPO or any other delegated agency or CPO, is then responsible for working with all cooperative entities to gather requirements and data for the solicitation – a process which if not managed by procurement and project managers experienced in multi-stakeholder procurements is an arduous task to manage and drive to and effective solicitation. Due to resource shortages resulting in this delegated procurement structure, and complex cooperative contracting processes, the State is challenged in its ability to aggregate statewide volume for the purpose of seeking the best pricing and terms for contracts across all governmental entities.

Further limiting the ability of the State in acquisition is the limitations on the use of cooperative contracting vehicles established outside of Hawaii. The act of the acquiring of goods, services, or construction using another agency contract without prior public notice and intent to participate is often referred to colloquially as "piggybacking" (HAR 3-128, 3-128-2). This rule precludes the use of existing state, federal and cooperative contracts even in circumstances where the initial contract contemplated use by other entities, such as the State. While piggybacking as a process must be carefully managed to allow for fairness in the process, current state interpretation regarding this option precludes the use of contracts established via robust competition where it was clear to the vendor community that the solicitations would be marketed to states, including federal contracts and others established by states or reputable cooperative purchasing programs.

Another key policy [HRS §103D-310(c)] that affects IT acquisition in current state is the requirement for vendors to certify compliance with state laws governing business in the State prior to award. For this process, vendors are required to establish an account on the Hawaii Compliance Express (HCE) system to register for compliance. This system must be used for all acquisitions $2,500 or above. The HCE system is quite capable and won recognition within the National Association of State CIOs (NASCIO) when launched. While important for ascertaining vendor compliance with State and Federal tax and business related financial obligations, the process is viewed as an impediment to doing business with the State, and a deterrent to local, small and minority businesses. Registration with the system requires the payment of a nominal fee, and although automated, the process is described by both vendor and agency stakeholders as inordinately cumbersome and lengthy due to concatenated delays in other departments in the process (e.g., workload in DoTAX may affect priority). As noted, this is generated through state statute, and optimizing this statute based on user experience is a matter that could be considered by state leadership.

In regards to IT acquisition, the recent state restructuring regarding the establishment of a state CIO is in part a result of a desire to be more proactive in the establishments of services than is previous models, in which the state ICSD had been primarily responsible for planning and initiation of IT services and related contracts. Previous models resulted in a limited statewide technology contract portfolio, especially concerning IT services. Contracts that do exist are primarily commodity goods leveraging external contract vehicles, such as hardware and software. Agencies that go to market and achieve success in the contracting process cannot share that success due to piggybacking limitations.

Act 200, the law that recently established OIMT and the position of the State CIO, provided the CIO authority to direct executive branch agencies (excluding certain agencies given special status as indicated in Figure 3, such as University of Hawaii, Department of Education, the Health and Human Service Commission, charter schools, and the Office of Hawaiian Affairs) regarding technology, including a provision requiring review of all IT related procurements. The law also directs the CIO to act in an expedited process regarding addressing several of these issues, and establishing new services in the current fiscal year to improve several of the issues addressed above. In development of this report the CIO and the CPO have established a memorandum of understanding to collaborate to move Hawaii forward on several of these key topics and in support of the change envisioned in this report.

Act 222 provides the CIO with responsibility and authority (in concert with the SPO) to acquire and implement the supplemental budget projects in Fiscal Year (FY) 2013 in an expeditious manner to demonstrate progress and investigate new ways to improve the IT acquisition process. Additional budget execution guidance from the Budget and Finance Director in FY 2013 provides the CIO with the requisite authority to oversee and approve all IT acquisitions in the executive branch of the State of Hawai'i (subject to general provisions in Figure 3).

2.2.3 PROCESS

Acquisition processes in the State are much like those in most states; numerous and hard to navigate without clear direction. Examples of the varying types of procurement processes that must be understood by buyers in the State include:

- Small Purchases
  - Under $5k
  - $5k to $15k
  - $15k to $100k
- Large Purchases
  - Invitation For Bids
  - Request For Proposals
- Sole Source
- Emergency
- Professional Services
- Exemptions

The SPO maintains a helpful web portal (http://www.spo.hawaii.gov/) with access to various procurement policy documents, presentations and forms, which provides a foundation to build on for defining acquisition practices. For administrators with responsibilities that span all aspects of the Acquisition cycle described in Section 2.1, a substantial amount of the synthesis of the various pieces of related policy is left to the agencies to incorporate, and in many cases the interpretation of policy may vary substantively from agency to agency.

Processes preceding the Procure phase in the Acquisition Life Cycle at the State are highly manual. For example, at this time there is a lack of a comprehensive strategic planning process for IT acquisitions that drives transparency into the planned initiatives and projects at agencies, and makes certain they are aligned with IT priorities of the State. Also directly affecting the agency buyers is a highly manual process to initiate the acquisition process that requires the manual completion of a six-part multi-color purchase order form and a non-automated circulation of the form for review and approvals.

Once responses are received, buyers are responsible for completing remaining Procure phase processes and coordinating with various external entities to navigate post-Procure phase processes. The first of these processes is a vendor negotiation process lead by an Attorney General staff assigned to support the agency. These negotiations are often focused on vendor efforts to create exceptions to the State standard terms and conditions. This process is often lengthy and cumbersome because the standard terms and conditions used in solicitations today are more appropriate for non-technical projects, such as construction, and are not contemporary with terms and conditions for the types of goods and services being acquired through IT acquisition.

The lack of a comprehensive contract portfolio, especially in regards to IT services, means that negotiations are frequently required and the effort drives no ongoing residual value due to the lack of an enterprise contracting approach; so each contract interaction retreads and retreads the same ground, agency by agency, political subdivision by political subdivision.

Before a contract can be executed, buyers must submit contract documentation to DAGS for certification, through what is referred to as the Pre-Audit process. This process occurs after all contract processes have been completed, including negotiation and contract signature by all parties, often leading to significant rework, delays and the need for further negotiation of terms or new signatures in cases where issues are raised in the Pre-Audit review.

The overall lack of guidance and direction and time required to complete these complex processes for acquisitions often limits the ability of buyers to expend funds appropriated to the agency in a timely manner. This not only leads to the inability of the agency to meet the policy objectives of the legislature and Governor, but also often leads to the lapsing of appropriated funds.

2.2.4 TECHNOLOGY

Further exacerbating the difficulty of the acquisition process is the lack of automation of key administrative processes such as requisitioning, purchasing approvals, purchase orders, invoice processing and payment. Each of these processes appears to be different at each agency, based on their established administrative hierarchy, and with few exceptions, are entirely manual processes.

An example of these manual processes is the continued use the six-part multi-color purchase order form by numerous state agencies that requires the use of a typewriter or strike printer to complete. The form has apparently been automated by DAGS and has been made available to some state entities, but is either restricted in use or has not been widely available for all agencies to use. In addition, the automation is limited to completion of the form and still requires the form to be printed and distributed for approvals.

The current state financial system either does not support or has not implemented automated tools to support these functions. The SPO maintains a website (http://www.spo.hawaii.gov) that houses policy documents and forms, and allows agencies to post their solicitation documents. The website also provides detailed contract and vendor information, for which it has received national recognition in an emerging category in a recent report by OMB Watch, a non-profit research and advocacy group (http://www.ombwatch.org/upholdingpublictrustreport). This clearly indicates that SPO has achieved recognition and been helpful and transparent despite many resource shortages. Given more resources, automation of acquisition and purchasing processes is a natural next step and evolution of the site into an Enterprise Resource Planning (ERP) system with acquisition management capability.

The SPO website does maintain a link to access the current eProcurement system, HePS. HePS, or the Hawaii eProcurement System, is an outsourced hosted solution that was implemented in 2001 with no upfront capital that provides government entities automation for some elements of the procurement function, including: posting of solicitations; notification of posting to registered vendors; and posting of bid responses by vendors.

The system is required for use by the set of executive branch agencies as described in Figure 3 and is available for use by other government entities in Hawaii. It is used primarily for Small Purchases ($15k to $100k), but can be used for larger acquisitions. Most state entities use it for to open the solicitation up to the largest possible vendor pool and not limit it to only registered vendors in the HePS system. Clearly, the ERP Acquisition module (when implemented) will facilitate additional use and posting of all acquisitions in one integrated system and process.

3.0 BEST PRACTICES

3.0 BEST PRACTICES

3.1 BEST PRACTICES

To identify potential IT acquisition models to be use by the State of Hawaii for a target future state, best practices in the area of acquisition, are where possible IT acquisition specifically, were reviewed. Examples of the research reviewed include research from the following entities:

- Gartner
  - IT sourcing and eProcurement research reports

- National Association of State Procurement Officials (NASPO
  - 2011-12 Survey of State Procurement Practices
  - NASPO Guide to IT Procurement

- American Bar Association
  - ABA Guide to State Procurement

- National Association of State Chief Information Officers (NASCIO)
  - IT Procurement Reform Initiative (in coordination with Tech America and NASPO)
  - 2010 State CIO Survey

- A.T. Kearney
  - 2011 Assessment of Excellence in Procurement Study

- Pew Center for the States
  - States Buying Smarter: Lessons in Purchasing and Contracting from Minnesota and Virginia

- Federal Acquisition Regulation

3.2 PEER STATE REVIEW

Another means of identifying possible models for a target future state for the State of Hawaii is to review to the people, policy, process, and technology of peer states. For the peer state review, efforts were made to choose states that were either similar in nature and organizational structure to Hawaii, or had best practice aspects in IT acquisition. The focus of the review for each state, focused on the following items based on the current state assessment:

- **Policy related to the procurement structure including the roles of the central procurement office and central IT office;**

- **Policies related to cooperative purchasing, and piggybacking;**

- **People and organization related to the procurement, and where applicable IT procurement, functions; and,**

- **Technology utilized in the state to facilitate the acquisition life cycle process. [DAGS/ICSD]**

Table 2 provides an overview of the states reviewed and the reason each state was chosen for the review.

Table 1: Current and Future State Summaries by Architectural Layer

State Reviewed	Significance to Hawai'i
Oregon OSPO website EISPD website	Closest in organization and procurement code to Hawaii. Member of the Western States Contracting Alliance (WSCA).
Texas TPASS website DIR website	A leading state in Cooperative Contracting acquisition. Provides a useful model of IT acquisition strategic planning.
Virginia DGS/eVA website VITA website	Considered a leading state in IT acquisition and organization. Also has deployed a best in state government eProcurement solution.
Michigan DTMB website	Similar in organization to Hawaii regarding acquisition models. Currently in the midst of transforming IT and IT acquisition and acquiring an eProcurement solution.
Minnesota MMD website MN.IT website	Considered a leading state in IT acquisition. Has deployed a best in state government eProcurement solution. Sponsoring state to the IT hardware and software contract for WSCA currently in use by Hawaii.
Georgia DOAS website GTA website	Considered a leading state in acquisition of all types, including IT acquisition. Has deployed a best in state government eProcurement solution. Provides a useful model for IT shared services deployment.

All of these states were reviewed in the research performed for the peer state review; a comparison of all states reviewed is provided in Table 3 in Section 3.3. Three states are spotlighted below for comparative purposes.

It is important to note that states selected were chosen to represent different best practices. These states have more substantive investment of resources, in terms of personnel and technology investment, in the procurement function than does Hawaii. As such the comparisons below are not intended to draw negative comparison to Hawaii, rather to present best practices in action to illustrate what is possible through a combination of optimizing people, policy, process and technology. Additional resources of similar size, scope and caliber would be required for SPO and CIO to compare equitably with these "best practice" and "benchmark" states.

Hawaii is a member of the Western States Contracting Alliance, and maintains close ties with the member states, which are typically considered to be relevant peers. As such the comparison begins with Oregon, perhaps the most highly relevant state for Hawaii comparison overall for reasons noted below.

3.2.1 OREGON

Oregon was chosen to review because it was seen as the closest peer to the State of Hawaii, as it was closest in organization and procurement code to Hawaii. It was also chosen due to it being a member of WSCA, a key cooperative contracting mechanism utilized by the State of Oregon for pricing and vendor lists.

ROLES

Oregon recently updated its procurement code in 2005, utilizing the 2000 American Bar Association (ABA) Model Procurement Code – the same model code utilized by Hawaii for its HPPC. Like Hawaii, Oregon has a highly delegated procurement model. The Oregon State Procurement Office (OSPO) is similar in scope and authority as that in Hawaii, and has the exclusive authority to establish statewide contracts that are broadly available to all state agencies – even though its authority is limited to executive branch agencies. The OSPO can also delegate this ability to agencies, when it benefits the state. The key exception is that the administrator for OSPO is the Chief Procurement Officer for the State.

The central authority for IT for the state is the Enterprise Information Strategy and Policy Division (EISPD). The administrator for EISPD is the State CIO, and is responsible for providing leadership for state government in enterprise information technology management, strategic planning and policy. Like procurement, IT management is highly delegated in the state with CIO's in each state agency. To facilitate coordination and cooperation, the state has established a CIO Council that advises the State CIO and acts as a forum for all agencies to collaborate in the management of IT resources across state government.

Both the OSPO and the EISPD are housed at the Department of Administrative Services (DAS) which facilitates cooperation and coordination in the area of IT procurements. Over the past several years, the Department of Administrative Services (State Procurement Office, Enterprise Information Strategy and Policy Division, State Data Center), Department of Justice, and various state agencies have partnered to put multiple Statewide IT Contracts and Price Agreements in place.

POLICY

Oregon policies related to cooperative purchasing and piggybacking provide an interesting case study. Oregon and Hawaii started with the same model code, and the statutory language relating to cooperative purchasing is nearly identical. The interpretation in Hawaii is vastly different from that Oregon. Instead of requiring agreements on each contract for cooperative purchasing, Oregon has chosen to establish the Oregon Cooperative Procurement Program. This program is open to qualified agencies and organizations as specified in statute, and provides access to:

- State contracts to purchase goods and services;
- Procurement training opportunities;
- Unlimited advertising on the Oregon eProcurement system (ORPIN); and,
- Designated State of Washington contracts through a reciprocal interstate agreement.

State entities meeting the qualifications to be a member of the program complete a program application, and pay a fee, ranging from $50.00 to $5,000.00, based on the entity's annual budget. Entities also complete and sign a participation agreement that sets the terms and conditions for the member services provided by the State.

PEOPLE

OSPO is comprised of the CPO and 39 staff members, which is four times larger than the Hawaii State Procurement Office (SPO), whose scope of responsibility has broader jurisdictional responsibility (i.e. Hawaii SPO encompasses all government jurisdictions, including DOE, UH, the Counties, Judiciary, Legislative Branch, etc.). The OSPO staff is generally organized into major spend categories, including a team of seven (7) staff dedicated to IT procurements. By comparison, Hawaii SPO has a much smaller staff (due to major resource cuts) with a much broader responsibility.

With a substantial delegation of procurement to agencies, most agencies in Oregon establish an administrative services division that includes a dedicated procurement section with dedicated procurement staff. Some larger agencies also have specialized procurement staff focused on IT procurements.

These staff are trained and certified by the OSPO who offers five (5) different certifications and certificates that are based on an employee's role and level of authority for procurement.

They track training and credentials in a credentials database and require certified employees to complete continuing education to maintain their certifications.

TECHNOLOGY

The State of Oregon has an internally developed sourcing tool, Oregon Procurement Information Network (ORPIN), which has been in use since 2005. The current ORPIN provides state entities and cooperative program members the ability to post bids and search existing contracts. In addition it allows vendors to register and receive notifications of current solicitation opportunities.

The State is in the process of implementing ORPIN 2.0 utilizing the SciQuest solution currently under contract with WSCA. The effort began in October, 2011. The state anticipates an autumn 2012 go live implementation timeframe. The first phase is focused on procure to pay backroom processing and catalog support. The next phase of the effort will replace ORPIN. The state of Oregon (and Hawai`i) will be utilizing new functionality available through WSCA – the eMarket Center – to leverage catalogs available through that marketplace for contracts they use.

3.2.2 TEXAS

Texas was chosen to review because it has separated out procurement authority for IT to the State CIO Office and is considered a leading state in the area of IT of cooperative contracting. Both factors provide insight to Hawaii when considering an appropriate future state model.

ROLES

Texas is a large state, with a highly decentralized model of government, which requires a highly delegated model for acquisition in the state. The procurement authority in the state is divided between two entities, segmenting out authority for IT procurement to the State CIO Office.

Authority for state purchasing for non-IT goods and services is the purview of the Texas Procurement and Support Services (TPASS) division of the State Comptroller's Office. TPASS is also responsible for establishing policies and procedures for all statewide acquisition and in that role takes a holistic view of the Acquisition Life Cycle providing training and certification and publishing manuals providing guidance to buyers in all phases the life cycle.

Authority for State purchasing for IT goods and services is the authority of the Texas Department of Information Resources (DIR). The director of this agency is the State CIO and is responsible for statewide leadership and oversight for management of government information and communications technology. DIR has established and manages a statewide IT strategic and procurement planning, reporting and budgeting process.

Over a two-year period in the state DIR and state agencies develop IT strategic plans that are used to develop reports to state leadership and the legislature. The reports help to develop requests for the budget for IT expenditures and enable DIR to have a consistent view of what agencies are buying. In addition, DIR also has authority for review and approval of certain IT procurements, with an established project planning process with review gates for high dollar IT acquisitions.

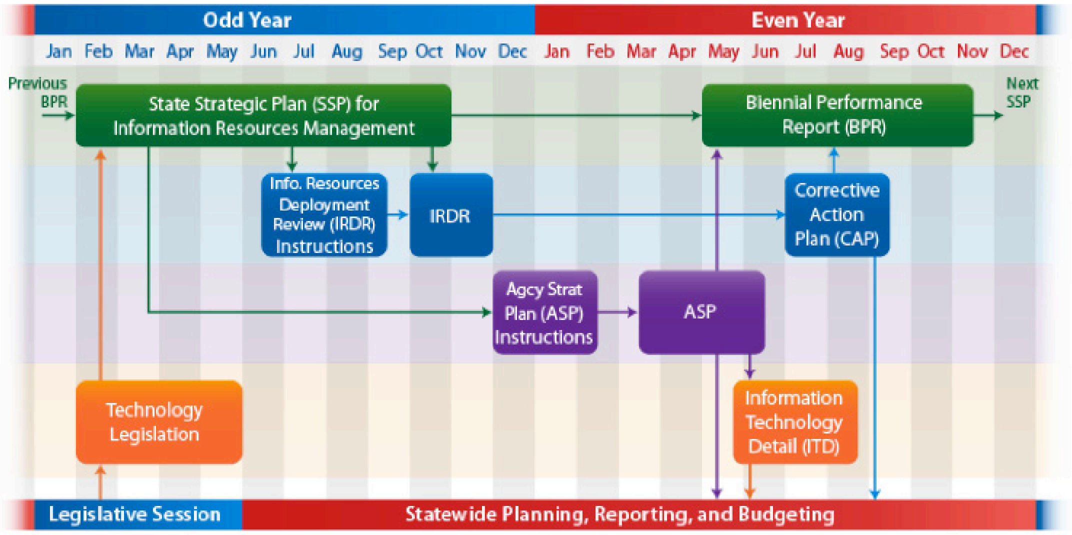

Odd Year
Even Year
Jan Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec
Jan Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec
Previous BPR
State Strategic Plan (SSP) for Information Resources Management
Biennial Performance Report (BPR)
Next SSP
Info. Resources Deployment Review (IRDR) Instructions
IRDR
Corrective Action Plan (CAP)
Agcy Strat Plan (ASP) Instructions
ASP
Technology Legislation
Information Technology Detail (ITD)
Legislative Session
Statewide Planning, Reporting, and Budgeting

Figure 4: Texas Planning, Reporting, and Budgeting Framework

Both the state procurement office and the CIO procurement division are very active central procurement authorities for the state and run highly regarded procurement organizations that provide valuable state contracts to state government and cooperative program members. It should also be noted that with small exception, statewide contracts established by both procurement entities are mandatory use for all executive branch state agencies and permissive use for all other state and cooperative entities.

POLICY

Texas policies related to cooperative purchasing and piggybacking provide comparisons to the State of Hawaii in strategic planning.

Both TPASS and DIR maintain broad cooperative purchasing programs. TPASS manages the Texas CO-OP Purchasing Program, a program that currently has over 1,900 members. The program was established through legislation and stipulated that the following entities are able to be a member:

- Local governments (municipalities, counties, school districts, etc.)
- Special districts
- Mental Health Mental Retardation (MHMR) community centers
- Assistance organizations (non-profits receiving state funds through a current state contract or grant)
- Texas Rising Star Providers (as certified by the Texas Workforce Commission)

To sign up to be a member of the cooperative program, entities complete and submit an application with proof of eligibility along with an annual $100.00 flat fee. Once approved, members have access to the statewide contract portfolio. In addition, members are provided access to automated tools provided by the State to facilitate procurement, including the ability to post solicitations to the state marketplace and access to TxSmartBuy, an e-catalog purchasing system for state commodity contracts.

DIR does not maintain a separate cooperative program. Instead their cooperative program is defined in statute and implemented through use of special contract language. They are provided the authority in statute to include terms in a procurement contract entered into by the agency that allow the contract to be used by:

- Another state agency;
- A political subdivision of the state;
- A governmental entity of another state; or,
- An assistance organization.

Any entity meeting these criteria is able to access the portfolio of contracts managed by the agency.

The state policy related to piggybacking is defined in the Texas Administrative Code (TAC) and stipulates that TPASS is allowed to piggyback on other contracts if it determines that entering into an agreement would be in the best interest of the state. This form of contracting is used sparingly at the state and is often only used when the original solicitation was bid with language that contemplated use by other states. Typically these contracts are developed by state or national cooperative purchasing programs such as U.S. Communities or National IPA.

TPASS has also established a specific program for inclusion of the U.S. General Services Administration (GSA) schedule contracts for use by state and cooperative entities called the Texas Multiple Award Schedule (TXMAS). This program allows vendors with GSA contracts to apply to be included in the TXMAS program, making their GSA schedule contract, pricing and terms available to entities wishing to use the contract.

PEOPLE

Although Texas has a highly delegated procurement model, as noted above it also has highly active central procurement authorities with large contract portfolios. TPASS maintains a staff of 45 full time equivalents (FTE) that are organized into 3 main groups:

- Purchasers (Non-IT goods & services)
- Contract Managers
- Program Managers (HUB, COOP, etc.)

This staff maintains and manages procurement related programs for over 200 state agencies and 1,900 cooperative purchasing entities and a contract portfolio of over 200 state term contract representing several thousand line items of products and services and billions in spend. The division also supports two unique state procurement groups, the Council on Competitive Government and Strategic Sourcing, who have unique and broad procurement authority in the state.

DIR maintains a staff of 30 FTE that are focused on IT procurement that are organized into 4 main groups:

- Enterprise Contracting
- Contract Establishment
- Contract Performance
- Program Analytics

This staff maintains and manages over 750 technology contracts with over $1.3 billion in sales. DIR estimates that through this contracting program they generated more than $171 million in taxpayer savings in FY 2009.

With a broad delegation of procurement authority to agencies, most agencies in Texas establish a dedicated procurement section with dedicated procurement staff. Some of the larger agencies have dedicated IT purchasers within this section. Purchasing is a job classification with a defined career path driven by the level of training and certification one receives. An employee's training level determines what level of procurement authority they are granted.

All staff that perform procurement in the state must be trained through a training program developed and administered by TPASS. TPASS offers two training tracks – Procurement and Contract Management – and three (3) different certifications. They track training and credentials in a credentials database and require certified employees to complete continuing education to maintain their certifications.

All procurement staff in the state must be trained through a training program developed and administered by TPASS. TPASS offers two training tracks, Procurement and Contract Management, and three different certifications. They track training and credentials in a credentials database and require certified employees to complete continuing education to maintain their certifications.

TECHNOLOGY

Texas has several systems in place to support the acquisition processes. The state has a central ERP and financial system that support the administrative purchasing functions such as requisitioning, purchasing approvals, purchase orders, invoice processing and payment.

Outside of the central ERP and financial system, TPASS maintains several automated tools that support procurement and purchasing functions for state agencies and cooperative program members. The state has not implemented a true eProcurement solution, but has over time built automated tools to provide functionality often found in an eProcurement solution. The systems maintained by TPASS include:

- Electronic State Business Daily (ESBD) – a system for posting and managing solicitation opportunities. ESBD is used by all state agencies and some of the cooperative program members. ESBD also provides entities and vendors the ability to search for current posted opportunities using several search functions.
- Central Masters Bidder List (CMBL) – a master database used by State of Texas purchasing entities to develop a mailing list for vendors to receive bids based on the products or services they can provide to the State of Texas. CMBL allows for vendor registration and self-service of their vendor profile and requires that vendors pay an annual registration fee of $70. The system can be searched by vendors to identify small or HUB businesses they may want to partner with.
- TxSmartBuy – a system that provides e-catalogs for state commodity term contracts. TxSmartBuy can be utilized by all state agencies and cooperative program members for state contract searching, side-by-side pricing comparison (if multiple vendors), and order placement. Upon placement of an order the system sends a PO directly to the vendor.

In addition to these systems, TPASS maintains a very thorough and useful website providing links to all of these systems and other relevant information such as state contracts not available for use on TxSmartBuy, the State Procurement Manual, State Contract Management Guide, Training and Certification (including class registration), and other procurement related documents.

Because agencies utilizing DIR contracts use TPASS systems for much of their acquisition processing, DIR has not built and deployed any additional automated tools for procurement. The department maintains a website with a section dedicated to its ICT Cooperative Contracting program that provides users with a catalog of all ICT contracts. The catalog website can be used to search products, services and/or vendors and provides users with detailed information on the contracts, vendors and ordering procedures.

3.2.3 VIRGINIA

Virginia was chosen to review because it has separated out procurement authority for IT to the State CIO Office and is considered a leading state in IT acquisition and organization. Additionally, Virginia has what is considered to be one of the best eProcurement solutions in the nation. Like Texas, the Virginia example provides insight as to possible alternative IT Acquisition operating models any state might consider for the future.

ROLES

Similar to Texas, Virginia employs a procurement organization model that separates procurement authority for IT and non-IT acquisitions. The Department of General Services (DGS), Division of Purchases and Supply is the centralized purchasing agency for non-IT materials, supplies, equipment, printing, and nonprofessional services required by any state agency or institution. In addition to its procurement authority, the division publishes a Procurement Manual that sets policy and process for state agency procurements, establishes standards and specifications for goods and services and maintains eVA, the eProcurement solution for the state.

IT acquisitions are the authority of the Virginia Information Technology Agency (VITA), the State CIO's office. The primary roles of the agency include:

- Governance of the Commonwealth's information security programs;
- Operation of the IT infrastructure, including all related personnel, for the executive branch agencies;
- Governance of IT investments; and,
- Procurement of technology for VITA and on behalf of other state agencies and institutions of higher education.

In addition, the agency supports the Information Technology Advisory Council that is responsible for advising the CIO and the Secretary of Technology on the planning, budgeting, acquiring, using, disposing, managing, and administering of information technology.

POLICY

Virginia does not maintain a special cooperative purchasing program but instead has taken its statutory authority to establish availability of contract to other governmental entities in the state. State contracts must stipulate up front if local entities are authorized to use the contract, and if they do, local entities can utilize the contract; there is no requirement for local entities to enter into an agreement to use the contracts. Similar to Hawaii, agencies can also work together for cooperative purchasing efforts, but there is no formal agreement process required to act in a cooperative manner for acquisitions.

Virginia statute permits piggybacking allowing a government entity to use any contract issued by another governmental entity. The statute stipulates that the original contract must have included language that included and option for other organizations to "ride," "bridge," or "piggyback" the contract as awarded, even if they did not participate in the original solicitation. Policy requires that any entity entering into a piggyback situation, should establish a separate contract and not rely on the piggyback contract, since there is no other legal relationship involved. Both DGS and VITA provide guidance to agencies for how to evaluate piggyback and cooperative contract opportunities for use and strictly controls its use by requiring reviews and approvals.

PEOPLE

With a central procurement authority at both DGS and VITA, both maintain ample staff resources focused on acquisitions. The Department of General Services maintains a significant staff to support the procurement of non-IT goods and services. The specific FTE count could not be determined, but it appears that there over 40 FTE performing direct procurements or supporting the acquisition process and eVA. Specifically, the staff is broken out into the following high-level groups:

- Purchase Management
  - Statewide Contracts and Services
  - Single Agency Contracts Support
- Bid Receipt and Analysis
- Contract Compliance
- Competitive Negotiation
- Training and Development
- eProcurement Bureau (eVA Support)

Within each Purchase Management group, staff is organized into sector managers responsible for managing specific categories of goods or services.

For acquisitions, VITA maintains a staff of 22 FTEs dedicated to IT procurement alone! The staff is broken into groups responsible for Strategic Sourcing and Contract Management. The Strategic Sourcing group is responsible for establishing competitive IT contracts; the Contract Management group is responsible for managing some of the larger contracts to be certain customers are receiving goods and services as stipulated in the contract, and vendor(s) are meeting contract requirements, including reporting to the contract manager.

Like most states, Virginia delegates some procurement authority to state agencies for contracts that are agency specific, or not already contracted for under statewide contracts. Because of this, most agencies establish a dedicated procurement section with dedicated procurement staff. Some of the larger agencies have dedicated IT purchasers within this section. Purchasing is a job classification in the state with and defined career path driven by the level of training and certification you have received. An employee's training level determines what level of procurement authority they are granted.

All staff that perform procurements in the state must be trained through a training program developed and administered by DGS through their Virginia Institute of Procurement (VIP). There are two certifications offered, requiring completion of a three-day or seven-day training program with testing. The certification required is based on the employees role and purchasing authority at the agency. They track training and credentials in a credentials database and require certified employees to complete ongoing continuing education to maintain their certifications.

TECHNOLOGY

Virginia has deployed what is considered to be one of the most robust eProcurement solutions in state government to date. "eVA", Virginia's online, electronic procurement system is a central tool for accessing all statewide contracts, including DGS and VITA contracts, that provides users with:

- Support for purchasing processes from requisition to receipt of goods;
- Support for procurement processes from bid to award;
- Hosted and punch-out catalogs;
- Vendor registration and acceptance of state Terms & Conditions;
- Purchasing Data Warehouse and a BI solution for spend analytics and performance management; and,
- Procurement related documentation and training.

In addition to being used by state entities, eVA is available for full implementation and use by local governments at no cost. Since implementation, eVA has processed over three million orders and $31 billion in spend and is estimated to save the state over $300 million annually in process efficiencies and reduced costs of goods and services. The system currently supports nearly 1,000 online catalogs, 171 agencies, 575 localities, over 53,000 vendors and over 22,000 users.

3.3 PEER STATE COMPARISON

Table 3 below provides a comparison of all the states reviewed in the research for the peer state review for specific components of research that are potentially pertinent in considering an appropriate future IT Acquisition model for the State of Hawai`i.

Table 2: Peer State Comparison

State	IT Acquisition at CIO Office	IT Acquisition in SPO	Cooperative Purchasing Program	Allows for Piggybacking	Deployed eProcurement*	IT Shared Services Offered	Procurement Manual	Procurement Templates	IT Acquisition Strategic Planning Process	IT Acquisition Coordinating Committee
Oregon		●	●	●	●					
Texas	●		●	●	●	●	●	●	●	●
Virginia	●		●	●	●	●	●	●	●	●
Michigan		●	●	●	●					
Minnesota		●	●	●	●	●	●	●	●	●
Georgia	●		●	●	●		●	●	●	

* Michigan is currently in the process of evaluating responses to an eProcurement solution solicitation.

4.0 TARGET FUTURE STATE

4.0 TARGET FUTURE STATE

4.1 CALL TO ACTION

4.1 Call to Action

For Hawaii to transform and modernize as envisioned by state leadership, there must be a call to action to actively implement the following key initiatives:

1. Establish mechanisms to allow all public entities to benefit from the collective volume of the State
2. Optimize the State acquisition process
3. Maximize state purchasing power through a comprehensive IT contract portfolio
4. Establish acquisition review practices that reinforce enterprise architecture and governance
5. Identify, prioritize and execute on shared service initiatives that create the foundation of success for Hawaii in the decades to come

The following sections provide an overview of each initiative and a set of discreet, actionable projects to meet the goal of each initiative. The overarching goal of these initiatives and projects in the long run is to optimize IT acquisitions by making them faster, better and cheaper; if we are to meet any one of these goals – good, two of them – great, all three of them – fantastic.

INITIATIVE 1: ESTABLISH MECHANISMS TO ALLOW ALL PUBLIC ENTITIES TO BENEFIT FROM THE COLLECTIVE VOLUME OF THE STATE

Hawaii statute allows for cooperative purchasing, and recent policy changes to allow for a standing memorandum of understanding to participate in go forward sourcing events is an important step to implementing this capability. As an island state, Hawaii has unique considerations regarding issues such as supplier diversity, product availability, and redundancy to name a few. Limitations on the ability for collective action that are not imposed in other states should be rethought and optimized. The state's new process should be fully implemented and communicated, and practices of other states in the management of cooperative contracting programs should be reviewed in order to determine the most optimize the process once it is put into practice.

PROJECT 1.1: PILOT OPTIMIZED COOPERATIVE PURCHASING PROGRAM FOR IT ACQUISITION

to build a way forward. The IT acquisition arena provides an ideal environment to test additional best practices of other states, including:

- A simple membership application for interested entities to use to apply for membership to the program and to collaborate on future purchasing needs;
- A one-time agreement for each member to enter into, that mimics the current cooperative agreement form used;
- Rules, as necessary, to establish the program and define eligible entities that can be members of the program; and,
- If a nominal fee should be charged for membership (if statutory allowed) to help support administration, marketing and training regarding the program.

PROJECT 1.2: OPTIMIZE THE RULE FOR CROSS ENTITY CONTRACT USE

Although piggybacking in the long term is not as effective as other means of contracting, the current inability to consider the use of this contracting method, given the gaps in the current contracting portfolio, is a detriment to the State. It is recommended the State revaluate HAR 3-128, Sec. 3-128-2, and amend it to enable piggybacking in limited situations where contracts have incorporated language anticipating the use of the contract by another state or governmental entity. The CIO and CPO should work together with the goal that the high majority (80%) of purchasing should still go through state-competed contract portfolio, or through alliance-competed contracts to which Hawaii is a party (such as WSCA). As complement to this state based procurement, the State should allow for the use of the following contracts (for the remaining 20% as required):

- Federal contracts and GSA Schedule contracts;
- Other state contracts bid with published piggybacking provisions; and,
- Other cooperative contracts that were competitively bid with piggybacking provisions

To provide assurances that piggybacking is appropriately leveraged, the State should establish a defined process that requires submission for approval with an analysis of contracting method, pricing and terms prior to entering into the contract. It should be noted that if a cooperative contracting program is established in the state, it will greatly eliminate many of the issues related to piggybacking.

PROJECT 1.3: ESTABLISH AN IT ACQUISITION COORDINATING COMMITTEE

To seek collective acquisition opportunities in IT acquisitions, OIMT should establish an IT Acquisition Coordinating Committee that meets regularly to discuss IT acquisition needs amongst key stakeholders and representative entities and with OIMT management and staff. The committee can also be an excellent forum for identifying problems or issues that have an impact across agency lines. To be sure to include all state entities in this committee it may be wise to establish multiple subcommittees for large agencies, small agencies and/or local government. It is recommended that the State use the State Agency Coordinating Committee in Texas or the CIO Council in Virginia as models for structure and organization of this committee.

INITIATIVE #2: OPTIMIZE THE STATE ACQUISITION PROCESS

Hawaii currently has a lengthy, resource intensive and manual process for acquiring goods and services. Much of this has been brought about by resource cuts to SPO (and other agencies), and the resulting delegation of authority to Agencies, who do not have the appropriate staff, support infrastructure or technology supporting the process to effectively and efficiently spend state budget funds to meet the policy objectives of the legislature and state leadership. To align with acquisition processes of other states, Hawaii must identify and implement opportunities to optimize processes in the Acquisition Life Cycle. Hawaii must consider adding critical resources and consolidating functions in the IT Acquisitions lifecycle within the SPO and OIMT.

PROJECT 2.1: CREATE A DEDICATED PURCHASING/ SOURCING GROUP AT OIMT

Although this project should ideally be a statewide effort, in an effort to establish the necessary support infrastructure to meet the legislative mandate for IT acquisitions in the current FY, it is recommended that OIMT move immediately to create a dedicated purchasing/sourcing capacity. Responsibilities that need to be addressed include:

- Complete required purchasing processes to acquire IT goods and services for OIMT;
- Identify needs and develop requirements for statewide IT contracts;
- Manage statewide IT contracts in a category manager approach; and,
- Provide assistance and guidance as SMEs for other non-statewide IT acquisitions.

Given the scope of work and the aggressive timelines, this requires an IT Procurement Manager and six to eight additional sourcing analyst resources, with the following core skillsets:

- Procurement and strategic sourcing;
- IT shared services procurements;
- Spend analytics and performance management;
- Business process reengineering; and,
- Contract management.

This dedicated sourcing group will not only enable OIMT deliver on the short-term directives of the legislature and Governor, but will also provide OIMT with the ability to execute on longer-term efforts toward establishing a comprehensive statewide contract portfolio for IT goods, services, and shared services that are critical to the State. The CIO should be resourced at a scale similar to other leading states in IT Acquisitions.

PROJECT 2.2: CREATE A DEDICATED IT PROCUREMENT SUPPORT GROUP AT SPO

For the same reasons OIMT should implement a sourcing planning group at the agency, it is highly recommended that SPO would add a dedicated IT procurement support resources. These resources should be tasked to assist OIMT in a buyer capacity in the procurement of statewide IT goods and services and assist agencies and other governmental entities in utilization of state IT contracts. At a minimum, this should include be a couple of dedicated resources in the short term, potentially adding more resources as an additional supplement once the two year bid schedule described below is completed. The SPO should be resourced at a scale similar to other leading states in IT Acquisitions.

PROJECT 2.3: DEVELOP AN IT ACQUISITION AND CONTRACT MANAGEMENT GUIDE

Due to special requirements for IT acquisitions and the need to provide specialized guidance to buyers, it is recommended that OIMT develop an IT Acquisition and Contract Management Guide. The Guide should be a single authoritative source for the entirety of the Acquisition Life Cycle processes (prioritize, plan, procure, manage and optimize) for IT acquisitions and should seek to compile, in an easy to follow way, all state policies and processes. The goal of the document should be to translate the policy to process – "can do"/"can't do" into "should do"/"how to." The guide should include a process flow chart to assist buyers in all process steps required to complete a purchase and should reflect all the different acquisition process, including all special and exception processes and special practices related to IT acquisitions. Additionally, as projects outlined in this plan related to IT acquisition planning and governance are implemented, these processes should be incorporated into the Guide as well.

PROJECT 2.4: REVIEW AND UPDATE ACQUISITION TEMPLATES

The goal of this initiative is to make the work of the buyer more effective and efficient. One means of helping buyers be more efficient is to provide them with tools that minimize the level of effort required to complete the process. One tool set that is especially helpful in the Acquisition Life Cycle is templates that provide direction and structure to the work.

It is recommended that the State identify, catalog and prioritize the review, and update and/or development of acquisition related document templates to facilitate the acquisition process. Examples of templates that could be created by the State include, but are not limited to:

- RFP Template for IT Goods and Services
- IFB Template for IT Goods and Services
- Standard Terms and Conditions for IT Goods
- Standard Terms and Conditions for IT Services
- IT Special Terms & Conditions
  - Hardware
  - Software
  - Services
  - Maintenance

These templates, if built and designed properly, will help the buyer to navigate the acquisition processes and make sure that necessary steps are completed that limit rework.

PROJECT 2.5: AUTOMATE THE CREATION AND PROCESSING OF PURCHASE ORDERS

Although the implementation of Project 2.7 below will address the underlying concerns driving the need for this project, the implementation of an eProcurement solution is a long-term solution. The manual processing of purchase is a current concern that may be addressed through implementation of a short-term fix while efforts are progressing to a longer-term solution. As such, it is recommended that the State do a short term assessment of automation of the creation and processing of purchase orders.

In review of the current state it was noted that DAGS had developed a tool for creation and completion of the purchase order form. The broad use of the tool was not evident, as numerous stakeholders noted frustration with the completion of the six-part NCR purchase order form that required the use of a typewriter to complete.

Deployment of an ERP Acquisition Module will address this issue in the long run, but in the short-term, the State should seek to eliminate use of the 6-part forms and rapidly assess the ability to deploy a uniform solution for creation and completion of Purchase Orders for use by all agencies. This assessment should consider the viability of the use of available short term options as a potential solution, and should seek to incorporate an automated workflow process for reviews and approvals of the Purchase Order as well.

Deployment of a solution will to lead to efficiencies in the creation and completion of the Purchase Order and eliminate unneeded costs associated with the use of the six-part form and the antiquated equipment required to complete it.

Deployment of an ERP or eProcurement solution will address this issue in the long run, but in the short term, the State should seek to eliminate use of the six-part form and rapidly assess the ability to deploy a uniform solution for creation and completion of purchase orders for use by all agencies. This assessment should consider the viability of the use of available short-term options as a potential solution, and should seek to incorporate an automated workflow process for reviews and approvals of the purchase order as well.

Deployment of a solution will to lead to efficiencies in the creation and completion of the purchase order and eliminate unneeded costs associated with the use of the six-part form and the antiquated equipment required to complete it.

PROJECT 2.6: REVIEW AND OPTIMIZE CONTRACT REVIEW PROCESSES

In the review of current state, stakeholders regularly expressed their frustration with processes that followed the identification of a successful vendor in evaluations. These processes included development of terms and conditions, contract execution, vendor compliance and contract pre-audit.

It is recommended that the State review these processes and seek to identify opportunities for process reengineering and optimization. This project should include developing clear guidance to buyers for each process for incorporation into the Procurement Guide identified in Project 2.3 above. Examples of specific issues raised in these processes that should be reviewed included:

- Attorney General State standard terms and conditions;
- DAGS pre-audit and encumbrance process;
- Contract execution and signature requirements;
- Use of e-signatures for contracts;
- Vendor compliance via use of the Hawaii compliance Express (HCE) system; and,
- Prompt payment of vendors.

PROJECT 2.7: PRIORITIZE AS A FOUNDATIONAL PROJECT THE MODERNIZATION OF STATE FINANCIAL AND PROCUREMENT SYSTEMS

The majority of the inefficiencies in the acquisition life cycle in Hawaii stem from the lack of deployed automated systems to support the acquisition processes. As such it is recommended that the State immediately prioritize as a foundational project the deployment of modern automated systems that support the acquisition process, including the modernization of the state financial and procurement systems. As part of this project, the State should consider the migration of HePS into a more complete ERP Acquisition module solution.

The state is in the early stages of development of a business case and functional requirements for an Enterprise Resource Planning (ERP) solution. A key component of this ERP solution is the incorporation of Acquisition as a line of business, either as a module from an ERP system, or leveraging one of several options for integrating a stand-alone eProcurement or eAcquisition system. ERP is often a significant deployment effort and because of the focus on ERP as a state financial system of record, procurement or acquisition is often not an initial module to be deployed. In its ERP business case, the state should assess both options, the deployment of eProcurement as a component of ERP or as a separate system, to determine which is best suited to meeting the needs of the State.

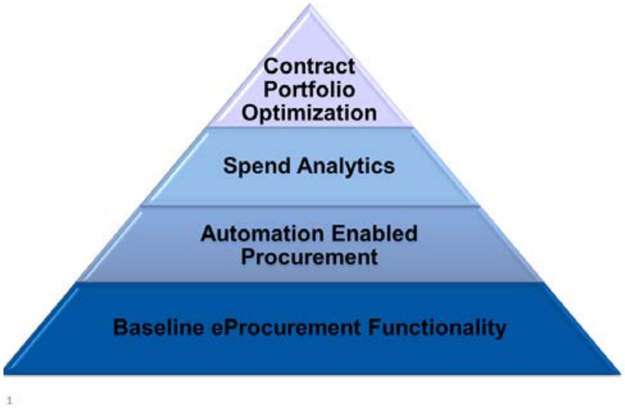

Contract Portfolio Optimization
Spend Analytics
Automation Enabled Procurement
Baseline eProcurement Functionality
1

Figure 5: eProcurement Maturity Model

Figure 5 provides an overview of an eProcurement Maturity Model that represents the value that an eProcurement solution can provide to the organization and the role it may play in a target future state. In developing a business case and functional requirements for an eProcurement solution the State should seek to deploy a solution that, at a minimum, seeks to deploy the first two levels of maturity with a long-term vision of implementing a solution that reaches the remaining levels of maturity in the model.

In doing this, the State can implement a solution that automates acquisition processes and uses technology to enforce the acquisition policies and rules of the State. Some of this functionality may be provided directly in an eProcurement solution, or it may be incorporated in the ERP solution and integrated with the eProcurement solution in a way that provides seamless end-to-end processing.

INITIATIVE #3: MAXIMIZE STATE PURCHASING POWER THROUGH A COMPREHENSIVE IT CONTRACT PORTFOLIO

Another means of making the acquisition process effective and efficient, and helping buyers to expediently acquire the goods and services they require, is to establish a comprehensive portfolio of broadly available statewide contracts. A well designed portfolio of contracts should seek to maximize state spend under management which allows buyer to:

- Acquire needed goods and services in an expedited manner by not having to solicit for every need; and,
- Focus acquisition efforts on unique or more complex agency specific needs.

Figure 6 below provides an overview of the impact the implementation of this initiative will have on reducing the acquisition effort of buyers at the State. Today the State performs a substantial amount of acquisition initiatives “from scratch,” i.e. starting in effect with a blank piece of paper. The middle line demonstrates what impact the implementation of Project 2.4 above would have on the process, providing buyers with templates and tools to expedite the acquisition process. With a broad statewide IT contract portfolio in place, buyers are able to focus on development of a statement of work, an accelerated determination process, and the ability to execute a purchase against an already solicited, negotiated and awarded contract set.

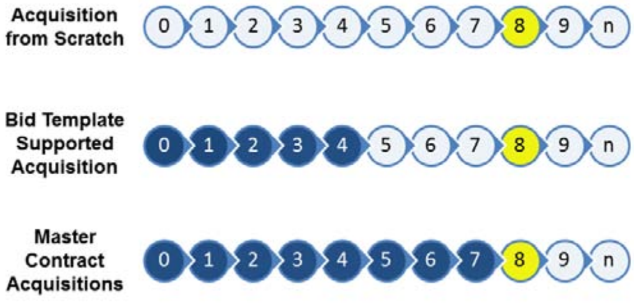

Acquisition from Scratch
0
1
2
3
4
5
6
7
8
9
n
Bid Template Supported Acquisition
0
1
2
3
4
5
6
7
8
9
n
Master Contract Acquisitions
0
1
2
3
4
5
6
7
8
9
n

Figure 6: Reducing Acquisition Effort

Transitioning the acquisition focus from "Acquisition from Scratch" to utilizing master contracts for goods and services that can be commoditized has two major positive impacts. For low complexity contracting areas, a comprehensive program of vendor contracts and state driven term contracts puts a substantial portion of the state spend under management. It also frees up the resources needed to pursue the large requirement based bids that provide an opportunity to transform the state, and emphasizes those as a professional discipline. This shift over time creates appropriate emphasis on both transactional acquisitions, and transformational acquisitions. These concepts are presented as a model in Figure 7.

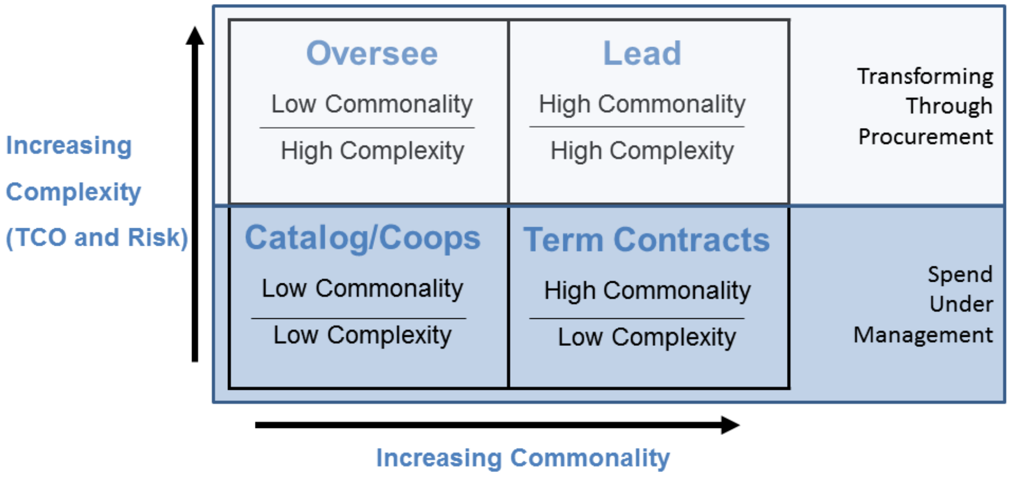


Figure 7: Transactional vs. Transformational Acquisition

PROJECT 3.1: DEVELOP AND EXECUTE ON A TWO YEAR SOURCING PLAN TO ESTABLISH A COMPREHENSIVE STATEWIDE IT CONTRACT PORTFOLIO

Before the State can establish a comprehensive statewide IT contract portfolio, it must identify contracting gaps and prioritize these opportunities. It is recommended that the State, lead by the CIO and OIMT, develop a two year sourcing plan to establish a comprehensive statewide IT contract portfolio and then work diligently to execute against the plan.

The first step in developing a comprehensive IT contract portfolio is to review the current IT contract portfolio at the State and determine what gaps exist. To accomplish this in the current environment the State will need to analyze existing statewide and agency IT contracts, vendor reports for existing contracts, and overall IT spend for the State.

With this information the contract gaps can be identified, and with the help of state leadership and key stakeholders, contracting opportunities identified can be prioritized toward the development of a prioritized two year sourcing plan to execute against. Focus for the two year plan should be on identifying contracting opportunities that maximize spend under management (see Figure 7) for IT goods and services.

Contracts should be solicited to allow for use by all state government entities, and non-state entities, to allow for the greatest aggregation of volume to drive the best pricing and terms for the State. Contracts should also be fully negotiated and have fixed contract terms and conditions to eliminate the need for renegotiation at each purchase against the contract. Because these contracts will be used for the procurement of IT infrastructure at the State, they must support the goals of OIMT for state IT standards and architecture and be mandatory use for executive branch agencies (with exclusions noted in Figure 3) under the newly created authority of the CIO.

PROJECT 3.3 ESTABLISH PERFORMANCE MEASURES FOR STATE IT CONTRACT PORTFOLIO AND VENDORS

The establishment of a comprehensive contract portfolio, while a major step forward for the State, is not enough on its own. In the longer-term, the State must be able to measure the performance of the contract portfolio to know if the portfolio is:

1. Meeting the needs of the buyers;
2. The right mix of contracts;
3. Competitively priced in the market; and,
4. Meeting the policy objectives of the state.

Examples of the performance measures the State should seek to track and monitor include, but are not limited to:

- Efficiencies driven through establishment of contract portfolio
  - How much is going through the contracts?
  - How much time to complete purchases on existing contracts?
  - How much time to complete steps in the procurement process?

- Quality of the contract portfolio
  - How well is the contract portfolio meeting the needs of state entities?
  - Do we have the right contracts?
  - Is the pricing on the contracts competitive with other available options?
- How do we enforce state policy through our contracting efforts?
  - Are we contracting with small business, minority business, local business, etc.?
  - How often do entities go off-contract or do special procurements?
  - Are we getting multiple valuable responses to bids?

With this information the State will be able to identify spend patterns, procurement patterns, perform comparative benchmarking and track performance of the contracts and vendors under contract in a way that enables them to make management decisions on the contract portfolio.

INITIATIVE #4: ESTABLISH ACQUISITION REVIEW PRACTICES THAT REINFORCE IT PRIORITIES, ENTERPRISE ARCHITECTURE AND GOVERNANCE

OIMT is establishing a governance and portfolio management process that will ensure that all acquisitions of information technology are reviewed to be in compliance with the Enterprise Architecture (EA). There are three tiers of reviews:

- **Tier 1:** Minor Acquisitions (<$100,000) – Reviewed by OIMT for compliance with priorities, EA, and security and privacy. Acquisitions in full compliance will be approved by CIO.

- **Tier 2**: Medium Acquisitions ($100,000 – $1,000,000) or non-compliant Minor Acquisitions – Reviewed and approved by CIO Council.

- **Tier 3:** Large Acquisitions (>$1,000,000) – Reviewed and recommended for approval by CIO Council, approved by Executive Leadership Council.

The EA establishes the standards and patterns for the envisioned future state of the State's business and IT/IRM environment. The EA reflects the priorities established in the IT Strategic Plan. Because mission, business, and technology needs and capabilities can change, proposed acquisitions that deviate from the established EA may be approved on a case-by-case basis. The EA will be updated to reflect the new information, and will also be updated periodically in consultation with the CIO Council and Executive Leadership Council.

It is important to note that the B&F Director (de facto CFO), CIO, Comptroller and CPO of the State of Hawai`i have no visibility as to the actual expenditures or associated breakout for enterprise IT with requisite detail and business intelligence/analytics. Consequently, there is no ability to mitigate duplication of effort, explore synergy opportunities, verify alignment with business needs, and realize cost efficiency and mission effectiveness on an enterprise scale. This situation needs an urgent fix.

PROJECT 4.1: DEVELOP AND IMPLEMENT A FORMAL IT STRATEGIC PLANNING PROCESS THAT INCORPORATES IT ACQUISITION PLANNING

In order for the State CIO to have transparency into the planned initiatives and projects at agencies, and to make certain they are aligned with IT priorities of the State it is recommended that the State establish a formal IT strategic planning process that incorporates IT acquisition planning as a key component of the process.

The strategic planning process should at minimum include the development of the following:

- State IT Strategic Plan that establishes the IT roadmap and priorities for the State;
- Agency IT Strategic Plans that identifies anticipated technology initiatives of the agency and speaks to how the initiatives align with the priorities established in the State Strategic Plan; and,
- Call for Projects that identifies anticipated agency IT projects for the coming biennium.

It is recommended that each strategic planning component be performed in a recurring manner on an established schedule that aligns with and facilitates the budget planning process. To be effective the process must not be obtrusive and complicated for agencies to complete and as such templates for the completion of each component should be developed that delineate the required information agencies must provide and that are simple and easy to complete and submit. Where agencies are already completing strategic plans, the IT strategic plan can simply be incorporated into the larger strategic plan.

PROJECT 4.2: DEVELOP AND IMPLEMENT A PLANNED ACQUISITION SCHEDULES PROCESS

To help the State CIO and OIMT stay abreast of the anticipated needs of the agencies for IT goods and services it is recommended that the State develop and implement a Planned Acquisition Schedule process. The Planned Acquisition Schedule is a rolling 12 month forecast of technology purchases that is updated on regular intervals always with a 12 month view. This process is valuable in helping provide the State CIO with a comprehensive view of overall IT needs of the State that enables the State CIO to determine the need for spend category prioritization and project contract portfolio reach.

Like the IT strategic planning process, to be effective the process must not be obtrusive and complicated for agencies.

As such the process should require agencies to provide the minimum level of information necessary to gain a comprehensive view of anticipated IT acquisitions. Additionally, templates for the schedule should be developed and provided to agencies that delineate the required information agencies must provide and that are simple and easy to complete and submit.

Like the IT strategic planning process, an effective process must not be obtrusive and complicated for agencies. The process should require agencies to provide the minimum level of information necessary to gain a comprehensive view of anticipated IT acquisitions. Additionally, templates for the schedule should be developed and provided to agencies that are simple and easy to complete and submit and delineate the required information they must provide.

PROJECT 4.3: DEVELOP AND IMPLEMENT POLICY RELATED TO CIO REVIEW OF IT ACQUISITIONS

Current policy requires that the State CIO review and approve certain IT acquisitions of executive branch agencies. To make certain this process is efficient and effective and meeting the policy objectives of the State, it is recommended that the State CIO develop and implement policy related to the review of IT Acquisitions. The policy should set expectations and timelines for agencies and should seek to highly constrain and eliminate emergency reviews.

Once enterprise architecture standards are established and supported through a comprehensive statewide contract portfolio, the process should also create pathways for agencies to bypass review for acquisitions using the contract portfolio or meeting established standards.

INITIATIVE #5: IDENTIFY, PRIORITIZE AND EXECUTE ON SHARED SERVICE INITIATIVES THAT CREATE THE FOUNDATION FOR SUCCESS FOR HAWAII IN THE DECADES TO COME

While Initiative 3 sought to establish a comprehensive contract portfolio of IT contracts for the state, those contracts are focused on addressing the standard IT goods and services needs of state entities. However, there are certain areas in IT where the whole is greater than the sum of the parts – referred to as shared services.

A shared service is the consolidation and provision of a common service by a central state entity that is utilized by other state entities. In this model, redundancy of resources and expenditures across state entities is eliminated and replaced with a model where funding and resourcing for the service is shared across state entities with the providing department effectively becomes an internal service provider.

To elevate the IT organization, it is recommended that the State begin efforts to identify and prioritize opportunities for shared services and execute to establish these shared services for the State under the auspices of the State CIO and OIMT. Implementing this initiative will move the State into the modern area of technology service delivery and create a foundation for success for Hawaii for decades to come.

PROJECT 5.1: DEVELOP AND EXECUTE ON A TWO YEAR SOURCING PLAN TO ESTABLISH A SHARED SERVICES PORTFOLIO UNDER THE CIO

Before the State can implement shared services, it must identify where shared services opportunities exist at the State. Toward that end, it is recommended that the State CIO and OIMT work with state leadership and state and local stakeholders to identify and prioritize shared services opportunities toward the development of a two year sourcing plan to execute against.

Examples of shared services areas the State should consider include, but are not limited to:

- Data Center Services
- Cloud Services
- Telecommunication (Landline and Wireless)
- Networking
- ERP
- Enterprise Email
- Data Warehousing/Business Intelligence and Logistics
- GIS data and systems

5.0 IMPLEMENTATION STRATEGY

5.0 IMPLEMENTATION STRATEGY

The following tables compile and sequence the project work described in the Section 4.0 providing a timetable for implementation of the projects associated with the key initiatives required move the state from the current "As Is" state to the envisioned future state model for IT acquisition.

5.1 IMMEDIATE STRATEGIES AND TIMEFRAMES (THE FIRST SIX MONTHS)

Project No.	Project
1.1	Pilot optimized cooperative purchasing program for IT acquisition.
1.2	Optimize the rule for cross-entity contract use.
2.1a	Create a dedicated purchasing/sourcing group at OIMT.
2.2	Create a dedicated IT procurement support group at SPO.
2.7	Prioritize, as a foundational project, the modernization of state financial and procurement systems.
3.1a	Develop a two-year sourcing plan to establish a comprehensive statewide IT contract portfolio.

5.2 SHORT-TERM STRATEGIES AND TIMEFRAMES (SIX MONTHS—ONE YEAR)

Project No.	Project
3.1b	Execute on the two- year sourcing plan to establish a comprehensive statewide IT contract portfolio.
5.1a	Develop a two-year sourcing plan to establish a shared services portfolio under the CIO.
2.3	Develop an IT Acquisition and Contract Management Guide.
2.4	Review and update acquisition templates.
2.5	Automate the creation and processing of purchase orders.
2.6	Review and optimize contract review processes.

5.3 LONG-TERM STRATEGIES AND TIMEFRAMES (ONE-THREE YEARS)

Project No.	Project
5.1b	Execute on the two-year sourcing plan to establish a shared services portfolio under the CIO.
1.3	Establish an IT Acquisition Coordinating Committee.
4.1	Develop and implement a formal IT strategic planning process that incorporates IT acquisition planning.
4.2	Develop and implement a Planned Acquisition Schedules process.
4.3	Develop and implement policy related to CIO review of IT acquisitions.
3.2	Establish performance measures for State IT contract portfolio and vendors.
2.1b	Create dedicated purchasing/sourcing groups at state agencies
N/A	Work with SPO on a detailed assessment of State acquisition policy and process.[1]

[1] This project is not specifically identified in the plan as the plan was focused on IT acquisition only, but is a project the State should seek to implement in the long-term.

		Year 1				Year 2				Year 3			
Project #	Project Name	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	Q12
1.1	Pilot Optimized Cooperative Purchasing Program for IT Acquisition	■											
1.2	Optimize the rule for cross entity contract use	■											
1.3	Establish an IT Acquisition Coordinating Committee					■	■						
2.1a	Create a dedicated purchasing/sourcing group at OIMT	■	■										
2.1b	Create dedicated purchasing/sourcing groups at state agencies												
2.2	Create a dedicated IT procurement support group at SPO	■	■										
2.3	Develop an IT Acquisition and Contract Management Guide			■	■								
2.4	Review and update acquisition templates			■	■								
2.5	Automate the creation and processing of Purchase Orders			■	■								
2.6	Review and optimize contract review processes			■	■								
2.7	Prioritize as a foundational project the modernization of state financial and procurement systems	■											
3.1a	Develop a two year sourcing plan to establish a comprehensive statewide IT contract portfolio	■	■										
3.1b	Execute on the two year sourcing plan to establish a comprehensive statewide IT contract portfolio			■	■	■	■	■	■	■	■		
3.2	Establish performance measures for state IT contract portfolio and vendors									■	■		
4.1	Develop and implement a formal IT strategic planning process that incorporates IT acquisition planning									■	■	■	■
4.2	Develop and implement a Planned Acquisition Schedules process									■	■	■	■
4.3	Develop and implement policy related to CIO review of IT acquisitions									■	■	■	■
5.1a	Develop a two year sourcing plan to establish a shared services portfolio under the CIO			■	■								
5.1b	Execute on the two year sourcing plan to establish a shared services portfolio under the CIO					■	■	■	■	■	■	■	■
6.1	Work with SPO on a detailed assessment of State acquisition policy and process[1]					■	■						

6.0 FUNDING CONSIDERATIONS

7.0 CONCLUSION

6.0 FUNDING CONSIDERATIONS

Many of the projects that are outlined in the plan, while requiring personnel resources to execute do not require significant outlays of funds to implement as they are business process reengineering efforts. While typical methods of funding projects outlined in this plan would be general revenue funds or bonding mechanisms, the State has an available funding mechanism is has not yet implemented related to procurement – administrative fees.

Administrative fees are fees that are assessed and paid to the State on statewide contracts. They are meant to generate revenue for the State to offset costs associated with administrative function of procurement, but in this case could also be used for costs associated with the reengineering efforts and technology deployments such as eProcurement and/or ERP. Administrative fees can be applied in several approaches to include:

- Fee paid by vendors based on total purchases with the vendor;
- Fee paid by vendor based on dollar value of the purchase order (with caps); or,
- Fee paid by the agency based on dollar value of the purchase order.

The majority of states use some sort of administrative fee to support the central procurement function and the IT procurement function (where applicable). The most common approach seen in states is to assess a vendor fee in either of the first two models outlined above. Vendors are then able to factor this into their pricing and build it into the bid responses provided to the State for contracts where the fee will be applied. In some cases the fee is sent directly to the state and simply retained as part of general revenue, in other cases it is directed to the procurement entity and in yet others it is some combination of the two. In all cases, it derives significant revenue to the State.

To be an effective revenue source for the State, the fee must be both reasonable and defensible. To meet both criteria the fee must not be excessive such that it deters vendors from wanting to do business with the state or causes unacceptable cost models for agencies, and should be based on an analysis of current and future revenue needs so as not to be viewed as a cash cow.

7.0 CONCLUSION

This plan represents a call to action to move Hawaii to be a model for the nation in IT acquisition strategy, and the work begins today. *Mahalo.*

APPENDIX A: CIO/CPO COORDINATION FACTORS MEMO

APPENDIX A: CIO/CPO COORDINATION FACTORS MEMO

KEY CIO-CPO COORDINATION FACTORS

Statement of Understanding Related to Technology Procurement in Hawai'i

CPO has the statutory authority to establish statewide contracts:

- Statewide is defined as the Executive Branch agencies
- Any additional entities – even if the contract is established by CPO – must be specified in the document under the administrative policy regarding "piggybacking"
- Agencies may establish co-operative contracts, but only within and among named parties
- Agencies have an option to request that SPO lead a statewide contract (Form SPO-018)
- • CPO indicated there would be scenarios where they would be willing to designate an agency to lead a statewide contracting effort – in effect, enable the statewide contracting authority to be led by an agency with a specific expertise if it advanced the state goals and purpose

CIO has the authority to direct Executive Branch agencies regarding technology:

- Oversees statewide information technology governance
- Develops, implements, and manages statewide information technology governance
- Develops, implements, and manages the state technology strategic plans
- Develops and implements statewide technology standards
- Legislation pending signature indicates that foundational elements of the technology strategic plan "must" be implemented in 2012-2013
- The same legislation described expedited procurement regarding these initiatives as "essential"

Technology direction is within the designated authority of the CIO, yet making true change in technology strategy and vendor behavior requires statewide contracting:

- With individual agency technology acquisition, success in one agency's T&C's/price/scope/etc. does not translate to any other agency's success
- Hawaii, with its unique characteristics, has an clear need for a coordinated technology vendor management strategy
- Coordinated vendor management strategy can only happen with buying strategy supported by enterprise architecture and new shared service offerings.
- The limitations described above (including piggybacking limitations) mean that technology contracts should be established with broad scope from the beginning to benefit as many agencies as possible as architecture converges

CIO and CPO can coordinate their authority and areas of expertise in a way that powers the future state technology strategy:

- CIO should have the subject matter expertise and resource base to develop, and coordinate a contract portfolio comprising the technology spend of the state
- CIO bid development should reinforce state acquisition policy
- CPO should coordinate with the CIO to release solicitations under the authority of the CPO in order to make them statewide contracts
- CIO should be responsible for the outreach necessary to interested parties outside of the executive branch consistent with state piggybacking policy
- • Recent examples of this type of collaboration: State Portal Contract and Network Equipment

APPENDIX B: CIO/SPO AGREEMENT

APPENDIX B: CIO/SPO AGREEMENT

AGREEMENT OF RESPONSIBILITY BETWEEN
State Procurement Office
and
Office of Information Management and Technology
Regarding the
Planning, Design, Procurement and Contract Management
of
Information Technology Goods and Services

August 2012

The **Primary (P)** entity is responsible for initiating and completing the tasking.
The **Secondary (S)** entity is responsible for assisting the effort.

PLANNING, DESIGN, SOLICITATION DEVELOPMENT

Activities	Reference	Responsible Entity Primary (P)/Secondary (S)		Approximate Completion Period
		OIMT	SPO	
General				
Overview/background		P		TBD by OIMT
Goals and objectives		P		TBD by OIMT
Obtaining all applicable approvals		P		TBD by OIMT
Operational IT standards		P		TBD by OIMT
Scope of Services /project configuration, systems design, integration & interoperability specifications		P		TBD by OIMT
Service prioritization		P		TBD by OIMT
Geographic location(s) involved		P		TBD by OIMT
Insurance requirements	DAGS, Risk Mgmt.	P		TBD by OIMT
Request for information (RFI), as applicable	HAR §3-122-9.02	S Provide SPO RFI details/content, review RFI responses and incorporate into procurement, as applicable	P Release RFI and receive responses	TBD by OIMT
Hardware, software, services				
Lease vs. purchase		P		TBD by OIMT
Product description, functional specifications		P		TBD by OIMT
Technical capabilities		P		TBD by OIMT
Software licenses		P		TBD by OIMT
Warranty information for service		P		TBD by OIMT
Maintenance requirements (annual maintenance cost)		P		TBD by OIMT
Installation requirements		P		TBD by OIMT
Consultant services		P		TBD by OIMT

PLANNING, DESIGN, SOLICITATION DEVELOPMENT

Activities	Reference	Responsible Entity Primary (P)/Secondary (S)		Approximate Completion Period
		OIMT	SPO	
Offeror qualifications				
License(s), experience, references, training, education, etc., as applicable		P		TBD by OIMT
Facilities,as applicable		P		TBD by OIMT
Location of contractor(s) office(s)		P		TBD by OIMT
Construction, if applicable (coordinate with DAGS-PWD)				
Plans/designs, building renovation, electrical, A/C, permits, contractor licenses		P Coordinate with DAGS/PWD		TBD by OIMT
Capital Improvement Projects (CIP) authorizations/allotments	HRS §103-7	P		Varies
Coordination of services				
Deliverables and installation requirements/timelines		P		TBD by OIMT
Trade-in or disposal of obsolete assets; applicable approvals		P		TBD by OIMT
Contractual responsibilities				
Department				
• Monitoring, measuring, and assessing contractor performance		P		TBD by OIMT
• Other responsibilities		P		TBD by OIMT
Contractor				
• Performance outcome, expectation measurements		P		TBD by OIMT
• Other responsibilities		P		TBD by OIMT

PLANNING, DESIGN, SOLICITATION DEVELOPMENT

Activities	Reference	Responsible Entity Primary (P)/Secondary (S)		Approximate Completion Period
		OIMT	SPO	
Procurement Requirements **OIMT to coordinate procurement requirements with SPO**		Coordinate with SPO		1-2 weeks SPO to coordinate with OIMT
Method of procurement determination • Competitive sealed bidding (IFB) • Competitive sealed proposals (RFP) • Professional services • Small purchase • Sole source • Emergency	HRS §103D-301 HAR §3-122-16	S	P	
Timeline: Release of solicitation; offer/proposal submittal deadline, contract execution, notice to proceed	HAR chapter 3-122 subchapters 5 and 6	S	P	
Determination of type of contract, i.e., fixed-price, cost-reimbursement, cost incentive, performance incentive, time and materials, labor hour, quantity, installment	HAR §3-122-135	S	P	
Single or multiple awards, and the basis of the awards	HAR §§3-122-145 and 3-122-146	S	P	
Term of contract, including extension periods	HAR §3-122-7 HAR chapter 125	S	P	
Provisions for early termination and renewals	HAR §§3-125-21 and 3-122-7	S	P	
Encumbered or open-ended contract	HAR §3-122-102	S	P	
Method of payment: e.g., unit rate, fee for service, deliverables/milestones	HRS §103D-309 HAR §§3-122-21 and 3-122-46	S	P	
Allowable contract price adjustments	HAR §3-125-2	S	P	
Bid security, contract performance bond, payment bond, as applicable	HAR chapter 3-122 subchapter 24	S	P	
Preferences, i.e., software development, tax preference	HAR chapter 3-124	S	P	
Public Procurement Notice	HAR §3-122-16.03		P	
Pre-bid/pre-proposal conference schedule, as applicable	HAR §3-122-16.05	S	P	

PLANNING, DESIGN, SOLICITATION DEVELOPMENT

Activities	Reference	Responsible Entity Primary (P)/Secondary (S)		Approximate Completion Period
		OIMT	SPO	
Competitive Sealed Proposals				
• Evaluation committee selection	HAR §3-122-45.01	P		2-3 weeks
• Basis of evaluation	HAR §3-122-52	P		
• Proposal evaluation criteria w/assigned points	HAR §3-122-52	P		

PROCUREMENT PERIOD (FROM POSTING OF PROCUREMENT PUBLIC NOTICE)

Activities	Reference	Responsible Entity Primary (P)/Secondary (S)		Approximate Completion Period
		OIMT	SPO	
Competitive Sealed Bidding				
Procurement public notice released	HAR §3-122-16.03		P	• Min. 10 days (single step) • Min. 15 days for 1st phase and 10 days for 2nd phase (multi-step)
Pre-bid conference, as applicable	HAR §3-122-16.05	S	P	Sufficient time before to allow offerors to review solicitation and sufficient time after to prepare offer
Addenda issued, as needed • Responses to questions • Changes to specifications, scope of work, provisions	HAR §3-122-16.06	S	P	Sufficient time before submittal deadline for offeror(s) to prepare proposal
Receipt, opening and recording of offers	HAR §3-122-30		P	1-2 days
Evaluation of offers	HAR §3-122-33	S	P	Varies
Award of contract	HAR §3-122-33		P	Varies
Posting of award	Procurement Circular 2010-01	P		Within 7 days from notice of award

PROCUREMENT PERIOD (FROM POSTING OF PROCUREMENT PUBLIC NOTICE)

Activities	Reference	Responsible Entity Primary (P)/Secondary (S)		Approximate Completion Period
		OIMT	SPO	
Competitive Sealed Proposals				
Procurement notice released	HAR §3-122-16.03		P	Min. 30 calendar days
Pre-proposal conference, as applicable	HAR §3-122-16.05	S	P	Sufficient time before to allow offeror(s) to review solicitation and sufficient time after to prepare offer
Addenda issued, as needed : • Responses to questions • Changes to specifications, scope of work, provisions • Best and Final Offer (BAFO), as applicable	HAR §3-122-16.06	S	P	Sufficient time before submittal deadline for offerer(s) to prepare proposal
Receipt and registration of proposals	HAR §3-122-51		P	1-2 days
Proposal evaluation by evaluation committee, based on established RFP criteria • Offeror interviews/product demonstrations/site visits, as applicable	HAR §3-122-52	P		Depending on procurement complexity and number of proposals received - Average 1 month
Discussion with offeror(s), as needed	HAR §3-122-53	S	P	Varies
Best and final offers, as needed	HAR §3-122-54	S	P	2 weeks
Award of contract	HAR §3-122-57		P	Varies
Posting of award	Procurement Circular 2010-01		P	Within 7 days from notice of award
Debriefing, upon request by offeror	HAR §3-122-60	S	P	Average 1 week after completion of evaluations (within 7 days)

PROCUREMENT PERIOD (FROM POSTING OF PROCUREMENT PUBLIC NOTICE)

Activities	Reference	Responsible Entity Primary (P)/Secondary (S)		Approximate Completion Period
		OIMT	SPO	
Protest				
Protest prior to receipt of offers	HAR §3-126-3	S	P	Varies
Protest of award	HAR §3-126-4	S	P	Filing of protest: within 5 working days after posting of Notice of Award
Procurement Officer written decision on protest	HAR §3-126-7	S	P	As soon as possible
Protest Appeal - Department of Commerce and Consumer Affairs, Office of Administrative Hearings (DCCA-OAH)	HAR chapter 3-126, subchapter 5	DCCA-OAH		Filing request for hearing within 7 calendar days

CONTRACT EXECUTION, MANAGEMENT, AND PAYMENT

Activities	Departments and Agencies Involved with the Process of Contracting with the State	Approximate Completion Period
Contract Processing		
Draft contract review by Deputy Attorney General	Office of the Attorney General	Varies
Contract term discussions with potential contractor(s)	OIMT	Varies
Contract Execution		
• By Contractor(s)	Contractor	5 weeks
• By Office of the Attorney General (approval as to form)	Office of the Attorney General	
• By SPO Procurement Officer (PO)	SPO	
Certification/encumbrance for IFB/RFP/Sole Source; forms (A-47, C-41, transmittal to DAGS, Pre Audit)	OIMT/SPO HRS §103D-309	Varies

CONTRACT EXECUTION, MANAGEMENT, AND PAYMENT

Activities	Departments and Agencies Involved with the Process of Contracting with the State	Approximate Completion Period
Contract Period		
Inventory		
• Assign inventory tags to equipment	OIMT and DAGS, Inventory Mgmt.	Term of contract
• Enter equipment into inventory system	OIMT and DAGS, Inventory Mgmt.	Term of contract
Contract Payment	OIMT and Department of Accounting and General Services	Term of contract
Contract Administration	OIMT	Continuous
Contract Management	OIMT/SPO	Term of contract
Contract Performance and Fiscal Monitoring	OIMT	Term of contract
Contract Performance and Fiscal Evaluation	OIMT	Term of contract
Contract Amendments/Extensions	OIMT/SPO	Term of contract
Responsible for the compliance with HRS chapter 103D, Hawai'i Procurement Code	SPO	Continuous
Promulgates the Hawai'i Administrative Rules (HAR) and issues Procurement Directives, as required	Procurement Policy Board (PPB) HRS chapter 103D	As required
Disclosure of government records	Office of Information Practices (OIP) and PO - HRS chapter 92F	As required
Requires applicable code of ethics for government employees and officers	State Ethics Commission and Purchasing Agency HRS chapter 84	As required
Contracting Requirements		
Verification prior to award and upon final payment on Hawai'i Compliance Express (HCE) to obtain Certificate of Vendor Compliance for: • Internal Revenue Service (IRS), • Department of Taxation (DOTAX), • Department of Labor and Industrial Relations (DLIR), and • Department of Commerce and Consumer Affairs (DCCA)	SPO HRS §103D-310(c)	Required upon award of contract
Obtain Certificate of Insurance, as applicable	SPO	Within 10 days to execute contract
Obtain bid/performance/payment bonds, as applicable (required for construction)	SPO HRS §103D-324	Within 10 days to execute contract

OTHER RELATED ADMINISTRATIVE REQUIREMENTS

Activities	Responsible Entity	Approximate Completion Period
Executive memorandums available at http://hawaii.gov/budget/, includes Budget Execution Policies requiring the Governor's approvals for expending funds Administrative Directives available at: http://hawaii.gov/budget/administrative-directives/	Office of the Governor	Continuous
Finance memorandums available at http://hawaii.gov/budget/, includes B&F requirements	Department of Budget and Finance (B&F)	Continuous
Comptroller memorandums available at http://hawaii.gov/dags/cm, such as: • Certificate of Insurance (Ref. CM 2010-39) on contractor's insurance policies • Contract Execution Date (Ref. CM 2009-14) for retroactive contracts approval • Personal Services Contractor Procedural Manual • Pre-Audit review/approval request for payment processing/vouchering	Department of Accounting and General Services	Continuous
Chief Information Officer (CIO) approval for design and implementation of IT infrastructure, IRM, and shared services pursuant to AD 11-02	OIMT	Continuous

OTHER RELATED ADMINISTRATIVE REQUIREMENTS

Activities	Responsible Entity	Approximate Completion Period
Contract forms; contract approval as to form: • AG-002 Contract for Goods and Services Exempt, Small Purchase, Sole Source, or Emergency • AG-003 Contract for Goods or Services Based Upon Invitation for Competitive Sealed Bids • AG-004 Contract for Goods or Services Based Upon Request for Competitive Sealed Proposal • AG-005 Supplemental Contract • AG-008 General Conditions • AG-009 Contractor's Acknowledgement • AG-010 Contractor's Standards of Conduct Declaration • AG-011 Attachment – S1, Scope of Services • AG-012 Attachment – S2, Compensation and Payment Schedule • AG-013 Attachment – S3, Time of Performance • AG-014 Attachment – S4, Certificate of Exemption from Civil Service • AG-015 Attachment – S5, Special Conditions • AG-016 Attachment – S6, Supplemental Special Conditions	Office of the Attorney General (AG)	Continuous

AARON S. FUJIOKA **Date**
Administrator and Chief Procurement Officer
State Procurement Office

SANJEEV BHAGOWALIA **Date**
Chief Information Officer
Office of Information Management & Technology

INFORMATION ASSURANCE AND CYBER SECURITY STRATEGIC PLAN

CONTENTS

1 EXECUTIVE SUMMARY....6

2 INTRODUCTION....8

2.1 Background....9

2.2 Current and Emerging Cyber Security Threats....9

2.2.1 Outlook for 2013-2015....10

2.2.2 Counterintelligence....10

2.3 Scope.... 10

2.4 Alignments.... 11

2.5 IA and CS Program Management Plan.... 11

2.6 Purpose and Benefits.... 11

3 FUNDAMENTALS OF INFORMATION ASSURANCE RISK MANAGEMENT.... 13

3.1 Basic Elements of the Risk Assessment Process....16

3.2 Establish Relationships....17

3.3 Develop Statewide Categorization Guidance....17

3.4 Identifying Types of Risks....17

3.5 Risk Categories....18

3.6 Current Risk Assessment Methodologies....19

3.6.1 Qualitative Method....19

3.6.2 Quantitative Method....20

3.7 Alternative Risk Assessment Methods....21

3.7.1 Probabilistic Risk Assessment (PRA)....21

3.7.2 Forensic Analysis of Risks in Enterprise Systems (FARES)....22

3.8 Challenges Assessing Information Security Risks....22

4 STRATEGIC INFORMATION ASSURANCE AND CYBER SECURITY GOALS AND OBJECTIVES....29

5 PERSPECTIVE ON INFORMATION ASSURANCE....32

5.1 Commitment....34

5.1.1 Department Heads and CIOs....34

5.1.2 Directors, Chairs, Managers, and Other Supervisors....34

5.1.3 Chief Information Security Officer (CISO)....34

5.2 Communication Plan....36

5.3 Resource Management....36

5.4 Measuring Quality Effectiveness....36

6 INFORMATION ASSURANCE AND CYBER SECURITY DIVISION....36

6.1 Garner Respect and Resources....37

6.2 Demonstrate Top Management Support....37

6.3 Establish Formal Communication Channels....37

6.4 Foster Coordinated Team Effort to Safeguard Information....37

6.5 Enable Better Allocation of Organizational Resources....38

6.6 Minimize Associated Costs for Security as a Service (SecaaS)....38

6.7 Reduce Single Point of Failure 38
6.8 Demonstrate Compliance 38
6.9 Increase Efficiency and Productivity 39
6.10 Cyber Security Controls Branch (CSCB) 40
6.11 Compliance, Auditing, and Policy Branch (CAPB) 40
6.12 Identity and Access Management Branch (IAMB) 40
6.12.1 Public Key Infrastructure-Certificate Management Services (PKI-CMS) 41
6.13 Security Operations Monitoring Branch (SOMB) 42
6.13.1 Deliver Situational Awareness 42
6.13.2 Meet Business Operations Requirements 42
6.13.3 Reduce Risk and Downtime 42
6.13.4 Threat Control and Prevention 43
6.13.5 Ease Administrative Overhead 43
6.13.6 People and Responsibilities 43
6.13.7 Escalation Path 43
6.13.8 Audit and Compliance Support 43
6.13.9 Incident Response and Recovery 44
6.13.10 Meet Technical Operations Requirements 44
6.13.11 Speed of Aggregation and Correlation 44
6.13.12 Device and System Coverage 44
6.13.13 Proactive Infrastructure Monitoring 44
6.13.14 Uptime 24/7, 365 Days of the Year 44
6.13.15 Support for Federated and Distributed Environments 44
6.13.16 Forensic Capabilities 44
6.13.17 Intelligent Integration with SOCs and NOCs 45
6.13.18 The SOC in Action 45
6.13.19 Multiple Security Operations Centers 46
6.13.20 Privileged Access Monitoring 46
6.14 State of Hawai`i Data Privacy Program 46
7 STRATEGIC PLAN ASSUMPTIONS 47
8 CONSTRAINTS 48
9 INFORMATION ASSURANCE AND CYBER SECURITY INITIATIVES 49
10 GUIDANCE FOR PROGRAM MANAGERS AND PROJECT LEADS 49
11 CONCLUDING REMARKS 50
APPENDIX A - INFORMATION ASSURANCE AND CYBER SECURITY PROGRAM STRATEGIC INVESTMENT INITIATIVES 51
CONTRIBUTORS 51
SOURCES 51

FIGURES

Figure 1 - CIO's IT/IRM Transformation Vision 11

Figure 2 - Security Life Cycle 14

Figure 3 - Risk Management Cycle 16

Figure 4 - Impact Assessment of Various Incidents to Enterprise 20

Figure 5 - Elements of Information Assurance and Cyber Security (Parkerian Hexad) 24

Figure 6 - Security Implementation Strategy Based on Importance vs. Complexity 25

Figure 7 - Information Assurance and Cyber Security Capability Maturity Model with Example Security Controls 28

Figure 8 - Information Assurance Branch Roadmap 29

Figure 9 - CIO Top Information Assurance and Cyber Security Concerns (2011) 33

Figure 10 - Recommended Information Assurance and Cyber Security Division Organization 39

Figure 11 - Notional Shared Services Center Vision for Hawai`i 46

TABLES

Table 1 - Security Controls Classes, Families, and Identifiers 15
Table 2 - Identified Risks 18
Table 3 - Differences in Methodologies 19
Table 4- Impact/Likelihood of Impact to the Enterprise Matrix 19
Table 5 - Factors in Risk Analysis Equation 21
Table 6 - Example Risk Analysis Table 21
Table 7 - CISSP 10 Domains of Information Assurance 23
Table 8 - Categories of Security Controls Related to Information Assurance 26
Table 9 - Maturity Levels of Security Controls Related to Information Assurance 26
Table 10 - IA and CS Staff Distribution of Full-time Equivalents 26
Table 11 - Description of Investment Initiatives Tables 53

1 EXECUTIVE SUMMARY

1 EXECUTIVE SUMMARY

In 2010, the Office of the Governor introduced a New Day Plan designed to take a fresh look at many of State's most significant investments with the aim of enhancing efficiency and effectiveness in key areas. The Information Technology (IT) program was an investment focused on early in the new administration. The State's IT program supports a complex, diverse, and multifaceted mission and has been identified as requiring enhancements to its IT security component. In recognition of the need to provide these enhancements, the State's IT management has undertaken efforts to address IT security and compliance areas that need enhancement to provide the additional protection to sensitive State and personal information by refocusing its resources and reevaluating its goals. The result of this re-evaluation is reflected in the following plans: Information Assurance and Cyber Security Program Management, the Information Assurance and Cyber Security Strategic, Information Assurance and Cyber Security Governance, Disaster Recovery and Continuity of Government, and Privacy.

This document presents State's Information Assurance and Cyber Security Strategic Plan supporting this initiative. Strategic plans covering all aspects of business, IT, and information resource management (IRM) have also been developed and identified as Phase II transformation efforts. Although the projects and the strategy have been well vetted, they are subject to change pending final approval of State's IT Governance Plan.

The Information Assurance and Cyber Security Strategic Plan, referred to as the Plan, has been prepared in response to the Chief Information Officer Council (CIOC), Enterprise Leadership Council (ELC), and the Enterprise Architecture Advisory Working Group (EA-AWG) as a vital component of the State of Hawai`i Business and IT/IRM Strategic Transformation Plan. The Plan is a direct result of briefings provided to the Chief Information Officer (CIO) addressing improvement of the Information Resources Management of information assurance and cyber security within the State. Under the leadership of the CIO, the Information Assurance and Privacy Advisory Working Group (IA&P-AWG), hereafter referred to as the authors, prepared this document. This Plan recommends both a strategic and tactical approach to IT security improvements using a risk management framework that addresses current and future needs of the State's security posture while recognizing the technical, financial, and cultural needs of State's organizational subcomponents.

The Plan includes initiative and project recommendations that specifically focus on enhancements and advancements that address specific security needs and establish a long-term (three-to-five year) strategic direction for the Information Assurance (IA) and Cyber Security (CS) Program.

As noted earlier, the strategy outlined in this Plan is a companion document meant to complement the Office of Information Management and Technology's (OIMT's) IT/IRM Transformation Architecture. The IA and CS Strategic, Program Management, Continuity of Operations and Disaster Recovery, Privacy, and Governance plans identify much of the foundational structure. The management roles, responsibilities, and oversight functions; risk-management processes; compliance, security, and efficiency goals; and foundational program and project management processes necessary to support the strategic direction and tactical efforts are identified in this Plan.

In preparing the Plan, the authors evaluated the current state of IA and CS within the State at the department, division, and branch levels. Using legislated requirements, educational studies, industry and government best practices and planning documents, department and organizational commitments and lines of business (LOBs), and the experience and knowledge of the team members to build a list of prioritized initiatives, a strategy was developed that will help to focus State's technology efforts.

By adopting any of the initiative recommendations identified, a significant improvement the State's security posture will be achieved.

All of the recommended initiatives represent significant investments of both capital and human resources; however, the benefits derived in implementing these initiatives greatly outweigh the potential risks associated with damage to State's reputation, mission activities, and public trust.

2 INTRODUCTION

2 INTRODUCTION

This Plan defines and prioritizes a number of IA and CS initiatives that the State must undertake to enhance the protection of information. While referred to as a strategy, the Plan is more properly a list of strategic investments. In preparing the Plan, the authors have made a strong effort to consolidate previously identified projects (where practical), provide scope and definition to each of the identified efforts, identify the general risks addressed by the initiative, and provide a foundation that can later be refined by formal project teams. In addition, to support a higher-level evaluation of which initiatives can be undertaken and when, the Plan attempts to identify any significant dependencies associated with the initiatives.

2.1 BACKGROUND

The State's various mission objectives, geographically diverse organizational structures, and many partnerships present unique technical challenges. The effectiveness of the techniques currently employed within the departments to address risks to information is inconsistent, and the use of the technologies has not been used to maximum capabilities. Former IA and CS programs and related management plans, strategies, processes, and initiatives established a succession of progressively elaborative IA and CS improvement tactics that built a sound foundation and established direction for the State's IA and CS program.

The approach in this Plan combines, defines, and prioritizes a list of multiple investments intended to consolidate all State departmental IT security initiatives into a shorter, more concise list of key investment efforts. Although it is still not a short list, the remaining initiatives can be evaluated with other IT/IRM program projects and available resources to decide which can be realistically accomplished. The risk assessments outlined in this Plan can provide key IT, mission, and stakeholder communities with an important decision-making tool when evaluating and documenting the risks associated with IA and CS projects that cannot or will not be completed.

This Plan builds heavily upon the development and deployment of a multi-layered defense strategy: the Acceptable Risk Management (ARM) and the IT Certification and Security Experts ISC2® Certified Information System Security Professional (CISSP) 10 Domains of Information Assurance.[1]

2.2 CURRENT AND EMERGING CYBER SECURITY THREATS

Cyber threats pose a critical national and economic security concern due to the continued advances in—and growing dependency on—the IT that underpins nearly all aspects of modern society. Data collection, processing, storage, and transmission capabilities are increasing exponentially; meanwhile, mobile, wireless, and cloud computing bring the full power of the globally connected internet to a myriad of personal devices and critical infrastructure. Because of market incentives, innovation in functionality is outpacing innovation in security, and neither the public nor private sector has been successful at fully implementing existing best practices.

The impact of this evolution is seen not only in the scope and nature of cyber security incidents, but also in the range of actors and targets. In the last year, we observed increased breadth and sophistication of computer network operations (CNOs) by both state and non-state actors. Our technical advancements in detection and attribution shed light on malicious activity, but cyber intruders continue to explore new means to circumvent defensive measures.

Among state actors, China and Russia are of particular concern. As indicated in the October 2011 biennial economic espionage report from the National Counterintelligence Executive, entities within these countries are responsible for extensive illicit intrusions into U.S. computer networks and theft of U.S. intellectual property.

Non-state actors are also playing an increasing role in international and domestic politics using social media technologies. We face a cyber-environment where emerging technologies are developed and implemented faster than governments can keep pace, as illustrated by the failed efforts at censoring social media during the 2011 Arab Spring revolutions in Tunisia, Egypt, and Libya. Hacker groups, such as Anonymous and Lulz Security (LulzSec), have conducted distributed denial of service (DDoS) attacks and website defacements against the government and corporate interests they oppose. The well-publicized intrusions into NASDAQ and International Monetary Fund (IMF) networks underscore the vulnerability of key sectors of the U.S. and global economy.

Hackers are also circumventing network security by targeting companies that produce security technologies, highlighting the challenges to securing online data in the face of adaptable intruders. The compromise of U.S. and Dutch digital certificate issuers in 2011 represents a threat to one of the most fundamental technologies used to secure online communications and sensitive transactions, such as online banking. Hackers also accessed the corporate network of the computer security firm RSA in March 2011 and exfiltrated data on the algorithms used in its authentication system. Subsequently, a U.S. defense contractor revealed that hackers used the information obtained from RSA to access its network.

[1] *International Information Systems Security Certification Consortium, "CISSP Domains, 2012." https://www.isc2.org/cissp-domains/default.aspx [1 May 2012]*

2.2.1 OUTLOOK FOR 2013-2015

We assess that CNO is likely to increase in coming years. Two of the greatest strategic challenges regarding cyber threats are:

1. The difficulty of providing timely, actionable warning of cyber threats and incidents, such as identifying past or present security breaches, definitively attributing them, and accurately distinguishing between cyber espionage intrusions and potentially disruptive cyber-attacks.

2. The highly complex vulnerabilities associated with the IT supply chain for networks.

3. The increase of "Advanced Persistent Threats (APTs)" from outside entities constitute a major challenge for information assurance and cyber security professionals. APTs require a high degree of stealthiness over a prolonged duration of operation in order to be successful. The attack objectives therefore typically extend beyond immediate financial gain, and compromised systems continue to be of service even after key systems have been breached and initial goals reached. Implementation of proactive continuous monitoring of network perimeter, computer systems and infrastructure is therefore critical for the survivability of state services and citizen support.

2.2.2 COUNTERINTELLIGENCE

Foreign intelligence services (FIS) are constantly developing methods and technologies that challenge the ability of information assurance professionals to protect data, information systems, and infrastructure. The changing, persistent, multifaceted nature of these activities makes them particularly difficult to counter.

Given today's environment, the authors assess that the most menacing foreign intelligence threats in the next two to three years will involve:

- Cyber-enabled Espionage. FIS have launched numerous computer network operations targeting various government agencies, businesses, and universities. Many intrusions into U.S. networks are not being detected or are being detected after large amounts of sensitive data have already been extricated. Although most activity detected to date has been targeted against unclassified networks connected to the internet, foreign cyber actors have also begun targeting classified networks.

- Insider Threats. Insiders have caused significant damage to government interests from the theft and unauthorized disclosure of classified, economic, and proprietary information and other acts of espionage. Trusted insiders who use their access for malicious intent represent one of today's primary threats to networks.

- Espionage by FIS. The U.S. Government reports that many foreign countries are aggressive and successful purveyors of economic espionage against the U.S. Foreign Intelligence Operations, including cyber capabilities, have dramatically increased in depth and complexity in recent years. FIS will remain the top threat to the United States and state interests in the coming years.

- Hacktivism (Hacker Activism). This is defined as "The activity of using computers to try to achieve social or political change."[2] Hacktivist organizations accounted for 58 percent of all data stolen in 2011.[3]

- Cyber Cartels (aka Cyber Mafia). These large, dispersed organized cybercrime syndicates use sophisticated and persistent attempts to gain access to private computer networks and systems to steal information for personal gains (e.g., identity theft and blackmail).

Evolving business practices and IT will provide even more opportunities for trusted insiders, hackers, and others to collect sensitive data. Corporate supply chains and financial networks will increasingly rely on global links that can be exploited by foreign collectors, and the growing use of cloud data processing and storage may present new challenges to the security and integrity of sensitive information.

2.3 SCOPE

The Plan presented in this document establishes a prioritized list of statewide departmental IA and CS investments and identifies a number of supporting rationale, including the risk reduction benefits for each. Recommended initiatives are generic to program needs and made without regard to specific department needs or future technologies. Initiatives have been evaluated for their do-ability; initiatives with higher project risk were not as highly favored as those with more mature implementation technologies. Although this Plan prioritizes IA and CS initiatives, it recognizes that the recommendations may not be approved or assigned to project teams as prioritized. Therefore, the Plan assumes that initiatives are reviewed by the IA&P-AWG prior to approval by the CIOC, IPSC, ELC, and EA-AWG, investments will be assigned to project managers, and then detailed project and implementation plans will be developed.

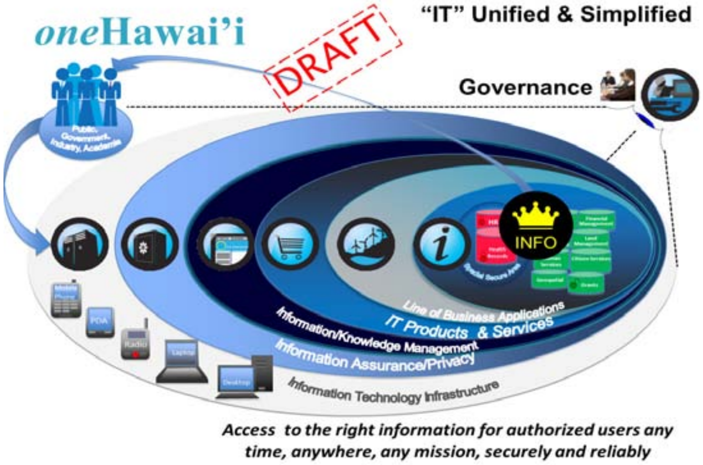
The Plan supports a multi-layered security model and identifies a number of technical and management-level recommendations that will improve the security posture of State. This document is not intended to be an implementation plan for the recommendations provided. The selection of any recommendation to be implemented, completion schedules, resource allocation, budgeting, and impact analysis is beyond the scope of this plan. As recommendations are reviewed by the IA&P-AWG and approved by the CIOC, each will be assigned to a project manager and implementation plans will be developed.

[2] *Hacktivism, as defined in the Cambridge Business English Dictionary, 2011 Edition*

[3] *"2012 Data Breach Investigations Report." Verizon RISK Team, March 14, 2012. .http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf?CMP=DMC-SMB_Z_ZZ_ZZ_Z_TV_N_Z037 [1 Jun. 2012]*

2.4 ALIGNMENTS

This document aligns with and complements the IA and CS Program Management Plan, materials presented to the CIOC during recent briefings, departmental priorities, the Governor's New Day Plan initiatives and priorities, and current legislation. Specifically, it is intended to align with the priorities outlined in the Governor's New Day Plan and the OIMT's IT/IRM Transformation Agenda pending legislative review and funding.



oneHawai'i
DRAFT
"IT" Unified & Simplified
Governance
Public, Government, Industry, Academia
INFO
Mobile Phone
PDA
Radio
Laptop
Desktop
Line of Business Applications
IT Products & Services
Information/Knowledge Management
Information Assurance/Privacy
Information Technology Infrastructure
Access to the right information for authorized users any time, anywhere, any mission, securely and reliably

Figure 1 - CIO's IT/IRM Transformation Vision

2.5 IA AND CS PROGRAM MANAGEMENT PLAN

This Plan complements the new IA and CS Program Management Plan, which defines departmental IA and CS program roles, responsibilities, and processes with respect to establishing IA and CS policy, standards, and operational/oversight functions. It establishes a framework for a common State risk-based approach that places emphasis on the control of likely (vs. less likely) risks and threats. This framework will ensure the safeguarding of organizational information assets while not ignoring other key factors, such as cost, performance, mission requirements, and efficiency. The framework will also establish and document a risk acceptance management chain based on program-level responsibilities and risk impact awareness by bringing risk management and acceptance processes closer to the program level with assurance statements supporting senior management's overall responsibilities.

This Plan's purpose is consolidation and prioritization of the improvement initiatives for implementation and commitment. Using the Risk Management Framework in the IA and CS Program Management Plan and associated governance, the processes will need to identify and accept residual risks as needed where remaining gaps exist. The IT/IRM governance processes will establish a set of those improvement initiatives that State believes are within our resources to implement and measure performance/success based on these. This Plan will identify opportunities for increased efficiencies, including specifying IA and CS services that are candidates for enterprise solutions. This Plan will also attempt to identify gaps in existing compliance functions, evaluate their related risks, and incorporate prioritized improvement strategies and risk reassessments into the Plan for continuous re-evaluation of the strategy.

2.6 PURPOSE AND BENEFITS

This document is intended to:

- Consolidate and replace previous departmental lists of priorities relating to IA & CS program functions and recommendations included in various departmental plans into a single coherent set of recommended initiatives. The proper prioritization[4] of the resulting consolidated list of recommended initiatives should be based on initiatives that:

  - First, contribute to both systemically improving security controls over information and information systems (as informed by both departmental and OIMT evaluations and assessments) and that relate to improving those aspects that adversely impact the ability to provide information in a reliable and secure way to support any mission.

  - Second, only contribute to systemically improving security controls over information and information systems (as informed by both departmental and OIMT evaluations and assessments).

  - Third, provide security operations to monitor continuously the status of security infrastructure in a proactive nature.

  - Fourth, provide information assurance guidance and align to future-state technology deployments in an Agile framework.

[4] Prioritization also attempts to take into account the appropriate sequencing of activities necessary to ensure that foundational capabilities exist to enable the success of dependent activities.

[5] This effort is a change in management approach aimed at efficiency improvements and cost avoidance. The goal of the change is to better select and manage IA resources and projects. An effective IA program will likely result in decreased costs through reduced risk of potential litigation or penalty associated with significant data breaches.

  - Fifth, contribute to security as an enabler to state business processes.
  - Lastly, contribute to improving security controls over information and information systems within individual department/branch IT security programs and specific information systems (as informed by both departmental and OIMT evaluations and assessments).
- Serve as the basis upon which comprehensive individual IA and CS initiative[5] project plans can be developed that will improve security and privacy controls:
  - Enhance compliance with State and Federal laws.
  - Reduce potential State/department liabilities.
  - Assist in the support of Federal and private grant proposals.
- Serve as a decision document in IT program-level planning and as a mechanism to improve resource planning, efficiency, and economies of scale by clarifying priorities and supporting integrated projects and enterprise solutions, including:
  - Provide a mechanism for the departments to collaborate on, implement, and establish priorities in a concerted and coordinated manner.

3
FUNDAMENTALS OF INFORMATION ASSURANCE RISK MANAGEMENT

3 FUNDAMENTALS OF INFORMATION ASSURANCE RISK MANAGEMENT

The management, assessment, and mitigation of risks to IT systems are a fundamental component of every organization's information assurance and cyber security program. An effective risk management process enables an organization to protect its information assets and supports its ability to carry out its mission successfully.

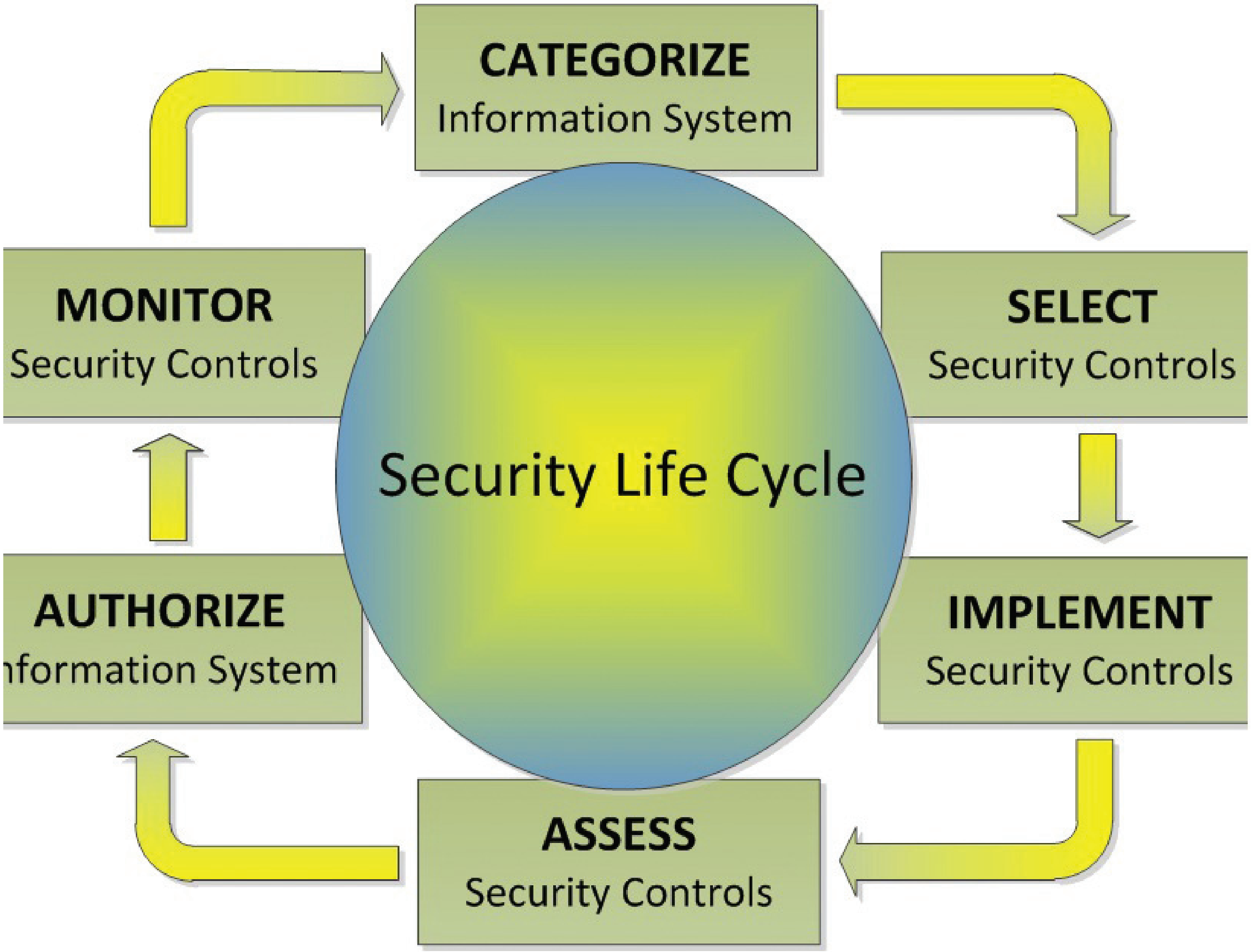


Figure 2 - Security Life Cycle

The following activities compose the Risk Management Framework. These activities are fundamental to the management of organizational risk and can be applied to both new and legacy information systems within the context of the System Development Life Cycle (SDLC) and the State of Hawai`i's Enterprise Architecture (EA).

Categorize the information system and the information processed; stored, and transmitted by the system, based on the potential impact to the organization should events occur to put the system and its information at risk. The organization assigns a security impact value (low, moderate, high) for the security objectives of confidentiality, integrity, or availability for the information and information systems that are needed by the organization to accomplish its mission, protect its assets and individuals, fulfill its legal responsibilities, and maintain its day-to-day functions.

Security categorization standards for information and information systems provide a common framework and understanding for documenting the potential impact to organizations or individuals should there be a breach of security (e.g., a loss of confidentiality, integrity, possession, utility authenticity or availability) to information or the information system. Federal Information Processing Standard (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems, can assist departments to determine the security category of data and information systems. The categorization process also promotes effective management of information systems and consistent reporting.

Select an appropriate set of security controls for the information system after determining the security categorizations. FIPS documents specify minimum-security requirements for information and information systems for seventeen security-related areas that represent a broad-based, balanced information security program. The 17 security-related areas encompass the management, operational, and technical aspects of protecting federal information and information systems. Furthermore, organizations must meet the minimum-security requirements by selecting an appropriately tailored set of baseline security controls based on an assessment of risk and local conditions including the organization's specific security requirements, threat information, cost-benefit analyses, or special circumstances.

To address minimum security requirements, the State will make use of security controls from "NIST SP 800-53, Recommended Security Controls for Federal Information Systems," summarized[6] below. This publication provides a catalog of controls that departments may select to protect their information systems in accordance with their missions and business requirements. An initial baseline set of security controls is determined based on the impact analysis conducted under the provisions of FIPS standards. Departments can tailor and supplement the selection of baseline security controls, based on their assessment of risks. Guidance on tailoring the baseline controls is provided by NIST.

Table 1 - Security Controls Classes, Families, and Identifiers

Identifier	Family	Class
AC	Access Control	Technical
AT	Awareness and Training	Operational
AU	Audit and Accountability	Technical
CA	Security Assessment and Authorization	Management
CM	Configuration Management	Operational
CP	Contingency Planning	Operational
IA	Identification and Authentication	Technical
IR	Incident Response	Operational
MA	Maintenance	Operational
MP	Media Protection	Operational
PE	Physical and Environmental Protection	Operational
PL	Planning	Management
PS	Personnel Security	Operational
RA	Risk Assessment	Management
SA	System and Services Acquisition	Management
SC	System and Communication Protection	Technical
SI	System and Information Integrity	Operational
PM	Program Management	Management

[6] *"NIST 800-53: Recommended Security Controls for Federal Information Systems." National Institute of Standards and Technology, 2011.*

Implement the security controls in the information system. Various Federal guides provide assistance in implementation of security controls; the State will use the NIST Special Publication Checklists for IT Products (http://checklists.nist.gov/) whenever available or vendor best practice standards. Checklists of security settings are useful tools that have been developed to guide IT administrators and security personnel in selecting effective security settings that will reduce the risks and protect systems from attacks. A checklist, sometimes called a security configuration guide, lockdown guide, hardening guide, security technical implementation guide, or benchmark, is a series of instructions for configuring an IT product to an operational environment. Checklists can be effective in reducing vulnerabilities to systems, especially for small organizations with limited resources. IT vendors often create checklists for their own products, but other organizations such as consortia, academic groups, and government agencies have also developed them.

Assess the security controls using appropriate methods and procedures to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. The IA and CS Division will provide certification services to assist departments in meeting assessment requirements.

Authorize information system operation based on a determination of the risk to organizational operations, organizational assets, or to individuals resulting from the operation of the information system and the determination that this risk is acceptable. NIST SP 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems, discusses the steps leading to an official management decision by a senior agency official to authorize operation of an information system, accepting the risks to agency operations, agency assets, or individuals based on the implementation of an agreed-upon set of security controls. Certification and accreditation of information systems are required activities for federal agencies.

Monitor selected security controls in the information system on a continuous basis including documenting changes to the system, conducting security impact analyses of the changes, and reporting the security status of the system to appropriate organization officials on a regular basis.

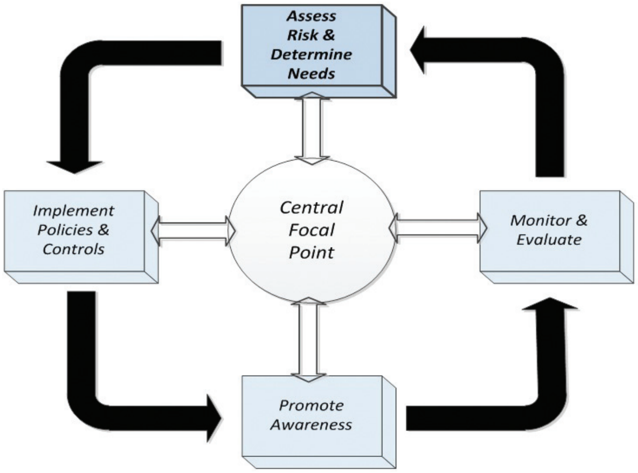


Figure 3 - Risk Management Cycle

Illustration from Information Security Risk Assessment - Practices of Leading Organizations

3.1 BASIC ELEMENTS OF THE RISK ASSESSMENT PROCESS

Whether they pertain to information security or other types of risk, risk assessments are a means of providing decision makers with information needed to understand factors that can negatively influence operations and outcomes and make informed judgments concerning the extent of actions needed to reduce risk. For example, bank officials have conducted risk assessments to manage the risk of default associated with their loan portfolios, and nuclear power plant engineers have conducted such assessments to manage risks to public health and safety. As reliance on computer systems and electronic data has grown, information security risk has joined the array of risks that governments and businesses must manage. Regardless of the types of risk being considered, all risk assessments generally include the following elements:

- Identifying threats that could harm and adversely affect critical operations and assets. Threats include such things as intruders, criminals, disgruntled employees, terrorists, and natural disasters.
- Estimating the likelihood that such threats will materialize based on historical information and judgment of knowledgeable individuals.
- Identifying and ranking the value, sensitivity, and criticality of the operations and assets that could be affected should a threat materialize in order to determine which operations and assets are the most important.

[7] *Information Security Risk Assessment - Practices of Leading Organizations. Supplemental Document. Washington D.C., U.S. General Accounting Office. 1999. page 6.*

- For the most critical and sensitive assets and operations, estimating the potential losses or damage that could occur if a threat materializes, including recovery costs.
- Identifying cost-effective actions to mitigate or reduce the risk. These actions can include implementing new organizational policies and procedures as well as technical or physical controls.
- Documenting the results and developing a plan of action and milestones for mitigating the any identified or residual risk.

There are various models and methods for assessing risk, and the extent of an analysis and the resources expended can vary depending on the scope of the assessment and the availability of reliable data on risk factors. In addition, the availability of data can affect the extent to which risk assessment results can be reliably quantified. A quantitative approach generally estimates the monetary cost of risk and risk reduction techniques based on 1) the likelihood that a damaging event will occur, 2) the costs of potential losses, and 3) the costs of mitigating actions that could be taken. When reliable data based on likelihood and costs are not available, a qualitative approach can be used by defining risk in more subjective and general terms such as high, medium, and low. This makes qualitative assessments depend more on the expertise, experience, and judgment of those conducting the assessment. It is also possible to use a combination of quantitative and qualitative methods.

3.2 ESTABLISH RELATIONSHIPS

The success of the Risk Management Framework is dependent upon the collaboration among the organization's many entities. Working together, senior leaders can make information risk decisions that ensure the organization's mission and business activities remain functional while also maintaining an acceptable security posture. The Information Security Program Office reaches out to the organization's information owners/information system owners to provide adequate guidance and direction on the categorization process. In addition, the Information Security Program Office develops and maintains relationships with the EA group, the Capital Planning personnel, and the technical operations personnel. 3.3 Develop Statewide Categorization Guidance

Information security programs should develop categorization guidance that supplements the existing guidance provided by Federal, State, and local compliance requirements and provides organization-specific procedures and documentation, approval, and reporting requirements. The specific guidance should address how information owners/information system owners:

- Integrate the categorization process into the system development life cycle.
- Handle new information types.
- Conduct the categorization process for their individual information systems.
- Document the categorization decision in the system security plan.
- Gain approval for the categorization decision.
- Report the categorization decision.
- Maintain the categorization decision by periodically validating that the categorization decision has not changed.

3.4 IDENTIFYING TYPES OF RISKS

Risks are very specific to the location, type of enterprise, and the size of the enterprise. A large multi-national enterprise will have very different risks than a smaller localized enterprise.

The first step in the risk assessment and analysis is to review the types of risks involved with a specific enterprise. There are four basic types of threat categories that can affect an enterprise: the insider, external, man-made, and natural disaster.

The insider threat is when the physical perimeter of the enterprise is compromised; this can be by an intruder, as when Ethan Hawk and company infiltrate the CIA offices in Mission Impossible. It is also when a current, trusted employee bypasses the in-place security protocols to gain access to information for which they do not have a need-to-know requirement.

External threats are less under control of the enterprise because they are instigated outside the network perimeter by individuals looking to do harm to the enterprise. Crackers/hackers are the typical category of external threats.

A sub-category of both internal and external threats is the man-made threat. The man-made threat can be categorized as a physical attack or accidents that affect the enterprise from performing business activities. Typical examples of man-made threats are the Transportation Security Authority (TSA) missing the shoe bomb scares in 2001 and 2009,[8] the accidental explosion of a power plant in Connecticut[9] during final stages of construction, and the explosion of the oil platform in the Gulf of Mexico.

Natural disaster threats are typically covered by the Business Continuity Process (BCP) or Disaster Recovery (DR) arenas of security, but are still just as relevant depending on the location(s) of the enterprise. For example, a New York office is more susceptible to a hurricane, but less likely to be disrupted by a tornado.

[8] *Richey, Warren, "Echoes of 2001 shoe bomber in Detroit attack – CSMonitor." December 28, 2009. The Christian Science Monitor. http://www.csmonitor.com/USA/Justice/2009/1228/Echoes-of-2001-shoe-bomber-in-Detroit-attack. [May 8, 2010].*

[9] *"Five dead in Middletown explosion, at least 12 injured, WTNH.com Connecticut." February 29, 2010. WTNH television. http://www.wtnh.com/dpp/news/middlesex_cty/middletown-power-plant-explosion. May 8, 2010.*

Table 2 - Identified Risks

Threat Type	Threat	Exploit/Vulnerability	Exposed Risk
Insider	Intruder	No security guard or controlled entrance	Theft
External	Hacker	Misconfiguration of firewall	Stolen credit card information
Internal	Current employee	Poor accountability; no audit policy; no security awareness program	Loss of integrity; altered data
Natural Disaster	Fire	Insufficient fire control	Damage or loss of life
External	Virus	Out-of-date antivirus software	Virus infection and loss of productivity
External	Spam overload e-mail system	No spam filtering	Loss of productivity
Internal	Hard drive failure	No data backup	Data loss and unrecoverable downtime
Man-made	Weapons of mass destruction; e.g., car bomb; package bomb; biological threat	No external facility monitoring; insufficient physical perimeter; no physical inspection of incoming packages	Data loss and unrecoverable downtime
Man-made	Accidental explosion	Non-compliance to OSHA requirements; bad construction practices	Loss of life; disruption of business; loss of reputation; environmental disaster

Once a list of risks to the enterprise is determined, the next step is to look at the methods and tools that can be used to determine what risks are the highest priority and/or will bring the greatest return on investment.

3.5 RISK CATEGORIES

This Plan discusses the prioritization of IA initiatives in terms of risks. The following generalized risk categories provide a basis for that discussion. A description has been provided in an attempt to clarify the types of risks included within each of the categories. The risks are not ordered by any weighting of importance nor are they equal in all applications.

1. Information Exposure/Loss: includes risks associated with the intentional or unintentional loss, theft, compromise, or disclosure of any type of sensitive department information or data, either in hard copy printed or soft copy electronic form that may be exploited by any unauthorized individual.

2. Unauthorized Use: includes risks associated with the intentional or unintentional use of any type of sensitive department information or data (in either hard copy printed or soft-copy electronic form), information system, or processes/procedures by an unauthorized individual.

3. Exposure to Contaminated Environments: includes risks associated with the intentional or unintentional exposure of any type of sensitive department cyber asset or information to potentially contaminated, untrusted, or insecure environments that may adversely affect the confidentiality, integrity, or availability of the exposed cyber asset or information. This can be done by the introduction of errors to information or data (in printed or electronic form); the introduction of malicious source code or software into an information system; or the introduction of unauthorized changes to automated processes/procedures.

4. Weak Processes: includes risks associated with the intentional or unintentional harm to any type of sensitive department information or data (either in hard copy printed or soft copy electronic form), information system, or processes/procedures resulting from inadequate controls either technical or manual (e.g., checks and balances, prone to human error and/or social engineering, etc.). These risks have the potential to affect the confidentiality, integrity, or availability of information or the information system adversely.

5. Unsecured Operating Environments: includes risks associated with the intentional or unintentional harm to any type of sensitive department information or data (either in hard copy printed or soft copy electronic form), information system, or processes/procedures resulting from inadequate controls either technical or manual (e.g., enabling the unauthorized modification of security controls within an information system increasing the systems vulnerability and susceptibility of information to compromise, enabling the unauthorized escalation of privileges to perform inappropriate functions on a system or to gain unauthorized access to information, etc.). These risks have the potential to impact the confidentiality, integrity, or availability of information or the information system adversely.

6. Loss of Public Confidence: includes risks associated with the intentional or unintentional harm to the reputation of the department and/or its leadership and the confidence of the public or senior government officials in the department's ability to conduct its mission effectively.

7. Exposure to Legal Action: includes risks associated with financial or non-financial legal actions taken against the department and/or its leadership. 3.6 Current Risk Assessment Methodologies

The two current base methodologies that are used by security professionals are the qualitative and quantitative methods. Each method is effective, but completely different in its approach to determining the level of risk. The issue is that each method could result in different outcomes.

Table 3 - Differences in Methodologies

Qualitative	Qualitative Quantitative
• Deals with descriptions	• Deals with numbers
• Designed to be a complete, detailed description	• Data is measureable
• Data is observed but cannot be measured	• Process uses mathematical tools
• Results are subjective	• Results are objective and testable
• Process is quicker	• More rigorous
• Less rigorous	

3.6.1 QUALITATIVE METHOD

The qualitative risk analysis is a process of assessing of the impact of the identified risks within an enterprise. By using this process, the priorities of vulnerabilities are determined to solve the risks based on the impact they could have on the enterprise. The definite characteristic of the qualitative method is the use, by the research team, of various subjective indexes such as ordinal hierarchy values: low-medium-high, vital-critical-important, benchmark, etc.

As described by Robert Jacobson in his analysis of Risk Assessment and Risk Management, once each risk is ranked, a risk matrix (shown in Table 4) can be developed.10

Table 4- Impact/Likelihood of Impact to the Enterprise Matrix

		Impact				
		Insignificant	Minor	Moderate	Major	Catastrophic
Likelihood	Almost Certain	🟧	🟧	🟧	🟥	🟥
	Likely	🟧	🟧	🟧	🟥	🟥
	Possible	🟧	🟧	🟧	🟧	🟧
	Unlikely	🟨	🟨	🟧	🟧	🟧
	Rare	🟨	🟨	🟧	🟧	🟧

[10] *Jacobson, Robert V., Computer Security Handbook, Volume 2, Risk Assessment and Risk Management. New York, NY: John Wiley and Sons, Inc., 2009. Chapter 62.*

In the example diagram in Figure 4, the point on the upper right is the risk that should be addressed immediately, while the lower left can be a risk that is accepted by management.

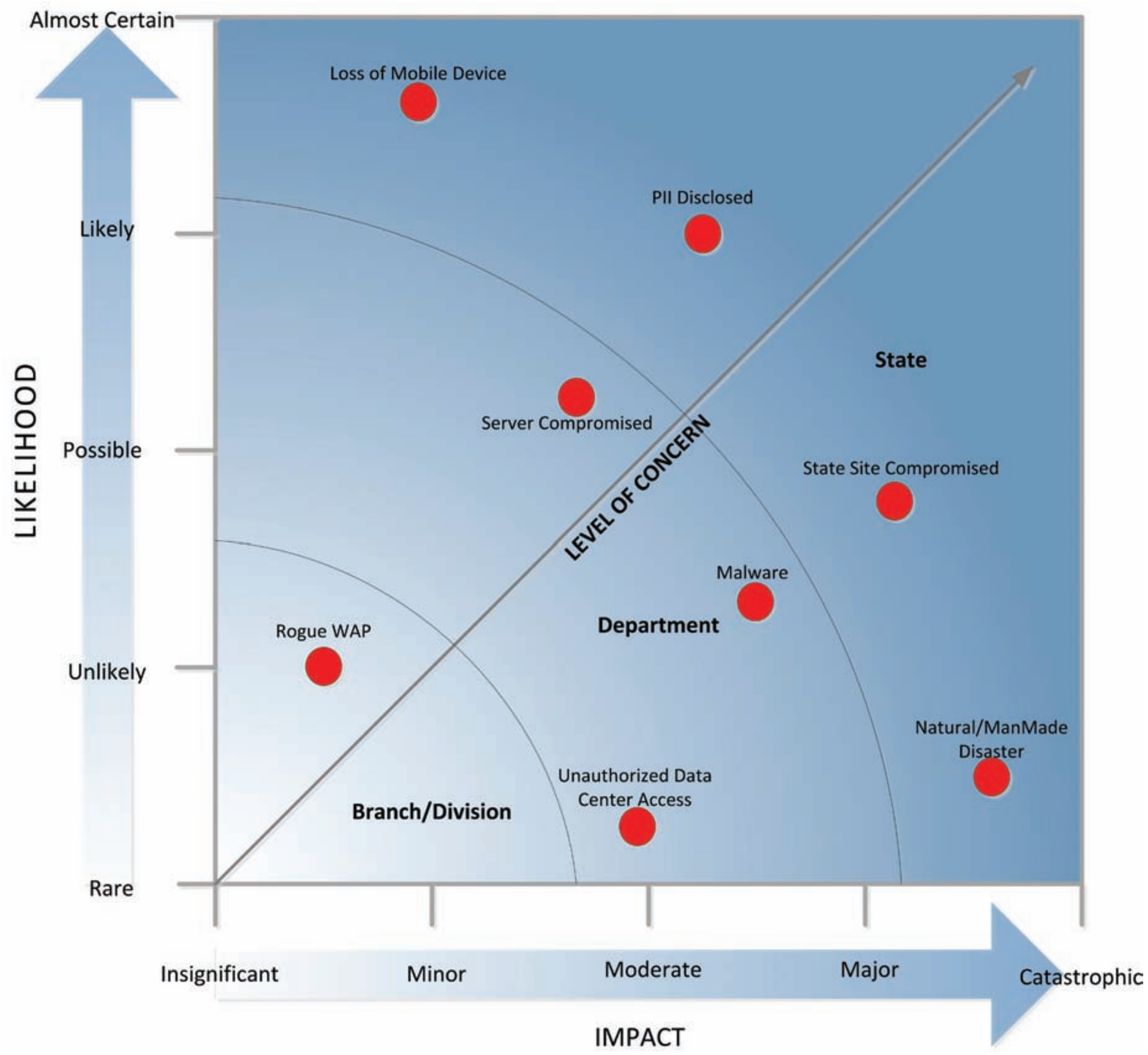


Figure 4 - Impact Assessment of Various Incidents to Enterprise

> "Estimating the likelihood of threat quantifiable as financial loss is difficult because it is based first of all on judgment and professional standing of the analyst."
>
> *Adrian Bogdanel Munteanu*

The statement above[11] describes the vital issue with the qualitative method. Typically, once the list of risks has been determined, the research is conducted by surveys and questionnaires. Even with a large cross section of the enterprise involved with the evaluation, the tendency will be for each functional area of the enterprise to rate their own areas high and vital. Once the surveys and questionnaires are collected and compiled, there is a high probability that the data will not identify a single risk or risks that need to be addressed. All the risks will have shown a high-vital mitigation need.

3.6.2 QUANTITATIVE METHOD

Through the quantitative risk analysis method, the assessment team can obtain some numerical results that express an approximate probability of each risk factor and its consequences on the objectives of the enterprise, but also the risks at the individual vulnerability level. The process uses several different mathematical techniques to evaluate the risks and make the determination based on the monetary loss if the risk occurs within a specific period.

[11] *Munteanu, Adrian Bogdanel, "Information Security Risk Assessment: The Qualitative Versus Quantitative Dilemma. Managing Information in the Digital Economy: Issues & Solutions," Proceedings of the 6th International Business Information Management Association (IBIMA) Conference, pages 227-232. June 19-21, 2006. (http://ssrn.com/abstract=917767)*

The most widely used mathematical models used in qualitative risk:

SLE = AV * EF

ALE = SLE * ARO

Table 5 - Factors in Risk Analysis Equation

Equation Element	Definition
Exposure Factor (EF)	The proportion of an asset's value that is likely to be destroyed by a particular risk (0% ≤ EF ≤ 100%)
Single Loss Expectancy (SLE)	The expected monetary loss every time a risk is exploited
Average Rate of Occurrence (ARO)	The probability that an exploitation of a risk will occur within a year (0.0 ≤ ARO ≥ 1.0)
Annual Loss Expectancy (ALE)	The monetary loss that can be expected for an asset due to a risk over a one-year period
Asset Value (AV)	A monetary value assigned to an asset at risk. This may be based on its actual cost, and/or the cost of its replacement.

Table 6 - Example Risk Analysis Table

Asset	Risk	AV	EF	SLE	ARO	ALE
Citizen database	Hacked	$432,000	74%	$320,000	.25	$80,000
Data files	User HDD failure	$9,450	17%	$1,650	0.9	$1,485
Domain controller	System failure	$82,500	88%	$72,500	.25	$18,125
E-commerce website	DDoS	$250,000	44%	$110,000	.45	$49,500

The problem of using the ALE to make the determination of risk is that, when the ARO is only evaluated at one loss per year and a risk occurs either during that year or future years, there can be considerable variance in the actual loss.

For example, using the second example in the table above, management decides, based on the low ALE value of the risk, not to implement the risk mitigation solution recommended, a tape backup solution.

The ARO is high (0.9), meaning that the likelihood of occurrence is high. With such a high potential, the chance for multiple occurrences during a single year will increase the actual ALE higher than what the risk analysis determined. So if a single enterprise with 10,000 employees has approximately 100 hard drive failures in a single year, the actual loss is 100 * $1,485 = $148,500. If the tape backup solution were only a capital cost of $50,000, then the risk must be ranked just behind the customer database risk.

Therefore, it is important to make sure when using the quantitative method of risk analysis not to look at the risk as a single point in time, but as a value that changes with the passage of time.

3.7 ALTERNATIVE RISK ASSESSMENT METHODS

3.7.1 PROBABILISTIC RISK ASSESSMENT (PRA)

To perform risk analysis in mechanical systems, the engineering community primarily uses a quantitative method of risk assessment. It looks at the concepts of "What can go wrong?," "What is most likely to occur?," and "What will be the consequences?"

By determining what can go wrong, the PRA then uses event tree and fault tree analysis to determine what lead to the failure. PRA then uses this information to determine the consequences of the failure.

An example might be the failure of an automatic teller machine (ATM) to dispense cash. To determine the possible reasons for the ATM's failure, the event tree and fault tree would be used. The consequences would be dissatisfaction of customers and loss of business.

3.7.2 FORENSIC ANALYSIS OF RISKS IN ENTERPRISE SYSTEMS (FARES)

FARES is a new risk-centric approach to risk analysis. The methodology takes a step back from traditional risk analysis, which looks at individual vulnerabilities, and looks at a broader view.

This approach uses both qualitative and quantitative aspects of risk analysis in combination instead of one or the other method.

Peter Stephenson mathematically defines risks in an enterprise system[12] as the following:

$$\rho = \Pi(\tau * v \Rightarrow \mu)$$

Information Systems Risk (ρ) is the probability (Π) that a threat (τ) will successfully exploit a vulnerability (v) to create an impact (μ).

Using this base equation, the basic concept of FARES is that risks consist of many vulnerabilities and threats that can be exploited. Attempting to identify and mitigate the multitude of vulnerabilities and threats is almost impossible to identify and manage. Creating larger supersets of vulnerabilities and threats makes the risk analysis and assessment a more manageable effort.

Instead of trying to identify individual software vulnerabilities, FARES suggests creating a superset using common criterion called software vulnerabilities and working towards the credible threats can exploit them. Next, look at the impacts that would be caused by a successful exploitation of the threats, and then countermeasures can be put into place to lessen or completely remove the impact to the enterprise.[13]

3.8 CHALLENGES ASSESSING INFORMATION SECURITY RISKS

Reliably assessing information security risks can be more difficult than assessing other types of risks, because the data on the likelihood and costs associated with information security risk factors are often more limited and because risk factors are constantly changing. For example:

- Data are limited on risk factors, such as the likelihood of a sophisticated hacker attack and the costs of damage, loss, or disruption caused by events that exploit security weaknesses.
- Some costs, such as loss of customer confidence or disclosure of sensitive information, are inherently difficult to quantify.
- Although the cost of the hardware and software needed to strengthen controls may be known, it is often not possible to estimate precisely the related indirect costs, such as the possible loss of productivity that may result when new controls are implemented.
- Even if precise information were available, it would soon be out of date due to fast-paced changes in technology and factors such as improvements in tools available to would-be intruders.

This lack of reliable and current data often precludes precise determinations of which information security risks are the most significant and comparisons of which controls are the most cost effective. Because of these limitations, it is important that organizations identify and employ methods that efficiently achieve the benefits of risk assessment while avoiding costly attempts to develop seemingly precise results that are of questionable reliability.

[12] *Stephenson, Peter R., "Forensic Analysis of Risks in Enterprise Systems." The Center for Digital Forensics Studies, Ltd. 2010. http://www.google.com/search?hl=en&source=hp&q=Forensic+Analysis+of+Risks+in+Enterprise+Systems&btnG=Google+Search&aq=f&aqi=&aql=&oq=&gs_rfai= [May 8, 2010]*

[13] *Ibid, page 4.*

Table 7 - CISSP 10 Domains of Information Assurance

Access Controls	Business Continuity and Disaster Recovery
A set of mechanisms (e.g. two-factor authentication, Personal Identification Numbers [PINs], card readers, etc.) that work in concert to create security architecture protecting information system assets	Addresses the preservation of the State’s IT/IRM infrastructure in the face of major disruptions, natural or man-made, to normal business operations and guarantee continuity of government
Cryptography	**Secure Application Development**
The principles, means, and methods of disguising (encrypt/decrypt) information during the storage, use, or transmission of information during its life cycle with the intent to make a foe take extraordinary measures to recover the data	Security controls implemented and tested during the SDLC.
Physical Security	**Operations Security**
Addresses the threats, vulnerabilities, and countermeasures that can be utilized to protect an enterprise’s resources and sensitive information physically. Includes site/facility design considerations, perimeter security, fire and security control mechanisms, etc.	Used to identify the controls over hardware, media, and the operators with elevated access privileges to any of these resources
Security Architecture and Design	**Telecommunications and Network Security**
The concepts, principles, structures, and standards used to design, implement, monitor, and secure operating systems, equipment, networks, applications, and those controls used to enforce various levels of security	Network structures, transmission methods, transport formats, and security measures to provide a secure infrastructure
Legal, Regulations, Investigations, and Compliance	**Information Security Governance and Risk Management**
Addresses computer crime laws and regulations; the investigative measures and techniques that can be used to determine if a crime has been committed and methods to gather evidence	Identifies the State’s information assets and the development, documentation, and implementation of policies, standards, procedures and guidelines

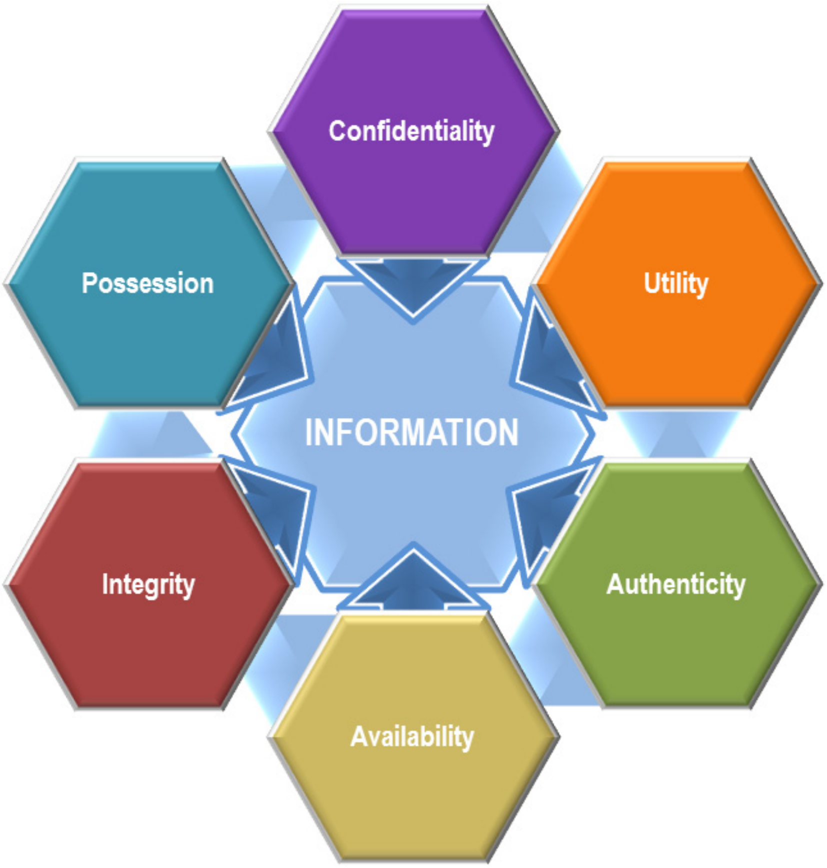


Figure 5 - Elements of Information Assurance and Cyber Security (Parkerian Hexad)

In 1998, Donn B. Parker expanded the original three fundamental elements of IA and CS into six elements of information security: Confidentiality, Possession (or Control), Integrity, Authenticity, Availability, and Utility.[14]

- Confidentiality – Limiting the access and disclosure to authorized users; at the same time, protecting information from unauthorized disclosure or not only the information but the existence of the information. An attacker cannot attack if the existence of the information is masked.

- Availability – Access to information is not restricted by time or circumstances; information anytime, for any mission, is the basic tenant of Business Continuity, Disaster Recovery, and Continuity of Government planning.

- Integrity – The trustworthiness or validity of the information being accessed or protecting it from modification by unauthorized users, corruption during transmission, or recovery of information from trusted sources.

- Possession – Also sometimes referred to as Control; maintaining control of the information. This includes physical controls and preventing copying or sending information to unauthorized users (e.g., using a single software license for an entire organization or software piracy).

- Authenticity – Misrepresenting information, repudiation, and misuse of information.

- Utility – Information maintains usefulness during its life cycle (e.g., an employee forgetting a decryption password or losing the master key to a data center).

This document also identifies multiple strategic investment recommendations, categorized in a multi-layer defensive solution framework and aimed at addressing inherent weaknesses in the State's internal and external security posture. While actions have been undertaken or are underway to address many of these earlier recommendations, some will be reiterated in this Plan where necessary to indicate the need for improved capabilities.

[14] *Parker, Donn B., Fighting computer crime: a new framework for protecting information. New York, NY USA: John Wiley & Sons. 1998.*

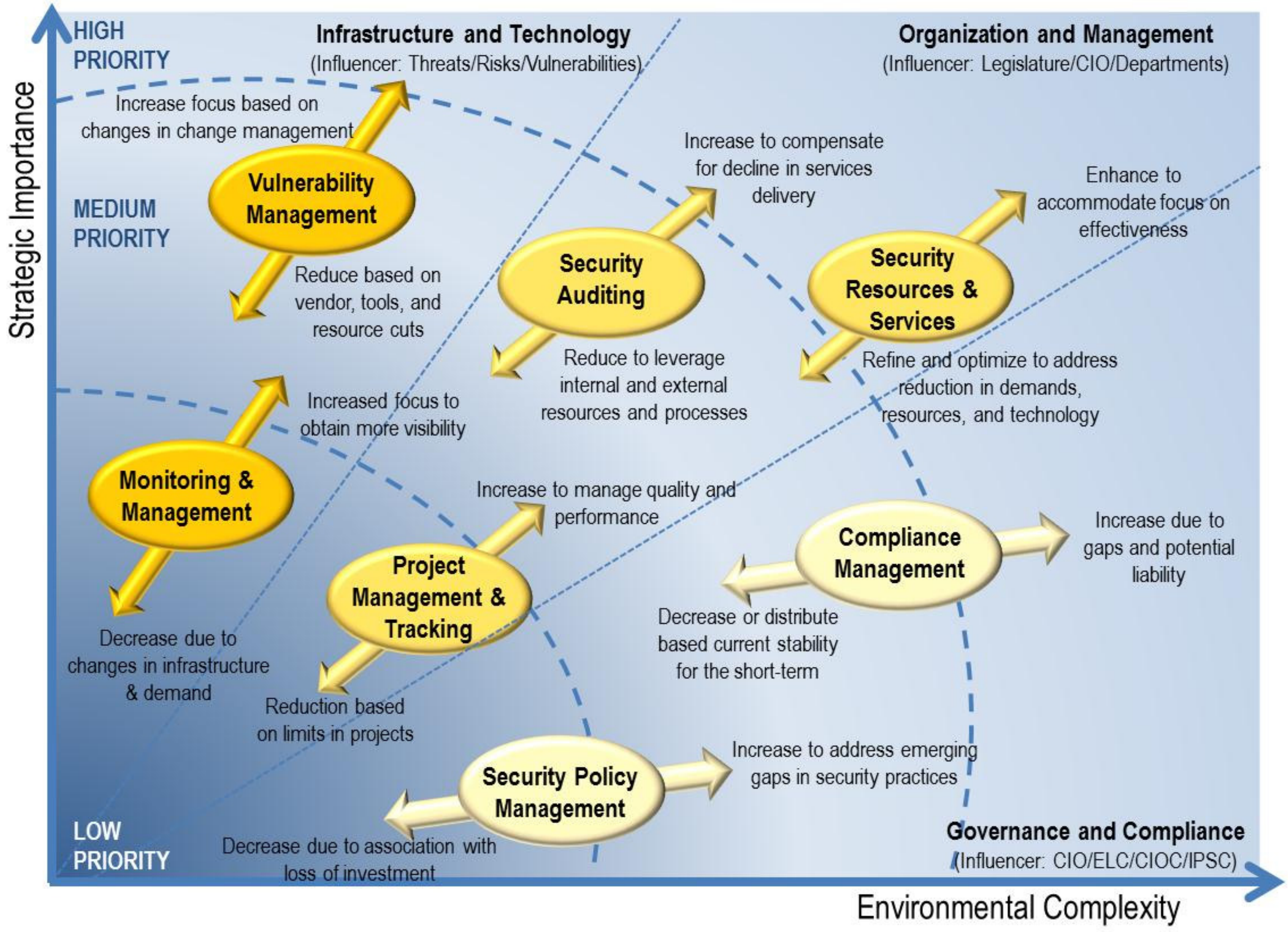

Strategic Importance
HIGH PRIORITY
MEDIUM PRIORITY
LOW PRIORITY
Environmental Complexity
Infrastructure and Technology
(Influencer: Threats/Risks/Vulnerabilities)
Organization and Management
(Influencer: Legislature/CIO/Departments)
Governance and Compliance
(Influencer: CIO/ELC/CIOC/IPSC)
Increase focus based on changes in change management
Vulnerability Management
Reduce based on vendor, tools, and resource cuts
Increase to compensate for decline in services delivery
Security Auditing
Reduce to leverage internal and external resources and processes
Enhance to accommodate focus on effectiveness
Security Resources & Services
Refine and optimize to address reduction in demands, resources, and technology
Increased focus to obtain more visibility
Monitoring & Management
Decrease due to changes in infrastructure & demand
Increase to manage quality and performance
Project Management & Tracking
Reduction based on limits in projects
Compliance Management
Increase due to gaps and potential liability
Decrease or distribute based current stability for the short-term
Security Policy Management
Increase to address emerging gaps in security practices
Decrease due to association with loss of investment

Figure 6 - Security Implementation Strategy Based on Importance vs. Complexity

Today's information systems[15] are complex assemblages of technology (e.g., hardware, software, and firmware), processes, and people working together to provide organizations with the capability to process, store, and transmit information in a timely manner to support various missions and business functions. The degree to which organizations have come to depend upon these information systems to conduct routine, important, and critical missions and business functions means that the protection of the underlying systems is paramount to the success of the organization. The selection of appropriate security controls for an information system is an important task that can have major implications on the operations and assets of an organization as well as the welfare of individuals. Security controls are the management, operational, and technical safeguards or countermeasures prescribed for an information system to protect the confidentiality, integrity (including non-repudiation and authenticity), and availability of the system and its information.

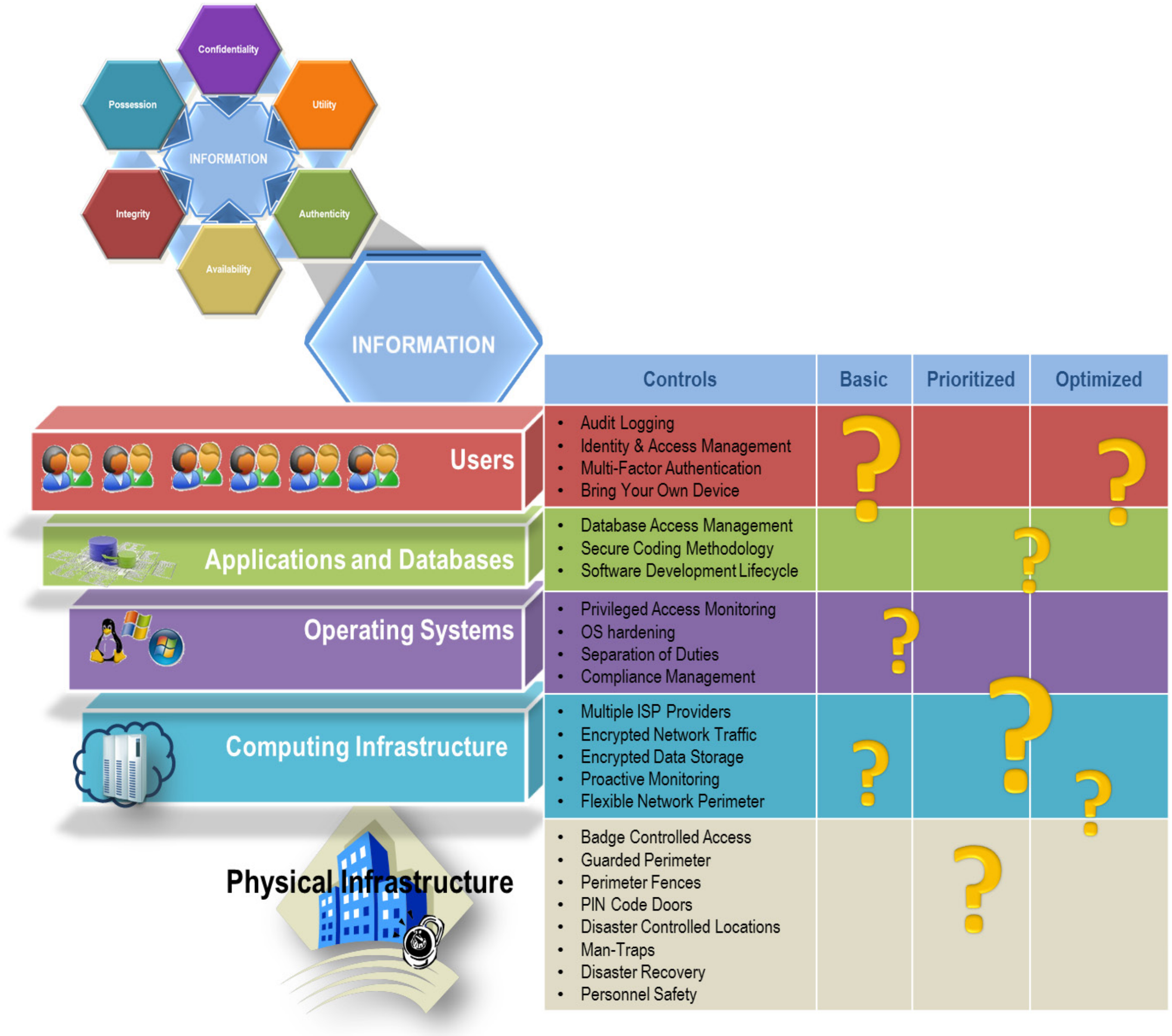
[15] *An information system is a discrete set of information resources organized expressly for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.*

Table 8 - Categories of Security Controls Related to Information Assurance

Control Types	Description
Physical Security	Preventive physical controls, traditionally “guards, guns and gates;” provide an environment to safely process information as well as barriers to unauthorized access to systems
Computing Infrastructure	Applies to all infrastructure components, networking, internet service providers (ISPs), servers, mobile devices, desktops, etc. sponsored by, developed for, or maintained or operated on behalf of the State, regardless of whether they are located at a State computing facility. The infrastructure also applies to pilot and proof-of-concept projects.
Operating Systems	An operating system (OS) is a set of software that manages computer hardware resources and provides common services for computer programs. The OS is a vital component of the system software in a computer system.
Applications and Databases	Security controls that cover software applications developed internally, by external acquisition, outsourcing/offshoring, or through hybrid approaches. These controls address all aspects of controls from determining information security requirements and protecting information accessed by an application or database to preventing unauthorized use and/or actions of an application.
Users	Ensure that unauthorized users do not get into the system and by encouraging (and sometimes forcing) authorized users to be security-conscious; for example, by changing their passwords on a regular basis. The system also protects password data and keeps track of who’s doing what in the system, especially if what they are doing is security-related (e.g., logging in, trying to open a file, using special privileges).

Table 8 - Categories of Security Controls Related to Information Assurance

Level of Maturity	Description
Basic	At the basic level, processes are usually ad-hoc and chaotic. The organization usually does not provide a stable environment. Success in the organization depends on the competence and heroics of the people in the organization and not on the use of proven processes. Organizations often produce products and services that work; however, they frequently exceed the budget and schedule of their projects. Organizations are characterized by a tendency to over commit, abandon processes in the time of crisis and inability to repeat their past successes.
Prioritized	The organization has achieved all the specific and generic goals at the basic level. In other words, the projects of the organization have ensured that requirements are managed and that processes are planned, performed, measured, and controlled. The reflected discipline for the process helps to ensure that existing practices are retained during times of stress. When these practices are in place, projects are performed and managed according to their documented plans. Project requirements, processes, work products, and services are managed. The status of the work products and the delivery of services are visible to management at defined points. Commitments are established among relevant stakeholders and are revised as needed. Work products are reviewed with stakeholders and are controlled. The work products and services satisfy their specified requirements, standards, and objectives.
Optimized	The organization has achieved all the specific goals of the process areas assigned to maturity levels basic, managed and optimized, including the generic goals assigned to maturity levels basic and managed. Processes are continually improved based on a quantitative understanding of the common causes of variation inherent in processes. Optimization focuses on continually improving process performance through both incremental and innovative technological improvements. Quantitative process improvement objectives for the organization are established, continually revised to reflect changing business objectives, and used as criteria in managing process improvement. The effects of deployed process improvements are measured and evaluated against the quantitative process improvement objectives. Both the defined processes and the organization's set of standard processes are targets of measurable improvement activities. Optimizing processes that are agile and innovative depends on the participation of an empowered workforce aligned with the business values and objectives of the organization. The organization's ability to respond rapidly to changes and opportunities is enhanced by finding ways to accelerate and share learning. Improvement of the processes is inherently part of everybody's role and results in a cycle of continual improvement.



Controls	Basic	Prioritized	Optimized
• Audit Logging • Identity & Access Management • Multi-Factor Authentication • Bring Your Own Device	?		?
• Database Access Management • Secure Coding Methodology • Software Development Lifecycle		?	
• Privileged Access Monitoring • OS hardening • Separation of Duties • Compliance Management	?		
• Multiple ISP Providers • Encrypted Network Traffic • Encrypted Data Storage • Proactive Monitoring • Flexible Network Perimeter	?	?	?
• Badge Controlled Access • Guarded Perimeter • Perimeter Fences • PIN Code Doors • Disaster Controlled Locations • Man-Traps • Disaster Recovery • Personnel Safety		?	

Figure 7 - Information Assurance and Cyber Security Capability Maturity Model with Example Security Controls

Once employed within an information system, security controls are assessed to provide the information necessary to determine their overall effectiveness; that is, the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. Understanding the overall effectiveness of the security controls implemented in the information system and its environment of operation is essential in determining the risk to the organization's operations and assets, to individuals, to other organizations, and to the nation resulting from the use of the system.

Not all security controls listed in NIST 800-53 are applicable, as each IT/IRM environment is unique. To select individual security controls better, it is necessary to understand that there are specific categories of controls.

4
STRATEGIC INFORMATION ASSURANCE AND CYBER SECURITY GOALS AND OBJECTIVES

4

STRATEGIC INFORMATION ASSURANCE AND CYBER SECURITY GOALS AND OBJECTIVES

The IA initiatives identified in this Plan largely fall into one or more of six strategic goal areas:

- Protect Data – As demonstrated in a succession of well-publicized security events, the protection of privacy and other sensitive information is one of the most significant challenges faced in organizations today. This becomes even more challenging when addressed in the context of protecting access. Opening the information infrastructures to provide improved access to the right information for authorized users—anywhere, anytime, and any mission securely and reliably—is fundamental to State's ability to preserve and improve its mission capabilities. Meeting this objective; however, increases the complexities associated with protecting our sensitive information.

- Proactive Continuous Monitoring – The goal of continuous monitoring is to provide real-time awareness of a department's security posture, enabling departments to address threats and to remediate vulnerabilities proactively before they can be exploited.

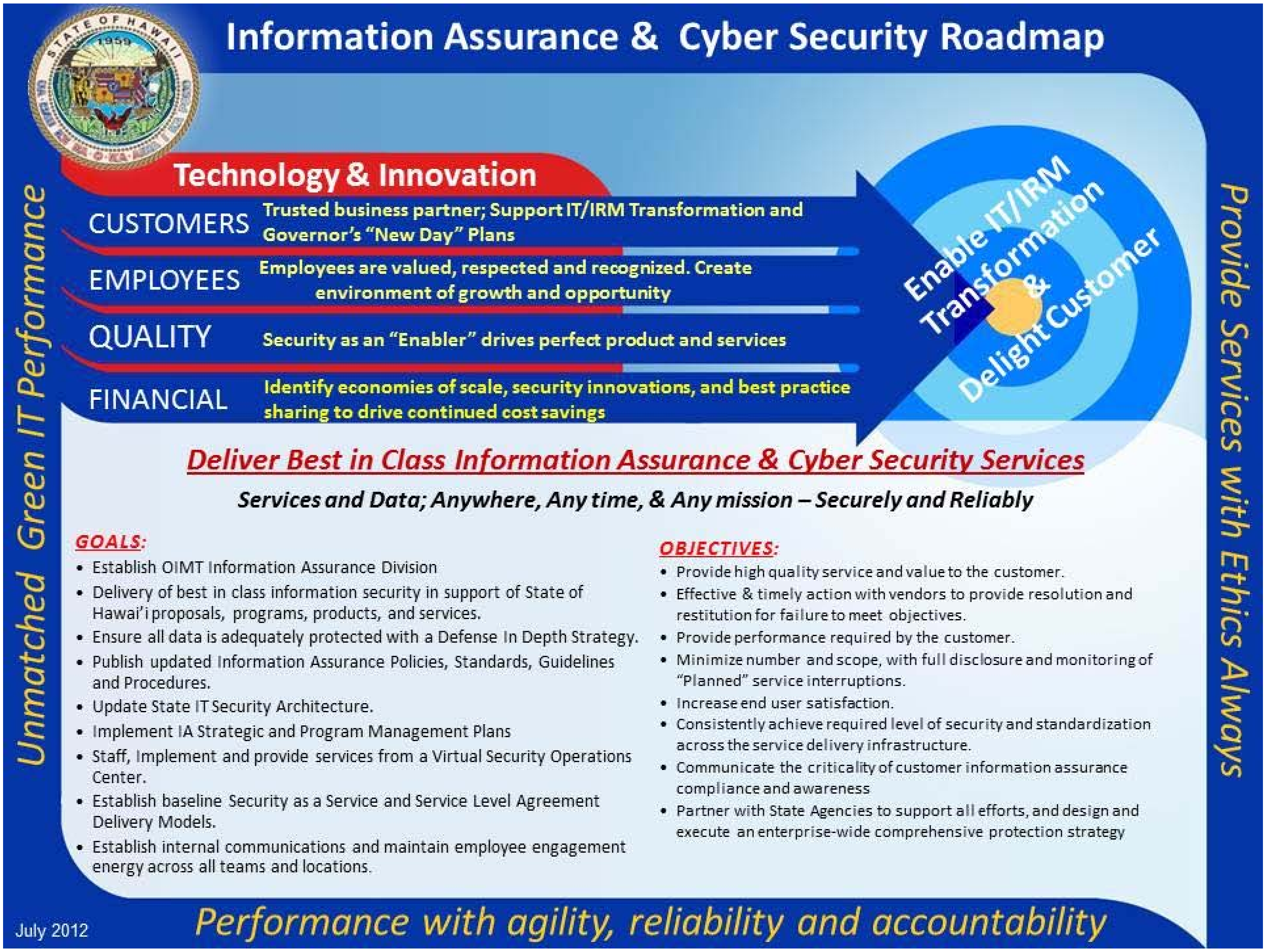
- Network Centric – The network-centric approach focuses on providing defense at the periphery. This is what many would consider the traditional approach to provide security to the enterprise. While this method of protection is still valid, a more radical approach to security must include the life cycle of data, from creation, how it is used when valid, its use during any archival or retention requirements, and through its proper method of destruction.

- Data Centric – The data-centric approach focuses on the data itself and where it lives: the database. Data-centric continuous monitoring protects the data by identifying and fixing database vulnerabilities before exploitation occurs.

- Protect Access – In meeting the two significant objectives of protecting authorized users' access to the right information, the State must first strengthen its ability to granularly establish and enforce access rules, and then tie these rules to its information assets so that only those individuals with rights to information have those rights. In addition, to address the access objective of reliability, the State must deploy secure, reliable, capacious, and diverse access solutions that allow users access to needed information—anywhere and at any time.

- Situational Awareness – To support an awareness of infrastructure or information risk related to configuration or patching weaknesses, exposure, attacks, and deliberate or accidental misuse, through implementation of security monitoring technologies and operational monitoring of these technologies.

The New Day Plan established a unity of purpose with One Team – One Mission – One Vision – One Set of Goals and Objectives. This Plan was one of the six focus areas identified as part of the proposed four phases to be completed over the next four years of the current administration.



Information Assurance & Cyber Security Roadmap

Unmatched Green IT Performance
Provide Services with Ethics Always
Enable IT/IRM Transformation & Delight Customer

Technology & Innovation

CUSTOMERS	Trusted business partner; Support IT/IRM Transformation and Governor's "New Day" Plans
EMPLOYEES	Employees are valued, respected and recognized. Create environment of growth and opportunity
QUALITY	Security as an "Enabler" drives perfect product and services
FINANCIAL	Identify economies of scale, security innovations, and best practice sharing to drive continued cost savings

Deliver Best in Class Information Assurance & Cyber Security Services

Services and Data; Anywhere, Any time, & Any mission – Securely and Reliably

GOALS:

- Establish OIMT Information Assurance Division
- Delivery of best in class information security in support of State of Hawai'i proposals, programs, products, and services.
- Ensure all data is adequately protected with a Defense In Depth Strategy.
- Publish updated Information Assurance Policies, Standards, Guidelines and Procedures.
- Update State IT Security Architecture.
- Implement IA Strategic and Program Management Plans
- Staff, Implement and provide services from a Virtual Security Operations Center.
- Establish baseline Security as a Service and Service Level Agreement Delivery Models.
- Establish internal communications and maintain employee engagement energy across all teams and locations.

OBJECTIVES:

- Provide high quality service and value to the customer.
- Effective & timely action with vendors to provide resolution and restitution for failure to meet objectives.
- Provide performance required by the customer.
- Minimize number and scope, with full disclosure and monitoring of "Planned" service interruptions.
- Increase end user satisfaction.
- Consistently achieve required level of security and standardization across the service delivery infrastructure.
- Communicate the criticality of customer information assurance compliance and awareness
- Partner with State Agencies to support all efforts, and design and execute an enterprise-wide comprehensive protection strategy

July 2012

Performance with agility, reliability and accountability

Figure 3 - Information Assurance and Cyber Security Roadmap

5 PERSPECTIVE ON INFORMATION ASSURANCE

5 PERSPECTIVE ON INFORMATION ASSURANCE

The most important aspect of effectively managing the risk to the organization's operations and assets associated with operating enterprise information systems is a fundamental commitment to information security on the part of the senior leadership of the organization. This commitment is the internalizing of information security, as an essential mission need. Fundamental commitment to information security translates into ensuring sufficient resources (both dollars and people) are available to provide an appropriate level of security for the organization's information systems. Information security must be a top priority within the enterprise and structurally embedded within the infrastructure of the organization. This implies that every new initiative within the enterprise from the development of corporate strategies and programs to the acquisition of goods and services incorporates information security considerations, preferably as early as possible in the system development life cycle process. Information security requirements must be considered at the same level of importance and criticality as the mainstream functional requirements established by the enterprise.[16]

In 2011, Gartner conducted a survey of CIOs in Federal, state, local, and private sector organizations to determine the current level of concerns about the security posture of organization's and where they saw the current threats in order to map these threats to available technology solutions.[17] The results are shown in Figure 9.

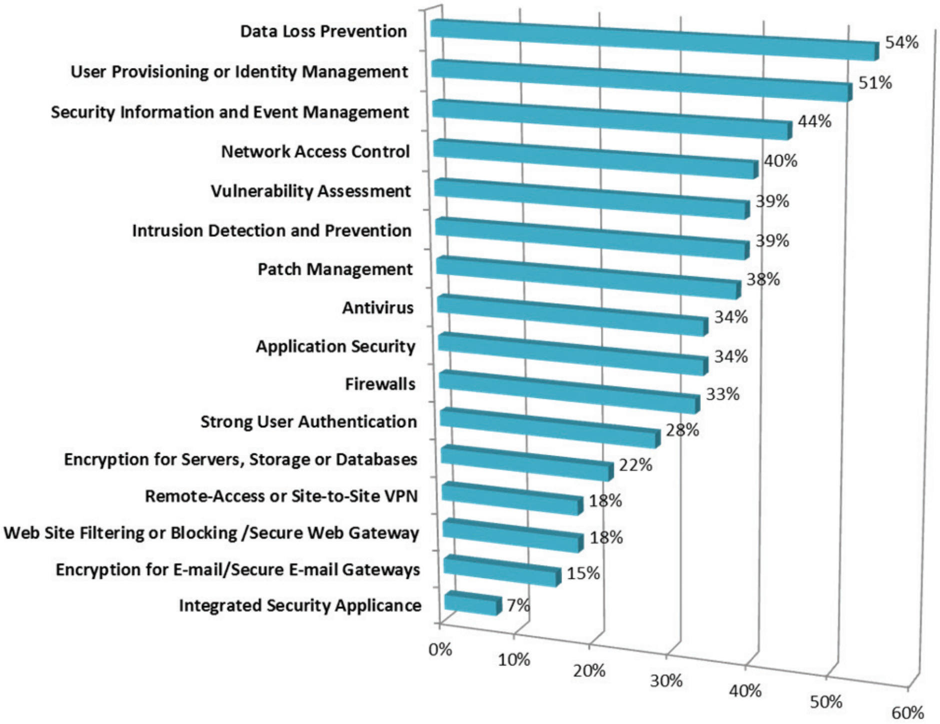


Figure 9 - CIO Top Information Assurance and Cyber Security Concerns (2011)

[16] *Ross, Dr. David, "Managing Enterprise Risk in Today's World of Sophisticated Threats." National Institute of Standards and Technology Washington: GPO. 2007.*

[17] *Gartner research at www.gartner.com*

5.1 COMMITMENT

To perform its mission effectively and efficiently, IT is an important component of each State organizational element's ability. Effective and efficient information security programs require clear direction and commitment from top management and administration. IA and CS are integrated functions that require effective organization and collaboration throughout the State. Protecting our electronic information and IT is the primary function of IT security. As an important mission enabler, IT security requires commitments on the part of both management and staff. These commitments will sometimes involve sacrifices. The loss of previously enjoyed computer use flexibilities that result in a gain in the overall level of protection against today's evolving IT threats can be the hardest hurdle for many organizations to make. Management's role is key to an organization's success in addressing the changes and impacts of any security improvement strategy.

As State employees, all of us have a shared responsibility to help maintain a strong security posture within our organizational environments. Nowhere is this more evident than with management. The security posture of State is only as strong as that of our weakest organizational component or user. This is evident in both outsider (external) and insider threat assessments conducted on the State's IT infrastructure. To be most effective, management must lead the way by demonstrating and emphasizing its commitment to improving the IT security of its organizations.

This Plan recommends departmental, division, branch, and office senior leadership re-emphasize that IT infrastructure contributes to our ability to accomplish our mission, and that every employee and contractor's actions are key to our overall success and contribute to the reliability and integrity of the infrastructure. IT security needs to be emphasized as an important means of protecting our IT infrastructure—one of the most important tools that we have today. To be most effective, IT security must be integrated into and considered in our everyday processes, planning, budgeting, and designs. IT security is not an IT responsibility, but every IT user's responsibility, from accountants, human resources specialists and scientists to budget analysts, planners, and engineers.

5.1.1 DEPARTMENT HEADS AND CIOS

Department Heads and CIOs are the offices of primary responsibility for information collected, maintained, and/or that has been identified as primarily utilized or owned by their respective departments. The CIOs may delegate operational management of these responsibilities by designation of a Department Information Security Officer (DISO) within their respective divisions. Vice Presidents may also designate other responsible parties to work with the DISO to assist in implementing this program. These designated individuals ensure information assets within their span of control have designated responsible parties (owners), that risk assessments are carried out for the departments, and that mitigation processes based upon those risks take place. The designated responsible party reports the status of the Information Security Program within the department as appropriate.

5.1.2 DIRECTORS, CHAIRS, MANAGERS, AND OTHER SUPERVISORS

Departments, divisions, branches, and attached agency directors, chairs, managers, and other supervisors responsible for managing employees with access to information and information systems are responsible for specifying, implementing, and enforcing the specific information security controls applicable to their respective areas. This includes ensuring all employees understand their individual responsibilities related to information security, and ensuring employees have the access required (and only the access required) to perform their jobs. Supervisors should periodically review all users' access levels to ensure they are still appropriate and take the appropriate action to correct discrepancies/deficiencies. Supervisors are required to notify Human Resources and the IT Help Desk proactively of any change in employment status that impact access requirements. Supervisors are also responsible for reporting suspected misuse or other information security incidents to the DISO, Chief Information Security Officer (CISO), and other appropriate parties.

5.1.3 CHIEF INFORMATION SECURITY OFFICER (CISO)

The State of Hawai`i CISO is designated as the Program Officer responsible for coordinating and overseeing the IA and CS Program. The CISO must work closely with the various departments throughout the State. The CISO may recommend that divisions/branches of specific departments delegate other representatives of the organization to oversee and coordinate particular elements of the Program.

The CISO also assists individuals who have the responsibility and authority for information (owners) with information security best practices relating to issues such as:

- Establishing and disseminating enforceable rules regarding access to and acceptable use of information resources
- Conducting/coordinating information security risk assessment and analysis; establishing reasonable security guidelines and measures to protect data and systems
- Assisting with monitoring and management of systems security vulnerabilities
- Conducting/coordinating information security audits
- Assisting with investigations/resolution of problems and/or alleged violations of state information security policies

Finally, the demonstration of commitment must be reflected in the allocation of resources, both human and capital, to the management and accomplishment of strategic security improvement goals. Without this important commitment, no significant progress can be made. 5.2 Communication Plan

Effective, efficient communication should involve a dialog. To ensure that communication lines remain open requires mutual respect for various disciplines and an equal voice in the process for all disciplines within the department, bureaus, and offices. Establishing that dialog means:

- Ensuring that all employees are engaged in the effort
- Ensuring opportunities for everyone to provide input to the process
- Recognizing that one solution may not work in every situation

When creating a new policy or recommendations and guidance, effective communication of these changes is often a last thought. Failure to implement new policy and directives throughout the state in a timely manner can often be attributed to the failure to raise awareness of the new guidance to the appropriate level in the IT workforce and user community. The lack of repetition and variety in the communication of policy perpetuates unawareness.

This Plan recommends the development of a comprehensive communication strategy to improve the dissemination and reception of IT security policies, procedures, standards, guidelines, directives and mandates. Specifically, the following areas of concern should be addressed in the communication strategy:

- Policy dissemination
- Management awareness
- Awareness training
- Consideration of the target audience
- Consideration of the culture of the various departments, divisions, branches, and offices within the State 5.3 Resource Management

To enable security programs at the department, division, branch, and office levels to succeed, this Plan recommends management establish realistic expectations and commit the appropriate resources. Those resources include adequate budget and staffing levels appropriate for the workload and the tools to assist in managing the security programs—asset/configuration management tools, automated certification and accreditation (C&A) tools, etc.

Separate recommendations with regard to resources are included elsewhere in the Plan. 5.4 Measuring Quality Effectiveness

The State of Hawai`i has instituted numerous improvement programs throughout the years. However, the sustainability and quality of the programs have, in many cases, deteriorated over time. Many programs provide quick-fix or check-the-box solutions and do not address the root causes. For any improvement or strategic plan to provide long-term value and not become shelfware, it must be continuously reviewed and re-evaluated for effectiveness.

It is recommended to review the Plan annually to ensure its relevance and effectiveness related to emerging technologies and threats.

6

INFORMATION ASSURANCE AND CYBER SECURITY DIVISION

6

INFORMATION ASSURANCE AND CYBER SECURITY DIVISION

There are key reasons the IA&CSP-AWG recommends establishing, defining, and documenting formal IA and CS roles and responsibilities. Even if roles have been defined, in this era of emphasis on security governance it is critical to document them as well. If information security roles are not clearly defined with the State and a roles and responsibilities clarification project is still missing in the overall IT/IRM governance structure, it is encouraged to use the following discussion to write a project justification memo to management.

Most departments have no dedicated security staff:

- There is simply not enough time to complete non-security tasks.
- Tasks are often put on hold as security functions are not seen as an immediate need.
- Time-sensitive tasks are completed as quickly as possible with no time for risk assessment, technology assessment, or training.

6.1 GARNER RESPECT AND RESOURCES

Documented role and responsibility statements are advisable for every department/division/branch and attached agencies, not just the IA and CS organization. Those organizational units with fully developed role and responsibility statements will enjoy greater respect and greater resources. Within many of the State's departments, information security is a new or still-undeveloped organizational function.

This means these same organizations are often missing documents that cover information security job descriptions, mission statements, and reporting relationships. When these roles and responsibilities are documented and approved, the information security function will be increasingly recognized as a legitimate and on-going organizational function, worthy of respect and its own share of organizational resources.

6.2 DEMONSTRATE TOP MANAGEMENT SUPPORT

One of the most important reasons to document role and responsibility assignments is to demonstrate top management support. Information security specialists often feel as though many people oppose what they are trying to do. Occasionally information security specialists must take an unpopular position, for example, postponing the cutover to a new software application until appropriate controls can be included. If the information security specialists are not going to be outvoted, outmaneuvered, and otherwise overruled, clearly documented top management support for the information security function must have been documented. With documented and approved roles and responsibilities, information security specialists can prevent or expediently resolve many arguments and get on with their work.

6.3 ESTABLISH FORMAL COMMUNICATION CHANNELS

At many organizations, the information security function has been repeatedly moved from department to department or distributed across many departments. Many of these departments may not have known what to do with the information security function. As a result, departmental management may not have seriously considered the recommendations offered by information security specialists. Consequently, management may have postponed or failed to fund a number of important information security projects. However, when roles and responsibilities for the information security function are specified and approved by top management, all this can quickly change. Then the information security function will have a real home; in other words, it will know where it fits into the organizational structure. In the course of defining a formalized and permanent home for the information security function, the ways that this function works with other internal groups will be defined. Then the information security function will have formal communication channels with top management that can be used to help get important projects underway.

6.4 FOSTER COORDINATED TEAM EFFORT TO SAFEGUARD INFORMATION

One additional important reason to document information security roles and responsibilities involves overcoming an erroneous viewpoint that information security is something that can be handled by specialists in the Information Security Department working alone. The job is way too big and way too important to be left to the Information Security Department. When roles and responsibilities are documented, specific people inside and outside the Information Security Department will be held accountable, and this in turn will cause them to become proactive. Without this accountability, in many cases they will wait until there is a problem, and then do their best to handle whatever has taken place. Today organizations can no longer approach information security with a fix-on-failure mentality. Research studies show that information security is ten times less expensive when it is built into application systems before they go into production instead of when it is added on after the systems have been placed in production. Stated a bit differently, when it comes to information security, proactive planning and management is considerably less expensive than reactive repair and correction efforts.

6.5 ENABLE BETTER ALLOCATION OF ORGANIZATIONAL RESOURCES

Many organizations are now turning to outsourcing firms to handle their information security needs. While some management responsibilities such as making final decisions about information security policies should ultimately rest on the shoulders of internal management, a considerable amount of the security work can be outsourced. If roles and responsibilities are not clearly established at the time that a contract is negotiated, the organization that contracted the outsourcing firm may find itself in a difficult spot. The outsourcing firm may claim that the requested service (such as forensic investigation of a system break-in) is not in the contract, and that the customer must pay an additional fee. All this of course assumes that the outsourcing firm has technically competent people available at the time they are needed.

Of course, other consulting firms can also be called in, but with any of these options, precious time will be wasted negotiating fees, defining the work to be done, etc. While all of these ad-hoc business arrangements are being made, a hacker could be on the loose inside an organization's internal network. To keep losses to a minimum, it is absolutely essential that roles and responsibilities for all important information security activities be defined in advance in outsourcing contracts.

On a related note, if management wishes to outsource some or all of the information security function or if management wishes to retain contractors, consultants, or temporaries to assist with information security, then roles and responsibilities must first be specified. Unless roles and responsibilities have been clearly defined, management will find it difficult or even impossible to draw up requests for proposals, legal contracts, outsourcing agreements, service level agreements (SLAs), and other documents adequately with these third parties. Thus, clear roles and responsibilities can be a significant enabler that allows management to better allocate organizational resources.

6.6 MINIMIZE ASSOCIATED COSTS FOR SECURITY AS A SERVICE (SECAAS)

A related business management reason to establish clear roles and responsibilities is that, in so doing, management will reduce costs to handle information security adequately. Through the specification of job descriptions, management can select and retain people who are adequately qualified, but not over-qualified. This will in turn help to keep salary costs down. Likewise, a number of organizations are increasingly taking the security tasks performed by Systems Administrators and assigning these tasks to new information-security-specific positions like Access Control System Administrator. Not only does this change provide better separation of duties, it also allows the organization to lower costs because the security-specific jobs often pay less than the Systems Administrator jobs. On a related note, when clear roles and responsibilities documentation exists, management will know exactly what types of training programs it should send internal staff to, and this will help avoid wasting resources on training that is not directly relevant to the jobs that the involved individuals perform.

6.7 REDUCE SINGLE POINT OF FAILURE

Rather than eliminating the need for human involvement, the new information systems that organizations are using today (such as ecommerce systems) are increasing the reliance on certain types of people with specialized skills. For example, if a critical technical person were to leave his or her employer abruptly, the organization might be hard pressed to continue certain technical computer operations without this person. This increased reliance on people with highly specialized skills and training can be reduced by backup personnel, cross training, sharing job responsibilities, documenting the work, and other tasks associated with the development of clear information security roles and responsibilities.

The IA field is still in its infancy when compared to the marketing, engineering, or accounting fields. While some interesting new technological solutions to information security problems are now on the market, in most organizations the achievement of effective information security critically depends on people. At this point in the evolution of the technology, many information security problems can only be handled by people. For example, there is no commercially available technological solution to protect against the social engineering (masquerading) threats that all organizations face. All too often, the people within an organization do not understand what management expects them to do, and this in turn will prevent the achievement of information security goals. When roles and responsibilities have been clarified and documented, and selected people are then appropriately trained, they can participate as essential members of the team that handles information security.

6.8 DEMONSTRATE COMPLIANCE

Another good reason to document roles and responsibilities is to demonstrate compliance with internal policies as well as external laws and regulations. Auditors and government examiners are impressed with documentation. It gives them the feeling that things are under control. A surprising number of modern laws include the requirement that information security roles and responsibilities must be specified. For example, in the United States, the Health Insurance Portability and Accountability Act (HIPAA) requires that organizations managing personal health information document information security related roles and responsibilities.

With clear documentation defining information security roles and responsibilities, an organization can show it is operating in a fashion that is consistent with the standard of due care. Being able to demonstrate this consistency may be very important in terms of reducing or eliminating management liability for losses and other problems. This documentation may help with a variety of liability concerns including computer professional malpractice and breach of management's fiduciary duty to protect information assets. One example of an authoritative statement of the standard of due care which includes the requirement to clearly specify information security roles and responsibilities is entitled Generally Accepted Information Security Principles (GASSP).[18]

Demonstrating compliance with the standard of due care can help shield the state from negligence and related liability claims.

6.9 INCREASE EFFICIENCY AND PRODUCTIVITY

Perhaps the most significant reason to establish and document clear roles and responsibilities involves increased productivity. Statistical studies of business economics indicate that about half of productivity growth over time comes from more efficient equipment, and about half comes from better trained, better educated, and better managed labor. Thus, the clarification and publication of information security roles and responsibilities can have a substantial positive impact on productivity, and thereby markedly improve cost savings. The information security field is a new area, and there is still great confusion about who should be doing what. For example, when a worker has his or her laptop computer stolen, to whom should the event be reported? Should a notice be sent to the Information Security Department, the Physical Security Department, or the Insurance Department? Maybe the notice should go only to the worker's manager? Without clear roles and responsibilities, users will unnecessarily spend time figuring out the answers to questions such as these. Likewise, if roles and responsibilities are clarified and documented, employees will not waste their time trying to figure out who to invite to certain meetings or who needs to sign-off on certain proposals.

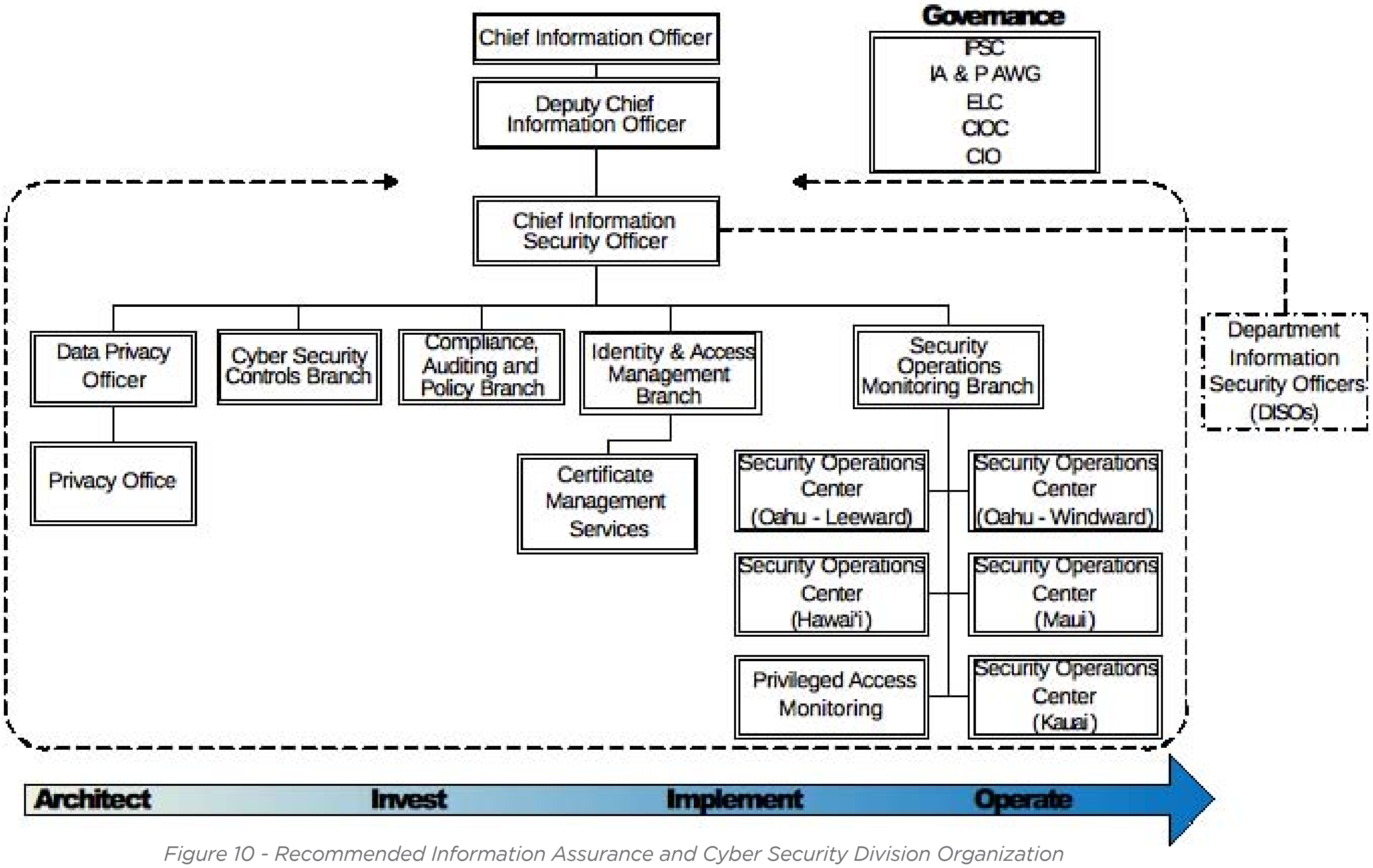

Chief Information Officer
Deputy Chief Information Officer
Governance
PSC
IA & P AWG
ELC
CIOC
CIO
Chief Information Security Officer
Data Privacy Officer
Privacy Office
Cyber Security Controls Branch
Compliance, Auditing and Policy Branch
Identity & Access Management Branch
Certificate Management Services
Security Operations Monitoring Branch
Security Operations Center (Oahu - Leeward)
Security Operations Center (Oahu - Windward)
Security Operations Center (Hawai'i)
Security Operations Center (Maui)
Privileged Access Monitoring
Security Operations Center (Kauai)
Department Information Security Officers (DISOs)
Architect
Invest
Implement
Operate

Figure 10 - Recommended Information Assurance and Cyber Security Division Organization

[18] *National Institute of Standards and Technology, Generally Accepted Information Security Principles for Securing Information Technology Systems. 1996, page 5.*

6.10 CYBER SECURITY CONTROLS BRANCH (CSCB)

Branch Services. Firewall (perimeter and server tier), web application firewall, DDoS protection/mitigation, DLP, IR management, and IDS/IPS

CSCB core functions:

- Data threats
- Access control threats
- Access and authentication controls
- Security gateways (firewalls, WAF, SOA/API, VPN)
- Security products (IDS/IPS, server tier firewall, file integrity monitoring, DLP, antivirus, anti-spam
- New security technology review and recommendations
- Denial of service attacks protection/mitigation
- Secure base services such as DNS and/or DNSSEC, DHCP, NTP, RAS, VPN, SNMP; management network segmentation and security
- Traffic/netflow analysis
- Integration with virtual technology layer

Challenges:

- Fluid network borders/perimeter (Instead of traditional clearly defined network boundaries, the borders between tenant and external networks can be dynamic and potentially blurred in a large-scale virtual/cloud environment.)
- Virtual segmentation of physical servers
- limited visibility of inter-virtual machine traffic
- Non-standard APIs
- Management of many virtual networks (VLAN in a complex environment; reliant on providers' policies and procedures)
- Separation of production and non-production environments
- Logical and virtual segregation of departmental networks/ systems/data

6.11 COMPLIANCE, AUDITING, AND POLICY BRANCH (CAPB)

Branch Services. Internal and/or external penetration test, application penetration test, host and guest assessments, firewall/IPS (security components of the infrastructure) assessments, and virtual infrastructure assessment

CAPB core functions:

- Governance — process by which policies are set and decision making is executed
- Risk management — process for ensuring that important business processes and behaviors remain within the tolerances associated with those policies and decisions
- Compliance — process of adherence to policies and decisions
- Policies can be derived from internal directives, procedures and requirements, or external laws, regulations, standards and agreements.
- Technical compliance audits — automated auditing of configuration settings in devices, operating systems, databases, and applications.
- Application Security Assessments — automated auditing of custom applications
- Vulnerability Assessments — automated probing of network devices, computers and applications for known vulnerabilities and configuration issues
- Penetration Testing — exploitation of vulnerabilities and configuration issues to gain access to a an environment, network or computer, typically requiring manual assistance
- Security/risk rating — assessment of the overall security/ vulnerability of the systems being tested, e.g., based on the OWASP Risk Rating Methodology

Challenges:

- Standards are on different maturity levels in the various sections
- Certification and Accreditation (C&A)
- Boundary definition for any assessments
- Skills of testers/assessors
- Accuracy
- Inconsistent ratings from different individuals/vendors
- Typically limited to known vulnerabilities

6.12 IDENTITY AND ACCESS MANAGEMENT BRANCH (IAMB)

The Identity and Access Management Branch (IAMB) should provide controls for assured identities and access management. IAMB includes people, processes, and systems that are used to manage access to enterprise resources (systems and data) by assuring the identity of an entity is verified and is granted the correct level of access based on this assured identity. Audit logs of activity such as successful and failed authentication and access attempts should be kept by the application/solution.

Branch Services. User-centric ID provider, federated IDs, web single sign-on (SSO), identity provider, authorization management policy provider, electronic signature, device signature, and user-managed access

IAMB core functions:[19]

- Provisioning/de-provisioning of accounts (both cloud and on-premise applications and resources)
- Authentication (multiple forms and factors)
- Directory services
- Directory synchronization (multilateral as required)
- Federated SSO
- Web SSO(e-granular access enforcement and session management; different from federated SSO)
- Authorization (both user and application/system)
- Authorization token management and provisioning
- User profile and entitlement management (both user and application/system)
- Support for policy and regulatory compliance monitoring and/or reporting
- Federated provisioning of cloud applications
- Self-service request processing such as password resets, setting up challenge questions, request for roles/resources, etc.
- Privileged user management/privileged user password management
- Policy management (including authorization management, role management, and compliance policy management)
- Role-based access controls (RBAC) where supported by the underlying system/service

Challenges:

- Insider threat
- Non-repudiation
- Least privilege/need-to-know
- Segregation of administrative (provider) vs. end user (client) interface and access
- Delegation of authorizations/entitlements
- Attacks on identity services such as DDoS
- Eavesdropping on identity service messaging (non-repudiation)
- Password management (communication, retrieval); different requirements across clients
- Resource hogging with unauthorized provisioning
- Complete removal of identity information at the end of the life cycle
- Real-time provisioning and de-provisioning of user accounts
- Lack of interoperable representation of entitlement information
- Dynamic trust propagation and development of trusted relationships among service providers
- Transparency: security measures must be available to the customers to gain their trust
- Developing a user-centric access control where user requests to service providers are bundled with their identity and entitlement information
- Interoperability with existing IT systems and existing solutions with minimum changes
- Dynamically scale up and down; scale to hundreds of millions of transactions for millions of identities and thousands of connections in a reasonable time
- Privacy preservation across multiple tenants
- Multi-jurisdictional regulatory requirements

6.12.1 PUBLIC KEY INFRASTRUCTURE-CERTIFICATE MANAGEMENT SERVICES (PKI-CMS)

PKI is a scalable security control consisting of a set of long-established techniques and standards that provides authentication, privacy, tamper detection, and nonrepudiation. PKI uses public/private keys and includes the infrastructure to manage and maintain the keys, resulting in an electronic environment that is private, confidential, and legally binding. The security industry is moving to PKI and certificates for safe internet transactions. PKI is currently the only technology that provides the required level of data integrity and protection to support electronic government.

Within a public/private cloud implementation is the need for a large-scale PKI deployment, both internal and external, as a part of identity and access management solution.

PKI-CMS core functions:

- Key distribution – how will keys be securely provided to employees, partners, devices, citizens, etc.
- Key management – who should receive keys and under what circumstances
- Key expiration – the default length of time that keys are valid, e.g., two years

[19] *Security as a Service Working Group, "Defined Categories of Service 2011." Cloud Security Alliance, 2011*

- Key rollover – re-issue of keys after a default expiration date is reached

- Key history – retaining a history of all keys issued to an entity can be important to ensure future access to items or functions protected by expired or revoked keys

- Key backup – essential for private encryption keys; not recommended for private signing keys due to the resulting risk of compromising nonrepudiation. (If someone else, for example, a system administrator, can access private signing keys, reliable authentication via the private signing key is no longer possible. However, organizations are advised to retain backups of private encryption keys to protect against technical failures or rogue encryption activity.)

6.13 SECURITY OPERATIONS MONITORING BRANCH (SOMB)

The Security Operations Monitoring Branch (SOMB) provides proactive monitoring of the technology infrastructure and data as it is used and flows into, out of, and within an organization.

Branch Services. Log management, event correlation, security/incident response, scalability, log and event storage, interactive searching and parsing of log data, and logs immutable (for legal investigations)

SOMB core functions:

- Real time log/event collection, de-duplication, normalization, aggregation, and visualization

- Log normalization

- Real-time event correlation

- Forensics support

- Compliance reporting and support

- IR support

- Email anomaly detection

- Reporting

- Flexible data retention periods and policies management, compliance policy management

Challenges:

- Standardization of log formats

- Timing lag caused by translations from native log formats

- Unwillingness of providers to share logs

- Scaling for high volumes

- Identification and visualization of key information

- Usability, segregated by client interface

6.13.1 DELIVER SITUATIONAL AWARENESS

Situational awareness will ensure that the State's enterprise is prepared to act and respond to threats to the network environment that occur hundreds of times a day and are detected by intrusion detection systems, antivirus systems, firewalls, system logs, and access logs. Many IT organizations struggle to compile the resources needed to review the data coming from all of these systems. On a network, security situational awareness is a constant ongoing health check. A zero-day threat can move through a network in seconds, wreaking havoc and putting business-critical systems at risk. The Security Operations Center (SOC) diagnoses attacks through constant monitoring of managed devices on the network and correlates the data in real-time so that operators can see what is happening as it is happening and quickly respond to the threat.

One of the SOC's most powerful functions is that it offers proactive awareness across multiple security-related systems. The SOC can consolidate all reports from the devices and tie the information together into a coherent visual representation to close windows of risk. By looking across the entire enterprise and combining this information with the data in the Network Operations Center (NOC), stealth attacks can be exposed and result in broader, more complete protection for the entire enterprise.

6.13.2 MEET BUSINESS OPERATIONS REQUIREMENTS

While each organization has its own specific security needs, there are some common top-level security information management business requirements that apply to most organizations.

6.13.3 REDUCE RISK AND DOWNTIME

For most networks and businesses, the most important requirement is to keep the network running at an acceptable risk level without downtime. In the past, it may have been possible for an organization to shut down the mail server when an e-mail virus was quickly spreading, but for most organizations, this is no longer an option. Email is a critical business function for delivering services to citizens.

The SOC must support the organization by intelligently and proactively alerting the right people at the right time about critical security events. If this risk can be mitigated before the security event begins attacking critical business systems, then the IT staff will not be forced to shut down those systems. When building the SOC, implement tools that will assist the organization to actively report security incidents in real-time using various methods for alerting, such as pagers, email, or a centralized security management console.

6.13.4 THREAT CONTROL AND PREVENTION

Organizations also must ensure that threats are either prevented or contained. This involves early notification of suspicious activity and the ability to implement a containment mechanism quickly. For example, if a firewall and network management system report the infiltration of a root kit aimed for a targeted host, the operator could be alerted to this root kit and remove it from the target host before the installation process is complete and the host has been compromised.

Organizations may not always be able to prevent threats from infiltrating a network entirely, but they can prevent their spread. Should a network system be compromised, organizations can use the SOC to quickly identify the affected hosts and lock them down from the rest of the network. Routers, switches, and VLANs could be reconfigured to limit the reach of the compromised system and prevent the spread of the threat, thus giving administrators time to remediate the risk before further damage occurs.

To feasibly contain and prevent security incidents, critical alert information must be disseminated quickly and accurately so that administrators can take action. The SOC must be able to validate and correlate alerts and information, put these events in context with the organization's network environment, and provide this critical intelligence to key staff in real-time via various alerting mechanisms such as emails, pagers, or trouble ticketing.

6.13.5 EASE ADMINISTRATIVE OVERHEAD

Organizations have implemented various threat management systems to protect them from the impact of security events. The millions of alerts generated by each individual system—such as intrusion detection systems, antivirus systems, firewalls, operating system logs, and access control systems—are overwhelming. Some organizations engage several staff members to monitor these systems for potential threats. Other organizations simply do not have the staff or budget to monitor them. Additionally, organizations are challenged to find staff with the appropriate skillsets to monitor one or more of these systems.

The SOC should be designed to involve the least amount of human overhead. The SOC provides organizations with the ability to centralize all critical security information into one single centralized console and reduce the need for multiple staff members to manage and monitor the unique devices. The goal is to empower a few administrators with the best information to enable fast, automated responses. Security information management tools that are open and interoperable make this goal easier to accomplish because the disparate data can be correlated and integrated into a single management tool.

6.13.6 PEOPLE AND RESPONSIBILITIES

State departments must agree to share trust and administrative control across departments, divisions, branches, attached agencies, and among partner organizations. For example, a state government may need to have a SOC that collects and manages information from distinct agencies such as the educational system and the police department. Leveraging the organization's security policy standards, responsibilities must be defined including who is responsible for specific tasks and assigning accountability for response and control for each business unit or agency.

As these responsibilities will be defined and communicated, the SOC tools must support these specific roles. Security information management products must provide the ability to federate trust across the departments and deliver near real-time reports based on unique roles.

6.13.7 ESCALATION PATH

A supplementary requirement to the people and responsibility need involves knowing how and when to escalate events. Consider a subsidiary company at a global corporation whose security is managed by the parent company's centralized SOC. If a fast-spreading worm is reported to the SOC and action is immediately required at the subsidiary location but the subsidiary staff is not available when the worm hits due to time zone differences, the SOC operator must know:

- Who to call to receive appropriate approval to enforce the remediation action
- Whether the nature of the threat is critical enough to implement the remediation immediately without approval

It is critical to have a SOC that is integrated within a corporate workflow chain and the Change Management systems. The security information management system should have the ability, based on the criticality of the threat and user's role, to administer the system from within the security console (restart or shut down a system), implement a remediation (e.g., push a patch through a software delivery system), or open a trouble ticket to deploy a technician to address the issue.

6.13.8 AUDIT AND COMPLIANCE SUPPORT

One of the most critical business needs that the SOC can help address is the requirement for auditing to comply with corporate, government, and industry regulations such as HIPAA, IRS 1075, and PCI-DSS. Having quick, flexible access to threat information, identity and access control data, and patch levels is critical for proving compliance. Historically, organizations rely on existing documentation or generate new documentation to prepare for an audit. The process of manually creating documentation for each audit is not only time consuming but prone to errors. SOCs are critical business tools when used for audit and compliance reporting. SOC real-time reports offer an accurate reflection of the system's current state. For example, consider an organization that has a corporate security policy for identity management that requires 30-day password aging for all accounts on all servers. The configuration settings of the servers can be reviewed, but the auditor can also use the SOC log data to search for accounts whose passwords were changed outside of the aging parameters.

6.13.9 INCIDENT RESPONSE AND RECOVERY

When systems are affected by a security event, administrators must be ready to respond as efficiently as possible to limit the damage, determine the root cause, and get the system back up and running quickly. A well-designed SOC empowers administrators to see attacks on the network and helps them leverage incident management tools to pinpoint and remediate problems.

6.13.10 MEET TECHNICAL OPERATIONS REQUIREMENTS

While the business requirements for the SOC are fairly clear and intuitive, organizations must also focus on the underlying technical components and functions needed to deliver on those business requirements.

6.13.11 SPEED OF AGGREGATION AND CORRELATION

Security devices on a network send a great deal of data and alerts. When these are aggregated into a single point for review, the sheer volume can be overwhelming. Depending on the size and complexity of the network, "a lot" can easily translate into hundreds of millions of alerts a day—far too many events for any human to monitor.

The SOC's intelligent console must support the business by sifting through these alerts quickly and prioritizing each event by its severity and threat to the business. Using security information management software, the SOC can provide information that can aid an escalation process to handle the resolution of an event, suppress repeat information, validate alerts to confirm their impact, and prioritize the most critical alerts.

6.13.12 DEVICE AND SYSTEM COVERAGE

A seemingly calm network could be teeming with problems that simply are not being reported properly. If critical devices on the network are not able to work with the security information management products, they are being overlooked and that can lead to dangerous blind spots in the network. For the SOC to deliver real value, it must support all of the security devices, servers, and applications.

Many security information management products offer integration with key threat management tools such as intrusion detection systems, firewalls, routers, operating system logs, and antivirus systems. However, additional sources such as vulnerability management systems, access management systems, business applications, physical security systems, network and system management systems, mainframe security systems, and database systems provide valuable event data that the SOC can leverage. The more data that can be gathered and correlated within the SOC, the more accurate the intelligence will be for mitigating and resolving events.

6.13.13 PROACTIVE INFRASTRUCTURE MONITORING

Zero-day threats, such as malware and viruses, can spread within minutes across the world and throughout an organization. The SOC must provide information in real-time, giving operators the data to take action immediately. At the same time, the SOC also must be able to provide automated actions and resolutions to threats such as restarting systems, initiating a trouble ticket to the help desk to initiate and implement shielding tactics, and working with a patch management system to push patches to vulnerable systems.

6.13.14 UPTIME 24/7, 365 DAYS OF THE YEAR

If a network is running 24/7/365, the SOC must also be up and running in conjunction with the network. Security information management tools help provide the high-availability support needed to meet the always-on requirement.

6.13.15 SUPPORT FOR FEDERATED AND DISTRIBUTED ENVIRONMENTS

Whether they support multiple business units, subsidiaries, or complex partner and customer frameworks, many enterprises run on a federated model. Various groups, sometimes with different business charters, manage portions of the federated network often. When it comes to managing these distributed organizational networks in a holistic manner, the SOC must support federated views and management roles. For example, a subsidiary might report all data to the central SOC, but control for remediation might not be shared with the parent organization. For the SOC to meet those parameters, security information management tools must provide flexible role-based views and accounts to accommodate these differing needs.

6.13.16 FORENSIC CAPABILITIES

Suppose an attack or vulnerability has occurred, action was taken, and the problem was remediated. Good news, right? Yes, but a thorough IT department must ask what can be learned from this incident to help prevent a similar type of attack in the future. Forensic and historical data are maps of what happened and can offer clues as to how the threat worked its way through controls and showed its path of attack. Security information management tools record the event activities report the information in the SOC, which in turn helps prioritize and visualize the data to give administrators the information needed to learn from an incident and prevent it from happening again.

6.13.17 INTELLIGENT INTEGRATION WITH SOCS AND NOCS

A SOC is an incredible business tool, but it should not work as an island. SOCs often live within or beside the NOC, and together these tools provide the statewide network and security view that businesses need for maximum efficiency. Security events can be sent to the NOC from the SOC to communicate the nature of incidents and provide additional intelligence for improved enterprise management. The NOC should have insight from the SOC so it can successfully respond to events and administer security processes and services. This bi-directional

communication is necessary for organizations to respond efficiently and keep risk and damage to a minimum.

6.13.18 THE SOC IN ACTION

With the SOC gathering information, an organization can respond quickly and effectively to security events and tthreats—even internal threats—in real-time. Consider the following example:

A security administrator at a company is in a room in Colorado that is lit by the glow of numerous monitors showing physical areas of the campus. Each monitor displays data that is being reported from the distributed geographic sites of the enterprise. The administrator receives an alert on the main console, clicks a button, and then picks up a phone and places a call to a local operator in California. The administrator responds to a security alert that showed someone improperly sending proprietary information out of the company. In just a few seconds, the user's access is blocked, the local operator is dispatched to remove the user from the building, and an investigation into the incident is initiated.

Cost avoidance. Building the SOC will cost far less than not detecting, preventing, and responding to attacks.

Cost efficiencies. Many of the SOC processes or technologies can help automate functions already taking place within the organization. By accepting a new data feed and producing automated reporting, a SOC can often save the organization money by reducing manual effort.

Cost sharing. Departments within the State either do not monitor or rely on untrained individuals are tasked with the responsibilities outlined for the future SOC. Are those groups willing to outsource these responsibilities to the SOC? Having other organizations help to foot the bill can minimize the overall impact to all.

Revenue/Cost Recovery. SOC services can be offered to all State departments. There is more work in determining separation of information among departments and other business aspects, but cost recovery can be leveraged to perform security services for all state departments.

6.13.19 MULTIPLE SECURITY OPERATIONS CENTERS

The current vision for the State's new IT/IRM infrastructure is a combination of five Shared Service Centers (SSCs) across five of the Hawai`ian islands (Oahu: two; Kauai: one; Maui: one; and Hawai`i: one).

Each of these Shared Service Centers will contain a manned security operations center to provide 7/24/365 rotational, proactive monitoring of the State's infrastructure and data.

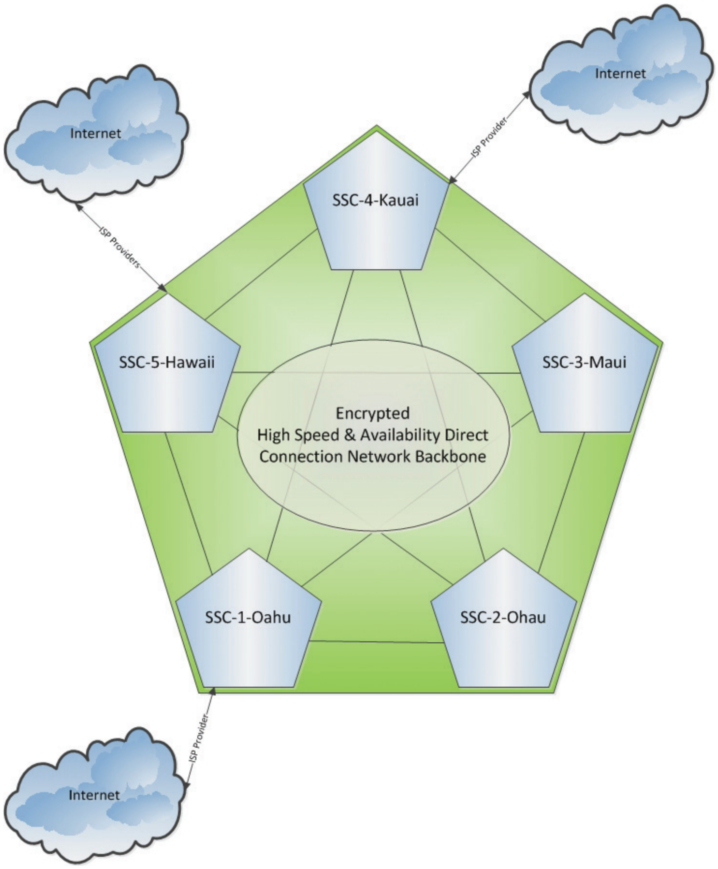


Figure 11: Shared Service Centers Vision for the State of Hawai'i

6.13.20 PRIVILEGED ACCESS MONITORING

Privileged Identity Management (PIM) is a domain within Identity and Access Management focused on the special requirements of powerful accounts within the IT infrastructure of an enterprise. It is frequently used as an Information Security and governance tool to help companies meet compliance regulations and to prevent internal data breaches by using privileged accounts.

6.14 STATE OF HAWAI`I DATA PRIVACY PROGRAM

Data Privacy and IA are often confused as the same solution. IA and CS are the tools, personnel, and monitoring, and data privacy is the result.

There are various U.S. state and international laws which govern the disclosure of personal, private, or financial information to individuals who do not have the need to know that information to properly perform duties associated with their daily work:

- Gramm-Leach-Bliley Act (GLBA)
- Health Insurance Portability and Accountability Act (HIPAA)
- Payment Card Industry Data Security Standard (PCI DSS)
- Australia's Privacy Law
- Canada's Privacy Law
- European Union (EU) Directive on Data Protection
- Organization for Economic Cooperation and Development (OECD)

These laws sometimes conflict with the concept of open data; it is therefore imperative that any policies, procedures and standards developed as an IA and CS solution take privacy and open data initiatives into consideration.

More details on the IT/IRM Privacy compliance are available in the IT/IRM Privacy Plan.

7 ASSUMPTIONS

8 CONSTRAINTS

9 INFORMATION ASSURANCE AND CYBER SECURITY INITIATIVES

10 GUIDANCE FOR PROGRAM MANAGERS AND PROJECT LEADS

11 CONCLUDING REMARKS

7 ASSUMPTIONS

In the development of the Plan, the following assumptions were made:

- A Enterprise Risk Management philosophy and processes will be put into place.
- An IA and CS Program Management Plan will outline the details of the necessary infrastructure to implement a SecaaS model successfully.
- The CIOC and government support will prioritize resources (staff and budget) to support the recommendations of the Plan.
- An Information Assurance and Cyber Security Division will be created under the State's CIO, led by a CISO.
- Each state department (and attached agencies where applicable) will designate a Department Information Security Officer as a primary point of contact for issues, concerns, and projects related to IA and CS.

Development of the Plan and implementation of its recommendations are long-term objectives that will continue to be refined through progressive elaboration. As IT Security is a constantly evolving field, the Plan will be updated continuously to reflect changes.

The concepts and strategies identified in the Plan will remain true barring additional requirements and mandates that may affect the Plan.

Implementation of the recommendations set forth in the Plan will not completely eliminate risk; this is not possible. The intent of the Plan is to reduce risk to an acceptable level. Residual risk will be manageable and should be acceptable if the recommendations of the Plan are adopted.

8 CONTRAINTS

In the development of the Plan, the following constraints were recognized:

- Magnitude of the effort. The creation of the Plan encompasses a vast number of technologies and requirements along with associated risks and is bound by the following scope constraints:
  - The number of risks to the environment is immense.
  - Technology and the associated risks are constantly changing.
  - Security requirements continue to increase.
- Resources. As with any effort, staffing and budget concerns must always be considered. The development of the Plan is bound by the following resource constraints:
  - Decreasing budget environment
  - Competing priorities vying for the same resources
  - Lack of resources to remediate identified issues
  - Increasing demands on available resources
- Implementation Challenges. Implementation of the Plan will require a great deal of effort and cooperation to achieve the level of security desired and is bound by the following implementation constraints:
  - Legacy system concerns
  - Policy communication and enforcement
  - SDLC challenges; build security into the design
  - Departmental mission impacts

9

INFORMATION ASSURANCE AND CYBER SECURITY INITIATIVES

In preparing the Plan, the IA&P-AWG team evaluated legislated requirements, prior studies and planning documents, department and organizational commitments, best practices, and the experience and knowledge of the team members to build a list of prioritized initiatives; a strategy that will help focus State's improvement efforts.

Detailed descriptions of the initiatives are in "Appendix A - Information Assurance and Cyber Security Program Strategic Investment Initiatives"

10

GUIDANCE FOR PROGRAM MANAGERS AND PROJECT LEADS

Each project initiated will adhere to the following tenants, goals, and objectives:

- Acquire and implement common enterprise security tools to maximize cost reductions with economies of scale.
- Technologies, tools, and solutions must—to the maximum degree possible—be able to be integrated in a fashion that provides automated enterprise-wide visibility into the security posture of State's information and information systems.
- Standardization decisions will be formally documented and the resulting standard, or specific product in cases where there are no standards-based solutions available, will be incorporated into the State's Enterprise Architecture Technical Reference Model (TRM).
- Consideration should be given to leveraging and integrating existing investments to the greatest extent possible to conserve available constrained budgetary resources.
- Solutions should not be conceived in a vacuum or stovepipe fashion where consideration is given towards addressing a single risk or requirement. The way other solutions collectively help to mitigate that risk while also effectively contributing towards mitigating a variety of other risks to achieve the greatest cost efficiency possible are factors.
- To achieve progress in a timely manner and to develop and maintain appropriate levels of expertise and support for each enterprise initiative, the Centers of Excellence (CoE) concept should be implemented. The CoE concept should be inclusive of the departments, divisions, and branches to participate in the incorporation of their respective requirements, vetting of all requirements, and majority consensus approach towards selecting the final solutions to include involvement in the testing and evaluation processes that result in formal standardization decisions incorporated into the TRM.

11 CONCLUDING REMARKS

Under the leadership of OIMT, the IA& P-AWG has prepared this document that recommends both a strategic and tactical approach to IT security improvements that address many of the systemic weaknesses of the State's security posture while recognizing the technical, financial, and cultural needs of State's organizational subcomponents.

In preparing the Plan, the IA&P-AWG evaluated legislated requirements, prior studies and planning documents, department and organizational commitments, industry best practices, and the experience and knowledge of team members to build a list of prioritized initiatives—a strategy—that will help to focus improvement efforts.

By adopting the recommended initiatives identified, the State's security posture can be significantly improved. Initiatives have been prioritized by the IA&P-AWG to provide the greatest immediate benefit to State. All of the recommended initiatives represent significant investments of both capital and human resources; however, the benefits derived in implementing these initiatives greatly outweigh the potential risks associated with damage to State's reputation, mission activities, and public trust.

APPENDIX A – INFORMATION ASSURANCE AND CYBER SECURITY PROGRAM STRATEGIC INVESTMENT INITIATIVES

APPENDIX A – INFORMATION ASSURANCE AND CYBER SECURITY PROGRAM STRATEGIC INVESTMENT INITIATIVES

A summary of each program investment is provided below that includes:

- The investment name
- Project name (where it exists in current project documents)
- The investment priority as determined by the Information Assurance Working Group; and change the last sentence on the page to read: “Risk information has been redacted for security concerns and cost estimates are not included as they are
- pending review.”
- Summary description
- Associated risk categories
- Maturity levels
- Performance periods
- Total cost remarks

For ease of distinguishing the types of investment initiatives, the tables are color-coded:

- Green—initiative is presently underway
- Purple—initiative is planned but is awaiting funding
- Blue—represents new high priorities reported to the CIOC
- Grey—represents long-term initiatives based on future IT/IRM transformation initiatives. [20]

Risk-specific details have been redacted for security concerns and cost estimates are not included as they are pending review.

Table 11 – Description of Investment Initiatives Tables

<table>
<tr><td colspan="3">Investment Name:</td><td colspan="3">1</td></tr>
<tr><td>Priority:</td><td><b>2</b></td><td colspan="2">Likelihood:</td><td colspan="2">Impact:</td></tr>
<tr><td colspan="4">Current Maturity Level:</td><td colspan="2"><b>5</b></td></tr>
<tr><td colspan="2">Funding Source:</td><td colspan="4"><b>6</b></td></tr>
<tr><td colspan="6">Summary Description: <b>7</b></td></tr>
<tr><td colspan="6">Risk (if not implemented): <b>8</b></td></tr>
<tr><td colspan="4">Level of Control</td><td>Performance Period</td><td>Cost Estimate</td></tr>
<tr><td colspan="4"></td><td><b>9</b></td><td><b>10</b></td></tr>
<tr><td colspan="5">Estimated Total Cost:</td><td><b>11</b></td></tr>
</table>

Legend

1. Investment Name—title of investment used for tracking purposes

2. Priority—level of priority:

- Critical: should be implemented immediately
- High: implementation within 6–12 months
- Medium: implementation within 12-18 months
- Low: implementation within 18+ months
- As required: when Enterprise IT transformation requires new security investment
- TBD: to be determined

3. Risk Assessment: Likelihood—how likely an event would occur if without the benefit of the protection of the investment.

4. Risk Assessment: Impact—the impact an event will have on the State's infrastructure and data if the investment is not implemented

5. Current Maturity Level—the maturity level currently implemented within the state.

6. Funding Source—expected source of state funding

7. Summary Description—brief description of the investment

8. Risk—description of the risk to the states computing infrastructure and data if the investment is not implemented.

9. Level of Control: Performance Period—the expected timeframe to architect, invest, implement, and operate the level of control.

10. Level of Control: Cost Estimate—cost estimate based on data gathered from vendors or previous state implementation for the level of control described and the period of performance. These costs include the hardware, software, consultant assistance and maintenance costs over the Performance Period.

11. Estimated Total Cost—total cost estimate for the investment, over the lifetime of the *Business and IT/IRM Strategic Plan*[21] (ten-year period). Industry best practices indicate that IA and CS budgets be based on eight- to ten-percent of the annual total IT budget spending. These estimates also take into consideration the economies of scale by engaging vendors with statewide enterprise-level purchases/licensing agreements; a cost savings across all State departments can be achieved.

[21] These costs do not reflect the precise cost of the investment and are given in 2012 dollars. They do not reflect changes in inflation nor do they reflect FTE expenses to implement and operate the investment, and will be subject to change when the investment is released for a Request for Proposal.

Investment Name:	Network Data Loss Prevention (nDLP)				
Priority:	TBD	Likelihood:	Almost Certain	Impact	Catastrophic
Current Maturity Level:	Optimized				
Funding Source:	Inderpartmental Transfers - U				
Summary Description: This investment implements a system to protect Personally Identifiable Information (PII) and other sensitive data from inadvertently leaving State's network without authorization or other appropriate protections.					
Risk (if not implemented):					

Level of Control		Performance Period	Cost Estimate
Triage	Implemented software, processes, procedures and support personnel to protect Personally Identifiable Information (PII) and other sensitive data types from unauthorized use, access, disclosure, and to report on any perceived or confirmed exposure of PII.	FY 2012–13 (Dependencies: None)	
Enterprise	Implementation of data loss prevention technology to the department, attached agencies and additional areas on OneNet.	FY 2013–16	
Estimated Total Cost			

Investment Name:		IT Security Policy Assistance			
Priority:	**5**	Likelihood:	Possible	Impact	Insignificant
Current Maturity Level:		Unknown			
Funding Source:		TBD			

Summary Description: This investment will support the development and promulgation of revised policies better articulating the responsibilities of organizational components to more effectively manage their IT security programs, internal security configurations and risks.

Risk (if not implemented):

Level of Control	Performance Period	Cost Estimate
Assist state with development, review and implementation of a common set of security policies, guidelines, standards and procedures.	FY 2012–13 (Dependencies: None)	
Estimated Total Cost		

Investment Name:	Network Data Loss Prevention (nDLP)				
Priority:	TBD	Likelihood:	TBD	Impact	TBD
Current Maturity Level:	Unknown				
Funding Source:	TBD				
Summary Description: This investment protects data stored on state owned mobile devices by allowing state employees traveling overseas to use devices with no state data stored on them permanently.					
Risk (if not implemented):					

Level of Control	Performance Period	Cost Estimate
Purchase mobile device pool (laptops, phones, etc.)	FY 2012–13 (Dependencies: None)	
Image Standardization for mobile devices	FY 2013–23	
Estimated Total Cost:		

Investment Name:	Data-at-Rest (DAR) Encryption				
Priority:	**5**	Likelihood:	TBD	Impact	TBD
Current Maturity Level:	Unknown				
Funding Source:	TBD				
Summary Description: This investment protects data resident on assets outside of the physical protection boundaries of State’s facilities – typically resident on mobile devices that can be lost or stolen.					
Risk (if not implemented):					

Level of Control	Performance Period	Cost Estimate
DAR encryption solution implemented on all endpoint computing devices.	FY 2013–23 (Dependencies: None)	
DAR encryption solution implemented on all removable media (USB, Optical, Magnetic, etc.) containing persisting sensitive information.	FY 2014–23	
DAR encryption on server based data and databases.	(Dependencies: None) FY 2013–23	
Estimated Total Cost:		

Investment Name:	Critical Infrastructure Risk Assessment				
Priority:	5	Likelihood:	TBD	Impact	TBD
Current Maturity Level:	Unknown				
Funding Source:	TBD				
Summary Description: Hire a respected third party organization to perform security audits to determine security baseline across all state departments and identify gaps in security.					
Risk (if not implemented):					

Level of Control	Performance Period	Cost Estimate
Perform third party security audit	FY 2013	
Review study and develop plan of action and milestones (POA&M)	FY 2013	
Execute POA&M based on external audit gaps	FY 2013-2023	
Perform biennium external security audit	FY 2014-2023	
Estimated Total Cost:		

Investment Name:	Server Configuration Stability Monitoring				
Priority:	**5**	Likelihood:	TBD	Impact	TBD
Current Maturity Level:	Unknown				
Funding Source:	TBD				
Summary Description: This investment helps identify alterations in operating system, database, applications and security configurations that result in State's assets being more susceptible to threats.					
Risk (if not implemented):					

Level of Control	Performance Period	Cost Estimate
Implement within ICSD server base	FY 2013 (Dependencies: None)	
Implement statewide all servers	FY 2014-23 (Dependencies: None)	
Estimated Total Cost:		

Investment Name:	Media Disposal and Destruction				
Priority:	**5**	Likelihood:	Possible	Impact	Insignificant
Current Maturity Level:	Unknown				
Funding Source:	TBD				
Summary Description: Purchase device(s) or a service to destroy media containing state sensitive or personal data.					
Risk (if not implemented):					

Level of Control	Performance Period	Cost Estimate
Purchase media destruction equipment	FY 2013	
Enterprise level hardware retention agreements with vendors	FY 2014-23	
Estimated Total Cost:		

Investment Name:	Information Assurance and Cyber Security Professional Training				
Priority:	**5**	Likelihood:	Possible	Impact	Insignificant
Current Maturity Level:	Unknown				
Funding Source:	TBD				
Summary Description: Provide training and certification resources for IA and CS Division and DISOs.					
Risk (if not implemented):					

Level of Control	Performance Period	Cost Estimate
Initial Training & Certification Testing	FY 2013–23	
Certification Maintenance	FY 2013–23	
Estimated Total Cost:		

Investment Name:	Enterprise Domain Name Service Security (DNSSEC)				
Priority:	**5**	Likelihood:	Possible	Impact	Insignificant
Current Maturity Level:	Unknown				
Funding Source:	TBD				
Summary Description: A set of extensions to DNS that provide to DNS clients (resolvers) origin authentication of DNS data, authenticated denial of existence, and data integrity.					
Risk (if not implemented):					

Level of Control	Performance Period	Cost Estimate
Initial Training & Certification Testing	FY 2013–23	
Certification Maintenance	FY 2013–23	
Estimated Total Cost:		

Investment Name:	Enterprise Domain Name Service Security (DNSSEC)				
Priority:	**5**	Likelihood:	Possible	Impact	Insignificant
Current Maturity Level:	Unknown				
Funding Source:	TBD				
Summary Description: Provide means to secure, trusted communications between multiple entities across unsecure public networks using public/private cryptography key pair.					
Risk (if not implemented):					

Level of Control	Performance Period	Cost Estimate
Pilot Implementation of PKI and Certificate Authority technology within ICSD	FY 2013 (Dependencies:	
Deployment and support of PKI across all state agencies.	AD infrastructure including internal certificate authority)	
Estimated Total Cost:	FY 2014-23 (Dependencies: Enterprise wide AD deployment and I&A Management)	

Investment Name:	Automated Compliance Monitoring and Reporting				
Priority:	**5**	Likelihood:	Possible	Impact	Insignificant
Current Maturity Level:	Unknown				
Funding Source:	TBD				
Summary Description: This investment helps identify alterations in security configurations that result in State’s assets being more susceptible to threats.					
Risk (if not implemented):					

Level of Control	Performance Period	Cost Estimate
Implemented continuous monitoring of security configurations on ICSD servers.	FY 2013-16 (Dependencies: Implementation of the IRM Asset Discovery and Inventory solution)	
Implemented continuous monitoring of security configurations on Department desktops and servers and department/division/bureau/office servers.	FY 2014-23 (Dependencies: Implementation of the IRM Asset Discovery and Inventory solution)	
Estimated Total Cost:		

Investment Name:	Personally Owned Remote Device OneNet Access				
Priority:	**5**	Likelihood:	Possible	Impact	Insignificant
Current Maturity Level:	Unknown				
Funding Source:	TBD				

Summary Description: Allow personally owned devices, (desktops, laptops, iPhone, iPad, Android tablets, etc.) access into state's IT Infrastructure, while still providing secure communications between the mobile device and state owned systems.

Risk (if not implemented):

Level of Control	Performance Period	Cost Estimate
Initial pilot project to include two-three state departments totaling no more than 500 mobile devices (one-time cost)	FY 2013	
Department-wide implementation and support (maximum 25,000 mobile devices)	FY 2014-23	
Citizen access to OneNet for access to public and private cloud services	FY 2015-23	
Estimated Total Cost:		

Investment Name:	Personal Mobile Device Management				
Priority:	**5**	Likelihood:	Possible	Impact	Insignificant
Current Maturity Level:	Unknown				
Funding Source:	TBD				

Summary Description: Remotely manage personally owned mobile devices to allow for secure communications between the device and the State's network, systems and applications.

Risk (if not implemented):

Level of Control	Performance Period	Cost Estimate
Initial Pilot project to include 2-3 state departments totaling no more than 500 mobile devices (one-time cost)	FY 2013	
Department wide implementation and support (max 25,000 mobile devices)	FY 2014–23	
Estimated Total Cost:		

Investment Name:	Enterprise Security Operations Center(s)

Priority:	**5**	Likelihood:	Possible	Impact	Insignificant

Current Maturity Level:	Unknown
Funding Source:	TBD

Summary Description: This investment supports State's ability to monitor threats presented by data loss from mission critical systems resulting from miss-configurations or unauthorized data transfers initiated by malicious actors.

Risk (if not implemented):

Level of Control	Performance Period	Cost Estimate
Implemented virtual capability for security event and incident monitoring, detection, reporting and response activities at Department level.	FY 2013–23 (Dependencies: None)	
Implemented integrated capability for vulnerability and security configuration compliance monitoring, threat management functions and penetration testing activities at Department level.	FY 2012–23 (Dependencies: Implementation of the IRM Asset Discovery and Inventory solution)	
Implemented integrated capability for security event and incident monitoring, detection, reporting and response activities at Department and bureau/office level.	FY 2014-23 (Dependencies: None)	
Estimated Total Cost:		

Investment Name:	Computer Security Incident Response Team (CSIRTs)				
Priority:	**5**	Likelihood:	Possible	Impact	Insignificant
Current Maturity Level:	Unknown				
Funding Source:	TBD				

Summary Description: This investment improves computer incident detection, reporting, prioritization, response, collaboration, and resolution capabilities throughout the Department.

Risk (if not implemented):

Level of Control	Performance Period	Cost Estimate
Upgrade forensics analysis tools	FY 2013	
Forensics tools and analysis training	FY 2013-23	
Estimated Total Cost:		

Investment Name:	Enterprise Penetration Testing Capability				
Priority:	**5**	Likelihood:	Possible	Impact	Insignificant
Current Maturity Level:	Unknown				
Funding Source:	TBD				
Summary Description: This investment will define, document, and implement a core capability enabling State to assess the effectiveness of security controls, when evaluated from an attacker’s perspective, to deny the compromise of mission critical systems.					
Risk (if not implemented):					

Level of Control	Performance Period	Cost Estimate
Penetration Testing Certification (10 FTEs)	FY 2013–23	
Penetration Testing Software and Licensing	FY 2013–23	
Estimated Total Cost:		

Investment Name:	Common Standards for Protecting Privacy and Other Sensitive Data				
Priority:	**5**	Likelihood:	Possible	Impact	Insignificant
Current Maturity Level:	Unknown				
Funding Source:	TBD				
Summary Description: This investment will fund the development and promulgation of common standards for protecting privacy and other sensitive information.					
Risk (if not implemented):					

Level of Control	Performance Period	Cost Estimate
Implemented and promulgated common standards w/catalog of security products and services for protecting sensitive data throughout State departments, divisions, branches and offices.	FY 2013– 23	
Estimated Total Cost:		

<table>
<tr><td colspan="3">Investment Name:</td><td colspan="3">Secure Application Testing Program</td></tr>
<tr><td>Priority:</td><td><b>5</b></td><td>Likelihood:</td><td>Possible</td><td>Impact</td><td>Insignificant</td></tr>
<tr><td colspan="3">Current Maturity Level:</td><td colspan="3">Unknown</td></tr>
<tr><td colspan="3">Funding Source:</td><td colspan="3">TBD</td></tr>
<tr><td colspan="6">Summary Description: This investment develops and implements solutions and testing regimens within application lifecycle development processes to help identify vulnerabilities and weaknesses in all custom source code (Forge.mil and RDE&T model).</td></tr>
<tr><td colspan="6">Risk (if not implemented):</td></tr>
<tr><td colspan="4">Level of Control</td><td>Performance Period</td><td>Cost Estimate</td></tr>
<tr><td colspan="4"><b>Developed and implemented statewide an Enterprise Application Security Testing regimen with standardized processes and procedures for all custom source code, web applications and databases</b></td><td>FY 2014–23</td><td></td></tr>
<tr><td colspan="4"><b>Estimated Total Cost:</b></td><td></td><td></td></tr>
</table>

Investment Name:	Enterprise Identity and Access Management				
Priority:	**5**	Likelihood:	Possible	Impact	Insignificant
Current Maturity Level:	Unknown				
Funding Source:	TBD				
Summary Description: This investment develops and implements a strong logical authentication for network logon and in addition supports the use of those credentials for application logon, digital signatures, and encryption.					
Risk (if not implemented):					

Level of Control	Performance Period	Cost Estimate
Pilot account management process standards developed and supported by the solution; the processes and solution support the monitoring and reporting on account management activities and changes to accounts and account privileges.	FY 2013	
Account management processes and solution are defined, documented and integrated with the Enterprise Directory Services (Active Directory (AD)) and associated AD Operational Standardization; and all end-user computers are routinely monitored for unauthorized password changes to local accounts and unauthorized changes to local user groups.	FY 2014–23 (Dependency: Implementation of single state AD infrastructure)	
As the state IT/IRM resources move to a public/private cloud environment it becomes necessary to implement	FY 2015–23 (Dependency: Implementation of state public/private	
Estimated Total Cost:		

Investment Name:	Network-based Access Control (NAC)				
Priority:	**5**	Likelihood:	Possible	Impact	Insignificant
Current Maturity Level:	Unknown				
Funding Source:	TBD				
Summary Description: This investment will implement a network-based solution to prevent unauthorized systems from inappropriately accessing State's network(s).					
Risk (if not implemented):					

Level of Control	Performance Period	Cost Estimate
Selected and deployed adequate network-based NAC solutions throughout selected bureau and office internal Local Area Networks (LANs). The network-based NAC is integrated with the host-based NAC solution within the Common End-Point Protection Platform investment.	FY 2013–16	
Deployed adequate network-based NAC solutions throughout all bureau and office internal Local Area Networks (LANs). The network-based NAC is integrated with the host-based NAC solution within the Common End-Point Protection Platform investment.	FY 2015–23	
Estimated Total Cost:		

Investment Name:	Network Security Upgrade				
Priority:	**5**	Likelihood:	Possible	Impact	Insignificant
Current Maturity Level:	Unknown				
Funding Source:	TBD				
Summary Description: This investment will implement a network-based solution to identify and automatically prevent attacks targeting State's networks and resources.					
Risk (if not implemented):					

Level of Control	Performance Period	Cost Estimate
Pilot implementation of new technology network perimeter security devices	FY 2013–14	
Full statewide implementation of new technology	FY 2014–16	
Estimated Total Cost:		

Investment Name:	Secure Wireless Access Solution				
Priority:	**5**	Likelihood:	Possible	Impact	Insignificant
Current Maturity Level:	Unknown				
Funding Source:	TBD				
Summary Description: This investment will support the selection, development, implementation, and migration to a standardized statewide wireless access solution(s) for both remote and local area network access.					
Risk (if not implemented):					

Level of Control	Performance Period	Cost Estimate
Selected, developed, implemented and migrated pilot organizations to a statewide wireless access solution performed incrementally in coordination with all remote access related initiatives/projects.	FY 2013–14 FY 2014–16	
Migrate all organizations to a statewide wireless access solution performed incrementally in coordination with all remote access related initiatives/projects.		
Estimated Total Cost:		

Investment Name:	Data in Motion Encryption				
Priority:	**5**	Likelihood:	Possible	Impact	Insignificant
Current Maturity Level:	Unknown				
Funding Source:	TBD				
Summary Description: This investment will support the design and implementation of secure internal network communications between mission-critical servers and locations.					
Risk (if not implemented):					

Level of Control	Performance Period	Cost Estimate
Pilot between data centers		
Implemented a common end-to-end encryption solution for the enterprise that encompasses all devices (desktops, laptops, mobile devices, workstations, servers, routers, etc.)	FY 2013–14 (Dependencies: None)	
Estimated Total Cost:		

Investment Name:	Statewide User Education, Training, and Awareness				
Priority:	**5**	Likelihood:	Possible	Impact	Insignificant
Current Maturity Level:	Unknown				
Funding Source:	TBD				
Summary Description: This investment enhances the department-wide IT security awareness and training program utilizing more frequent and targeted offerings in order to increase the state of security at State through improved education.					
Risk (if not implemented):					

Level of Control	Performance Period	Cost Estimate
Planned and designed an enhanced training program and delivered department-wide to reduce the number of security-related incidents and increase the state of security at State by institutionalizing the State IT Security Policy Handbook.	FY 2013 (Dependencies: None)	
Improved training program annually to better target reducing largest security-related incident types	FY 2013–23 (Dependencies: None)	
	FY 2013–23 None)	
Estimated Total Cost:		

PRIVACY PLAN

TABLE OF CONTENTS

1. EXECUTIVE SUMMARY....5

2. INTRODUCTION....7

2.1 Purpose 8

2.2 Scope.......... 8

2.3 Associated Documents....8

2.4 The Threat....8

2.5 Program Mission....9

2.6 Program Vision....9

2.7 Program Goals....10

2.8 Fair Information Practices....11

2.9 Health Data....13

2.10 Criminal Justice Data....13

2.11 Protection of Data belonging to Minors....13

2.12 Privacy Training and Awareness....13

2.13 Privacy Risk Management and Compliance Documentation....13

3. MAJOR SCHEDULED EVENTS (MILESTONES AND REOCCURRING)....15

3.1 Privacy Program Milestones (Non-staffing)....16

3.2 Privacy Program Milestones (Staffing)....17

4. COSTS....18

4.1 Identify Program Costs (Including Costs Approved by the OIMT)....19

4.2 Critical Success Factors....21

4.3 Program Staff Deliverables....21

4.4 Assumptions....22

4.5 Technical Constraints....22

5. RISKS....23

6. STAFFING PLAN....25

6.1 FY 2014-15 Team Structure (Notional)....26

7. RESOURCE REQUIREMENTS....27

7.1 Roles and Responsibilities....28

7.2 Program Staffing Plan....30

7.3 Contract Services Requirements....31

7.4 Staffing Plan for Ongoing Operations....31

8. DELIVERABLES....32

8.1 Program Deliverables....33

8.2 Program Management Deliverables....33

9. PROGRAM CONTROLS....35

9.1 Scorecards (Quarterly and Annually)....36

9.2 FISMA Privacy Annual Report (Annual)....36

9.3 Annual Review of System of Records Notices and Automatic Requirement to Write PIA for New Systems within 90 Days....36

9.4 Review and Processing of Privacy Impact Assessments (PIAs) for All Electronic Systems....36

9.5 Annual Survey/Review for Reducing Use of SSNs and Other PII in Conducting OIMT Business....36

9.6 Review Departmental Enterprise Architecture Repository (DEAR), Cyber Security Assessment Management (CSAM) and Privacy Websites for Compliance Annually....36

9.7 Perform Privacy Technical Evaluations Annually....36

9.8 Privacy and Security....36

REFERENCES.............. 37

GLOSSARY OF ACRONYMS....39

FIGURES

Figure 1: Privacy Assessment Cycle....10

Figure 2: Kaizen Continuous Improvement....11

Figure 3: Privacy Program Team Organization Fiscal Year 2014-15....26

TABLES

Table 1: Milestones (Non-staffing)....16

Table 2: Milestones (Staffing)....17

Table 3: Estimated Program Costs....19

Table 4: Annual FY-2014 Operating Costs....19

Table 5: Estimated Additional Funding Requirement (FY-2015)....20

Table 6: Risks....24

Table 7: Roles and Responsibilities....28

Table 8: Program Staffing Plan by OIMT Entity....30

Table 9: Minimum Program Staffing Plan....31

Table 10: Contractor Requirements....31

Table 11: Operational Support Requirements....31

Table 12: Program Deliverables....33

Table 13: Program Management Deliverables....33

1. EXECUTIVE SUMMARY

1. EXECUTIVE SUMMARY

A review of the State's Privacy Program by the Office of Information and Management Technology (OIMT) concluded that there is currently insufficient funding and staff support to meet today's Privacy requirements. Most agencies do not have a dedicated privacy officer, and consistent methods are not used across the State to protect personally identifiable information (PII) as defined in HRS §487(N), HRS §487(R) and in the Federal standards as required.

This document describes the structure and method of the establishment of an Executive Branch Privacy Office and program organization. This document is a living document that will be kept current throughout the course of the program. The intended audience for this document is currently all Executive Branch Agencies.

The OIMT maintains the information technology (IT) infrastructure for a large portion of the state agencies under the Officer of the Governor of the State of Hawai`i.

In addition to guidance and directives regarding IT infrastructure, the Chief Privacy Officer (CPO), under the Chief Information Officer (CIO), also provides guidance, oversight, and assistance regarding privacy.

The CPO is responsible for formulating overarching State privacy policy and overseeing agency/office implementation and achieving the State's strategic goals in support of the OIMT vision for enterprise IT privacy performance. Value to both the customer and the public is promoted through the use of State-approved standards and industry best practices. The CPO will also interface with the Information Privacy and Security Council (IPSC) and assist them with development of their deliverables as well as act as a subject matter expert (SME) when needed.

2. INTRODUCTION

2. INTRODUCTION

2.1 PURPOSE

Protecting privacy is a core need for every State agency, and it is best attained when it is an integral part of the agencies' business operations. Privacy must be considered as part of the up-front appraisal of policy and programmatic decision-making as well as business operations, application development, and associated activities; it should not be an afterthought. Privacy stewardship and governance are keys to a successful privacy program and can reduce the risk that government programs erode privacy protections and ultimately lose the public's trust.

Privacy is a broad and complex concept that arises in a variety of contexts: information privacy (rules that govern collection, handling, and use of PII), bodily privacy (protection against assault of a person's physical being), territorial privacy (limits on the ability to encroach into another person's environment), and communications privacy (protection of mail, telephone, and email). Laws and regulations tend to focus primarily on information privacy issues, particularly as organizations increasingly use technology to collect, process, and store PII on employees and the public. However, information privacy is only one of many privacy issues that agencies must manage.

This document will provide a framework to improve how the State protects PII it is responsible for and also defines the major steps needed to build a consistent and comprehensive privacy program.

Examples of the proposed privacy program requirements include the following:

- Ensure that data at rest and in motion adhere to best practices and federal regulations.
- Ensure success throughout the State with reviews, protection, and reporting requirements under privacy elements including the Federal Information Security Management Act (FISMA) and State of Hawai`i Act 10.
- Oversee privacy training programs and other types of outreach for both agency Privacy Officers and for all departmental personnel.
- Promote analysis, expertise, and remediation efforts for breaches, and partner with security staff in the development of breach prevention measures.
- Monitor all agencies' website PII content and verify their privacy notices for statutory compliance.
- Coordinate with others in promoting adherence to sound privacy practices and procedures, both within and beyond the Executive Branch.
- Establish standards and guidelines for systems logging, cookies, web beacons, statistical aggregation, inclusion, disclaimers for external links, and sharing of information between agencies.
- Serve as chief privacy advisory to senior agency personnel.
- Partner and serve as advisory to the IPSC on privacy subject matters.

2.2 SCOPE

This document will define scope and structure for the privacy program for all Executive Branch agencies. In the future, this program may extend to other State of Hawai`i branches ensuring consistency of privacy protections across the State.

This document relies on the structure and processes detailed in the following OIMT plan documents:

- The State of Hawai`i Information Assurance Plan provides the security plan, phasing, and framework, including security tools and training.
- The State of Hawai`i Policy Plan provides the framework and policies, including structure for classification, protection, transport, and storage of data.

2.3 ASSOCIATED DOCUMENTS

- State of Hawai`i Business Transformation Strategy and IT/IRM Strategic Plan, 2012 (referred to as the Plan)
- Baseline of Information Management and Technology and Comprehensive View of State Services (referred to as the Final Report) prepared for the State by SAIC
- Federal Segment Architecture Methodology (FSAM)

2.4 THE THREAT

There has been growing public concern over identity theft and fraud, and employers are a tempting target for criminals seeking precisely the kinds of data needed to open, access, or change a financial account—such as information combining a name with the associated SSN, driver's license or passport number, current employer, home address, home telephone number, and date of birth.

In 2005, at least 14 large U.S. employers reported security breaches of PII data concerning thousands of current and former employees and dependents. The incidents involved Bank of America, Science Applications International Corporation (SAIC), Adecco Employment Services, Time

Warner, MCI, Purdue University, the U.S. Justice Department, the U.S. Air Force, Motorola, the Federal Deposit Insurance Corporation (FDIC), Eastman Kodak, San Diego County, Boeing, and Ford Motor Company. In early 2006, Ameriprise Financial and Honeywell reported similar security breaches involving employee data. In February 2006, computer security firm McAfee notified employees that a Deloitte & Touche auditor had left an unencrypted compact disc containing their names and social security numbers on an airplane. In March 2006, Fidelity Investments lost data on nearly 200,000 Hewlett-Packard employees on a stolen laptop computer containing retirement fund details. These last two incidents illustrate how a reputable third-party service provider may jeopardize the security of personal data held by an employer.

Notably, most of these data losses were not targeted hacks but simply lost tapes and stolen laptops, which in most cases did not demonstrably lead to instances of identity theft. Nevertheless, the incidents were made public, and in most cases, the affected employees were given free

credit-monitoring services for one to three years and other forms of assistance (such as letters to their financial institutions) to minimize their exposure to theft.

The landscape of the losses continues to change and has shifted away from simple loss of physical media or laptops common ten years ago to more recently the remote hacking of systems. Starting with the 2005 IBM Security Index Reports, there have been strengthening statements that cybercrime will continue to shift away from complex hacking and mass disruption through malware to smaller, more targeted attacks on organizations as a prelude to extortion demands. The reports warn that criminals will increasingly take aim at the most vulnerable point of access to an organization: its own personnel—authorized users who may be tricked or, less frequently, bribed. They state that in some cases, thieves have taken jobs in a target organization for the purpose of gaining access to valuable data. IBM concludes that computer users must be educated to recognize that they may be targeted either as intended victims or as a means of gaining access to their employer's systems and data. Successful efforts to assume the identity of an employee may be designed for fraud or extortion of the employer. This is another instance in which personal privacy and organizational security are corresponding interests—a point that should be emphasized throughout the organization.

2.5 PROGRAM MISSION

The OIMT Privacy Program's mission is to ensure the protection of the privacy information the State holds about individuals, to oversee privacy compliance by the Executive Branch, and to fulfill all State and Federal legal requirements associated with privacy matters.

This protection must occur in conjunction with the government's legitimate need to collect appropriate information about individuals in order to carry out its diverse missions.

As the government strives to increase transparency, improve communications both across government and with the public, and enhance efficiency through the use of new technologies, balancing these imperatives with vigilant privacy protection becomes increasingly difficult. Paired with the explosion of new technologies that support instantaneous communications between people and across continents, the potential for privacy breaches has also increased exponentially.

The State needs to develop and adopt a comprehensive strategy to limit the government's collection, use, and dissemination of personal information, and privacy protection is now more challenging than ever:

- There is increased computerization of records permitting new levels of analysis.
- There is a dramatic increase in the sheer volume of privacy information and in the number of systems containing such information maintained by agencies, including privacy data arising from other agencies as the vision of shared services in the State is realized.
- There are increased opportunities for breaches to occur in both electronic and paper records
- There are increased compliance and reporting requirements from oversight agencies.

We are governed by numerous laws, regulations, and policies that we must comply with in order to fulfill both our privacy protection responsibility and our privacy reporting and related requirements.

2.6 PROGRAM VISION

The OIMT must proactively implement policy that will provide a statewide standard to ensure uniformity in technology standards, process, methods, and system. The OIMT must ensure that these policies are implemented to include recommendations and requirements associated with FISMA, the National Institute of Standards and Technology (NIST), the Federal Bureau of Investigation (FBI), the Criminal Justice Information Services (CJIS) Security Policy, Health Insurance Portability and Accountability Act (HIPAA), PCI Data Security Standard (PCI DSS), Americans with Disabilities Act (ADA), Internal Revenue Service Publication 1075, and other standards, agency audit requirements, guidelines, and best practices to comply with numerous laws and reporting requirements concerning policy. The Privacy Policy vision is a lofty one that will take concentrated effort and cooperation across the State for many years. Substantial parts of the vision will require not only funding, but also dedicated staff and ongoing training for employees. By putting solid and consistent privacy policies in place, we will build trust in government by the public in being good and secure stewards of their information, make it easier for staff to understand and meet expatiations, and develop standardized procedures streamlining processes.

2.7 PROGRAM GOALS

The OIMT Privacy Program's goal is to achieve excellence in privacy compliance and protection while reducing the risks to the public, OIMT, and State employees regarding privacy information. A cycle of continuous assessment and improvement will be put in place to not only ensure that we design and build systems and processes with privacy in mind, but also to ensure staff awareness of privacy requirements and put in place automated monitoring to assist them in meeting privacy goals. These risks include civil and criminal penalties: employees can be individually sued or prosecuted, and the department also has civil liability vulnerability. These risks involve general compliance issues with wide-ranging and very serious ramifications. We must work to ensure public trust, to ensure the minimization of negative media exposure, and to guarantee compliance with State and Federal requirements in order to prevent funding issues, additional scrutiny, and loss of State or public confidence.

Privacy Assessment and Compliance: Periodic privacy impact assessments are a vital tool for establishing and maintaining privacy compliance. A privacy impact assessment should be part of the System Life Cycle Development (SLDC) Plan triggered when new personal or PII information is implicated.

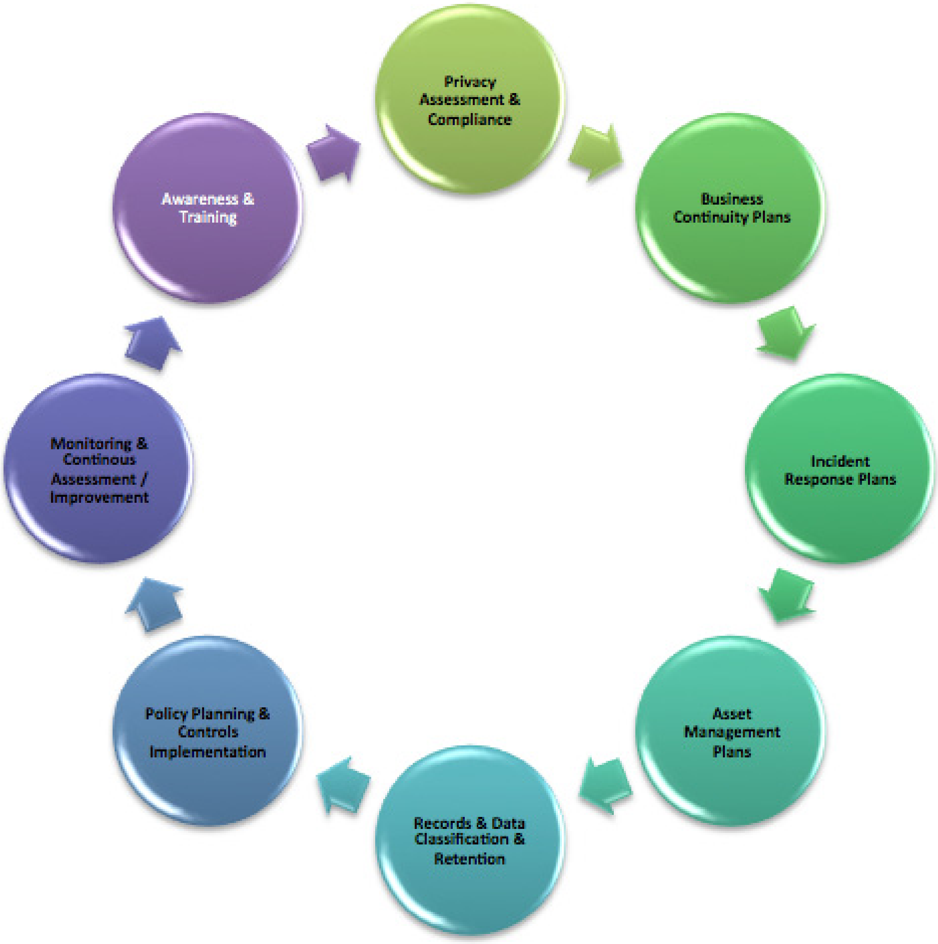

Privacy Assessment & Compliance
Business Continuity Plans
Incident Response Plans
Asset Management Plans
Records & Data Classification & Retention
Policy Planning & Controls Implementation
Monitoring & Continous Assessment / Improvement
Awareness & Training

Figure 1: Privacy Assessment Cycle

A privacy impact assessment provides information about how well policies are understood and followed and identifies areas where policy should be updated to reflect changes in law, regulation, best practices, or organizational business objectives. Periodic assessments demonstrate a strong commitment to a privacy culture and are excellent evidence of compliance efforts. Assessments take into account three perspectives:

- Risks—what are the exposures and what can be done to minimize the effects?
- Readiness—what privacy controls are in place and how effective are they in preventing or detecting privacy breaches?
- Compliance—how well privacy obligations are met and is existing documentation sufficient?

Business Continuity Plan: Identifies exposure to internal and external threats and integrates hard and soft assets to provide effective prevention and recovery for an agency. This document will not go in depth on this subject in that it is covered as a primary subject in other parts of the Plan.

Incident Response Plan: An organized approach to addressing and managing the aftermath of a security breach or attack. The goal is to handle the situation in a way that limits damage, prevents additional exposure of data, and reduces recovery time and costs. An incident response plan includes a policy that defines, in specific terms, what constitutes an incident and provides a step-by-step process that should be followed when an incident occurs. Because it is covered as a primary subject in other parts of the Plan, this document will not go in depth on the subject (specifically, it is in the sections on policy and Information Assurance [IA]).

Asset Management Plan: The International Infrastructure Management Manual (2011 edition) defines an Asset Management Plan as "a plan developed for the management of one or more infrastructure assets that combines multi-disciplinary management techniques (including technical and financial) over the life cycle of the asset in the most cost effective manner to provide a specific level of service." As part of this plan, methods to protect data must be tightly integrated. As new systems are put in place, only obfuscated or highly redacted data should be utilized. For systems that are coming out of production, procedures must be put in place to protect and promptly remove any latent data. Because it is covered as a primary subject in other parts of the Plan, this document does not go in depth on this subject.

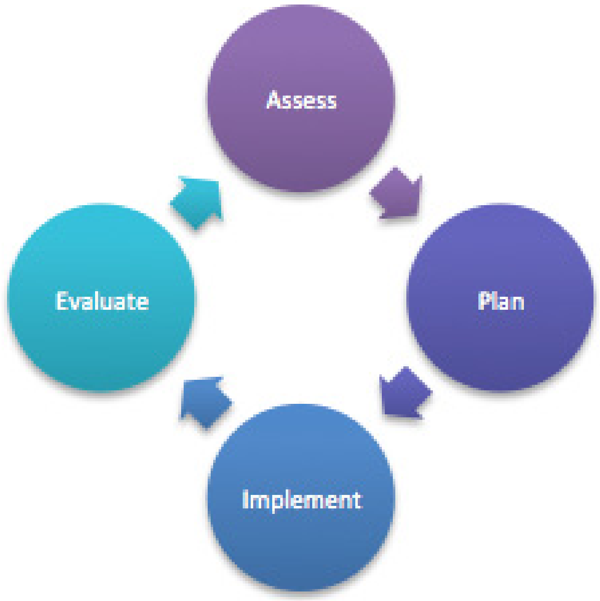


Figure 2: Kaizen Continuous Improvement

Records and Data Classification and Retention: There must be a documented plan put in place for each system and data element defining the need to collect, process, store, and dispose of PII data. Similar to tracking the physical assets you have, you must also keep vigilant track of the data elements you are also entrusted with. Data in a system should also be properly classified. Data classification needs to be coupled as a part of the Information Lifecycle Management (ILM) process—defined as tool for categorization of data to enable agencies to effectively answer following questions:

- What data types are available?
- Where are certain data located?
- What access levels are implemented?
- What protection level is implemented and does it adhere to compliance regulations?

When implemented, it provides a conduit between IT specialists and process or application owners. IT staff is informed about the data value by application owners who better understand the relationships of the data and if it needs to be more securely protected.

Policy Planning and Controls Implementation: Policies are put in place to not only regulate the administration of systems, but how data is handled, what types of logs are required, separation of duties, and many other controls. This is done not only to ensure that a system performs the functions it was built for, but that the data that it depends on is handled and with appropriate care and security.

Monitoring and Continuous Assessment/Improvement: Once privacy controls and policies are put in place, they need to be cared for and adjusted.

First you would need to assess how well things are doing. When the assessment is completed, you would need to plan the changes to be made to ensure the intended outcome. Implementation of the planned changes then takes place, followed by an evaluation of how well those changes faired. This process, illustrated in Figure 2, is commonly known as Kaizen, which can be roughly translated from Japanese to mean "good change." The philosophy behind kaizen is often credited to Dr. W. Edward Deming, resulting in the process sometimes referred to as a Deming Circle. This process may take place in the Privacy Assessment Cycle, shown in Figure 1, to improve the each step in the cycle.

Awareness and Training: If staff is not aware of and do not understand privacy concerns and the elements of data they work with that comprise PII, you cannot expect them to be vigilant in carrying out their duties as intended. Reliance on the coconut wireless is even worse in that as the message moves along, slight changes are made, and if not promptly corrected, result in becoming incorrect institutional knowledge. When privacy best practices, guidelines, or policies are issued, a comprehensive communications and training plan must be at the ready to ensure a successful outcome.

2.8 FAIR INFORMATION PRACTICES

There are many new laws in the U.S. that affect data security obligations, particularly for securing and protecting the kinds of data that potentially place employees and the public at risk of identity theft or fraud (such as SSNs, driver's licenses, and bank account and credit card information) or that touch on the medical and financial aspects of their private lives. This legislation is partly driven by publicity of the growth and cost of identity theft and several substantial security breaches involving employee data. In addition, U.S. state and federal legislators (and occasionally the courts) are increasingly focusing on the privacy of medical and financial information and certain common employer practices that impact privacy interests, such as criminal background and credit checks, alcohol and drug testing, genetic profiling, and employee monitoring and surveillance.

Despite differences in terminology and detail, the typical definition of personal information or personal data is set broadly as any information that is identifiable with a person, and within Hawai`i it is in the Hawai`i Revised Statutes §487(N), HRS §487(R). There are a few collective principles of fair information practices which could be summarized as follows:

- **Purpose and collection limitation:** Personal information should be gathered by fair and lawful means, preferably with the awareness of the individual, and it should be used and disclosed only for legitimate, specified purposes.

- **Data quality and retention:** The personal information collected should be relevant, complete, and not excessive for the intended purpose. The information should come from reliable sources. The information should be kept as accurate and up-to-date as needed for the intended purposes, and it should be retained no longer than needed for those purposes.

- **Notice and awareness:** Individuals normally have a right to know when personal information about them is being collected, saved, used, or revealed to others. They should be told what kind of information is collected, who has access to it, how it will be used, how it will be protected, and the options they have regarding its collection and use.

- **Choice and consent:** Individuals should be given choices, whenever feasible, about the personal information collected and how it is used. For example, legal and business requirements specify the information that must be collected, stored, and disclosed to banks or intermediaries when persons order a service and pay for it by credit card, but additional use of some of those personal details (e.g., to create a marketing mailing list) should be subject to an opt-in or opt-out choice.

- **Security:** Personal information should be protected at all times by appropriate technical and organizational security safeguards to avert loss, misuse, destruction, modification, or unauthorized access or release.

- **Accountability, enforcement, and recourse:** Agencies that handle personal information should appoint staff to be responsible to develop privacy and security policies, train relevant staff and contractors, and take proper steps to ensure that privacy and security policies are effective and enforced. Agencies should provide contact points for questions.

As a result of these trends and needs, system architects and owners are faced with the task of reconciling privacy requirements with systems and applications that were designed for organizational efficiency and security. Privacy policies usually result in new or modified system requirements, such as:

- Displaying privacy notices and options online and in printed forms and reports

- Recording and implementing individual opt-in or opt-out choices

- Creating and enforcing fine-grained internal access controls and authentication procedures designed to protect privacy

- Using spiders or other software to find all the instances in which the organization collects personal data online or stores personal data on its systems

- Scrambling or abstracting personal data in certain applications and reports. This could be done in such a manner to suppress the display of all but the last four digits of identifier. Note that due to privacy concerns in Hawai`i, it is not recommended to use the last four digits of an SSN on documents or reports.

- Logging or tracking the use of personal information and its disclosure to third parties

- Monitoring the interfaces with outsourced service providers that handle personal information from the organization, and establishing the capability to assess their compliance with privacy and security requirements

- Applying legal or contractual restrictions on personal information transmitted from other organizations or jurisdictions (such as credit reports and background checks, health insurance enrollment and claims records, and HR data transmitted from Europe subject to Safe Harbor Privacy Principles or model data-protection contracts)

- Establishing mechanisms to identify personal information compromised in security breaches and to comply with security breach notice requirements

- Ensuring compliance with applicable data retention and data destruction requirements for sensitive personal data

As is true for information security in general, privacy solutions tend to be lower in cost and more effective when they are designed into a system from its inception rather than bolted on later. For example, encrypting or redacting SSNs or replacing them with a randomly assigned identifier in an existing application or report is notoriously costly and time-consuming if the application was not designed with this prospect in mind. Self-service access to personal data, with automated means of making or requesting options and alterations, is much more efficient over the long term than responding manually to every such request. The ability to tag data originating from a particular party or jurisdiction may be a critical feature for compliance with a law or contract that is very difficult to add to an established database.

Ideally, system designers should identify privacy requirements as early as possible in the development or procurement cycle, as well as when revising existing systems. Architects may have to prompt the agencies to help delineate requirements when new or modified systems are envisioned. To do this, it helps to have a basic understanding of trends in privacy norms and regulations and the kinds of functionality that may be required to comply with the State's current and near-future privacy requirements.

There are many more data flows than ever before between the State and third parties (often crossing jurisdictional borders), and many of these include personal information. The reality is that information is rarely an in-house affair in its entirety. Outsiders such as business partners, vendors, auditors, insurance underwriting, and claims personnel, and a variety of technical and management consultants have at least limited or intermittent access to some of the State's data. As a result, we must manage the operational, security, and liability risks that follow from multiple data flows and distributed access to personal information collected and used by the State. Ultimately, this complicates the job of the architects and owners of enterprise systems.

2.9 HEALTH DATA

In 2001, the Federal Department of Health and Human Services (HHS) finalized medical information privacy and security regulations required by the Health Insurance Portability and Accountability Act of 1996 (HIPAA), 42 USC §1301 et seq. The HIPAA Privacy Rule, 45 CFR Parts 160 and 164, took effect in 2003 (it is available, along with related materials, on the HHS HIPAA website). A separate HIPAA Security Rule was later adopted, and it specifies much more detailed security standards effective in 2005 or 2006, depending on the size of the health plans involved.

Due to the complexity and expertise required in the proper execution and compliance of required HIPAA privacy elements, the development of privacy policy for HIPAA data elements within the State are intended to remain the primary responsibility of the privacy SMEs in the agencies that collect and/or process HIPAA data. The privacy team proposed by the OIMT will act as a privacy consultant to these agencies as well as a gathering point across the State agencies to share best practices, ensure consistency with the overall plan, and publish the collective final policy.

2.10 CRIMINAL JUSTICE DATA

Due to the complexity and expertise required in the proper execution and compliance of required Criminal Justice Information Services (CJIS) privacy elements, the development of privacy policy for CJIS data elements within the State are intended to remain the primary responsibility of the privacy SMEs in the agencies that collect and/or process CJIS data. The privacy team proposed by the OIMT will act as a privacy consultant to these agencies as well as a gathering point across the State agencies to share best practices, ensure consistency with the overall plan, and publish the collective final policy.

2.11 PROTECTION OF DATA BELONGING TO MINORS

The proper protection for data associated with minors (persons under the age of 18) is very nuanced and best left under the direct input from those who interact and manage the data on a daily basis. The *Privacy Plan* will place the primary responsibility for the development of specialized privacy protections for these data elements with the privacy SMEs in the agencies that collect and/or process this type of data. The privacy team proposed by the OIMT will act as a privacy consultant to these agencies as well as a gathering point across the State agencies to share best practices, ensure consistency with the overall plan, and publish the collective final policy.

2.12 PRIVACY TRAINING AND AWARENESS

Privacy training and awareness programs are key elements of building a culture of privacy. Training programs reinforce the implementation of a privacy policy and reduce the risk of privacy incidents throughout the State. Training and awareness are critical elements of an effective privacy program. One project goal is to put in place the requirement that all employees and contractors receive mandatory annual privacy training. Successful completion must be documented (and on file) at least once per year.

A best practice is that all personnel must successfully complete privacy training before permitted access to State information and information systems. Additional or advanced training should also be provided commensurate with increased responsibilities or change in duties. Another best practice is to require those personnel who cause or commit a PII breach to take PII refresher training with documented completion for every reportable breach. Both the annual and PII refresher training should include acceptable rules of behavior and the consequences when the rules are not followed. For areas that have authorized telework and other remote access programs, training should also include the rules of those programs.

2.13 PRIVACY RISK MANAGEMENT AND COMPLIANCE DOCUMENTATION

The Federal government Privacy Impact Assessment (PIA) and System of Records Notice (SORN) are the primary tools to identify holdings of PII, assess privacy risks, and implement privacy protections in their systems and programs. Currently in the State, the Information Privacy and Security Council collects yearly information about PII systems. This manual process is envisioned to be transformed into an automated system and aligned following best practices of the proven Federal system. Requirements for a PIA for all IT systems, whether or not they collect PII, would be established as well as a blanket or adapted PIA for third-party social media. This would not only assist staff awareness of the need for additional protection of systems, but would also streamline systems administration processes and raise overall staff awareness of privacy requirements and concerns.

The Privacy Act requires Federal agencies to issue SORNs for every system of record under their control that collects PII and from which a person's records are retrieved by a unique identifier. A SORN is a legal document used by the Federal government to promote transparency and provide notice to the public regarding their rights and procedures for accessing and correcting PII maintained by the agency. This process can also be adopted for State use as part of the Privacy program.

Another Federal PII tool is the Privacy Act Statement (PAS). A PAS is required on all Federal official forms (paper and electronic) that an organization uses to collect PII from members of the public or Federal employees. These statements inform individuals at the time their information is collected what the legal authority for and purpose of the collection is, and how the organization will use the information. Privacy Act Statements also notify individuals whether providing the information requested is mandatory or voluntary and the consequences of failing to provide the information. Implementation of a similar program in the State can help to instill confidence and provide transparency to the public in the data that we collect.

3. MAJOR SCHEDULED EVENTS (MILESTONES AND REOCCURRING)

3. MAJOR SCHEDULED EVENTS (MILESTONES AND REOCCURRING)

The Privacy FTE and resources will be utilized to provide coordination, oversight, and comprehensive privacy program direction for privacy matters across the Executive Branch. This will support OIMT mission goals by increasing accountability, and enhancing functional integration; the results orientation to be utilized will also permit increased alignment between OIMT privacy across the Executive Branch with OIMT enterprise initiatives. We will utilize this FTE to assist in the updating of procedures and training. The FTE will conduct improved oversight of the new procedures and training, which will decrease the State's risk. It will provide support to all the Executive Branch agencies for successfully complying with the various FISMA reviews. Efforts can be undertaken to promote greater privacy and security awareness throughout the State. Providing the required FTE and resources as well as implementing recommendations in the Security and Privacy programs can be expected to reduce not only the number, but also the severity of the privacy breaches.

3.1 PRIVACY PROGRAM MILESTONES (NON-STAFFING)

Table 1: Milestones (Non-staffing)

Milestones	Person or Team Responsible	Planned Completion Date
OIMT Directive on Administration Policy	Privacy Officer, Information Management Chief, OIMT	
FY15 Annual Privacy Report (recurring)	Privacy Officer	FY-2015 (need FTE on board)
Annual Review of Privacy websites for compliance	Privacy Officer	Continuing; Annually (need FTE on board)
Agency/Office Quarterly/Annual PII Assurance Report	Agency and Departmental Privacy Officers, OIMT	
Complete and deploy computer-based training (CBT) for all OIMT employees, contractors, etc.	Privacy Officer	FY-2015 (need FTE on board)
Develop and deploy at least nine role-based training modules (CBT)	Privacy Officer, Contractors	FY-2015 (need FTE on board)
Employee awareness and outreach to agencies/offices	Privacy Officer	FY-2015 (need FTE on board)
Monitoring/oversight of agency/office Privacy implementation	Departmental Privacy Officers	FY-2015 (need FTE on board)
Certification and Accreditation for Privacy Officers and specialists	Agency/Departmental Privacy Officers	FY-2015 (need funding)
Update OIMT Privacy regulations/Privacy Manual sections	Privacy Officer	FY-2015 (need FTE on board)
Full training program for all staff	Privacy Officer	FY-2015 (need FTE on board)

3.2 PRIVACY PROGRAM MILESTONES (STAFFING)

Table 2: Milestones (Staffing)

Milestones	Person or Team Responsible	Planned Completion Date
Meet with Human Resources	Privacy Office, Information Management Chief, OIMT Business Manager	
Write PDs	Privacy Officer	
Classify PD	OIMT HR	
Advertise vacancies (open continuously)	OIMT HR, OIMT Business Manager, DHRD	
Pull first set of applicants (SR 22-26)	DHRD, OIMT HR	
Set up interviews	CIO Business Manager, Privacy Officer	
Finalize interviews; give cert and recommendations to CIO for approval	Privacy Officer	
Pull second set of applicants	OIMT HR	
Approval from CIO	Information Management Division Chief, Dept CIO, CIO	
Provide cert to OIMT HR for processing	OIMT Business Manager	
Set up Interviews for second set of applicants	OIMT Business Manager, Privacy Officer	
Make first offer	OIMT HR	
Finalize interviews (second Group); give cert and recommendations to CIO for approval	Privacy Officer	
Pull third set of applicants (if needed to fill two FY-2014 vacancies)	OIMT HR	
Hire first applicant (on-board)	OIMT HR	
Make second offer	OIMT HR	
Set up interviews for third set of applicants	OIMT Business Manager, Privacy Officer	
Finalize interviews (third group); give cert and recommendations to CIO for approval	Privacy Officer	
Make third offer	OIMT HR	
Hire second applicant (on-board)	OIMT HR	
Using hiring sequence/procedures/milestones above, additional hiring in FY-2015 to cover shortfalls in hiring in FY-2014, up to two positions	OIMT Business Manager, Privacy Officer, CIO, Information Management Div. Chief, OIMT HR	
Using hiring sequence/procedures/milestones above, additional hiring in FY-2015 = one additional position	OIMT Business Manager, Privacy Officer, Deputy CIO, Information Management Div. Chief, OIMT HR	
Using hiring sequence/procedures/milestones above, additional hiring in FY-2016 = one additional position	OIMT Business Manager, Privacy Officer, Deputy CIO, Information Management Div. Chief, OIMT HR	

4. COSTS

4. COSTS

4.1 IDENTIFY PROGRAM COSTS (INCLUDING COSTS APPROVED BY THE OIMT)

Table 3: Estimated Program Costs

Description	Estimated FY-2014 Costs (in Thousands $)	Basis of Estimates (Formulation Method and Source)
Meet with Human Resources	Pending Review	Based on existing union contract wages
Contractor support for development of up to nine Privacy role-based training modules[1]	Pending Review	Based on estimate for CBT development
Total	Pending Review	

In addition to the program costs summarized above, the annual operational costs in Table 4 below are expected for each subsequent fiscal year starting in FY-2014, with an increase of one FTE SR-22/24 in FY-2015 and an additional one in FY-2016, which brings the total Privacy staff to three FTEs SR-22/26. These annual costs will be used as the basis for Total Cost of Ownership.

Table 4: Annual FY-2014 Operating Costs

Description	Estimated Annual Budget (Starting in FY-2014 – 4 % Increase for Each Out Year) (in Thousands $)	Basis of Estimates (Formulation Method and Source)
Ongoing FTE expenses for two Privacy Specialists	Pending Review	Estimate of salaries
Travel:		
Travel to Agency locations for Privacy Compliance and Training	Pending Review	Based on contractual expenses for no less than four trips/annually (includes transporting supporting documentation)
Other Services:		Based on estimates from the International Association of Privacy Professionals, OPM security clearance estimates, and professional insurance
IAPP membership	Pending Review	
IAPP cert exams	Pending Review	
IAPP cert courses	Pending Review	
Bookmarks, monuments	Pending Review	
Training for Privacy staff	Pending Review	

[1] *Cost assumes that a statewide CBT system is procured as noted in "The Plan" that these modules can be installed in.*

Description	Estimated Annual Budget (Starting in FY-2014 – 4 % Increase for Each Out Year) (in Thousands $)	Basis of Estimates (Formulation Method and Source)
Update/new security clearances	Pending Review	
Professional insurance	Pending Review	
Equipment:		
Scanners, printers, laptops, docking stations, monitors, etc.	Pending Review	Based on estimates provided by previous procurement and contracts
Communications:		
BlackBerries, teleconference lines, etc.	Pending Review	
Print pamphlets, supplies, and minor contracts for updating CBTs	Pending Review	Based on estimates from OIMT, current supply expenditures, and privacy pamphlets
Total	**Pending Review**	

Table 5: Estimated Additional Funding Requirement (FY-2015)

Description	Estimated Annual Budget (FY-2015 and FY-2016) (in Thousands $)	Basis of Estimates (Formulation Method and Source)
Develop performance metrics, analytics, investigation, and compliance tools	Pending Review	Based on contractor support estimates
Personnel Costs:		
Ongoing FTE expenses for one additional Privacy Specialists	Pending Review	Estimate of salaries
Travel to agency locations for Privacy Compliance and Training	Pending Review	Based on contractual expenses for no less than 4 trips/annually. (Includes transporting supporting documentation)
Other Services:		Based on estimates from the International Association of Privacy Professionals, OPM security clearance estimates, and professional insurance
IAPP membership	Pending Review	
IAPP cert exams	Pending Review	
IAPP cert courses	Pending Review	
Training for Privacy staff	Pending Review	
Update/new security clearances	Pending Review	
Professional insurance	Pending Review	
Contractor assistance	Pending Review	

Description	Estimated Annual Budget (FY-2015 and FY-2016) (in Thousands $)	Basis of Estimates (Formulation Method and Source)
Equipment:		
Scanners, printers, laptops, docking stations, monitors, etc.	Pending Review	Based on estimates provided by previous procurement and contracts
Communications:		
BlackBerries, teleconference lines, etc	Pending Review	
Total	**Pending Review**	

4.2 CRITICAL SUCCESS FACTORS

Critical Success Factors (CSFs) increase the probability of success when management focuses attention in these areas. This program's CSFs are:

- Timely commitment of funds and processing of required acquisitions
- Availability of appropriately skilled staff and contractors to complete program tasks and deliverables
- Participation and commitment of program team to complete their tasks and deliverables on schedule

4.3 PROGRAM STAFF DELIVERABLES

With a complement of two Privacy Specialists identified to be hired FY-2014, the OIMT Privacy Office will accomplish the following in FY-2015:

- Enhance agency oversight for FISMA (quarterly and annual) review and reports.
- Improve coordination with Cyber Security with the provision of coordination between the agencies in support of responding to PII Breaches.
- Provide greater oversight and guidance on handling Privacy information contained in systems being decommissioned, transferred or migrated.
- Review agency/office system notices for accuracy and validity. Correct notices where needed and provide guidance to agencies/offices.
- Provide oversight and reviews of the information classification documentation, ensuring Agency Privacy Officers utilize the correct data from these databases in their work with systems documentation, privacy reporting, and other privacy concerns.
- Review of System Privacy Impact Assessments (PIAs) as currently collected by the IPSC for Privacy requirements.
- Review of web pages for Privacy compliance through reports provided by the Access Hawaii Committee.
- Update the OIMT Privacy manuals and handbooks and write new policies, procedures, and templates where needed.
- Provide assistance to the Information Privacy and Security Council.
- Build the plan for incorporating SORN, PIA, and PAS within the State

With the hiring of one additional Privacy Specialist per year until the OIMT reaches the recommended three specialists, one Privacy Officer, and the purchase of automated PII assurance solutions, the Departmental Privacy Office will be able to accomplish:

- Enhanced agency oversight for FISMA (quarterly and annual) review and reports
- Better coordination with Cyber Security with the provision of coordination between the Department's and agency's Identity Theft Task Forces in support of responding to PII breaches
- Provide greater oversight and guidance on handling Privacy information contained in systems being decommissioned, transferred or migrated
- Develop and update Orientation to the Privacy CBT (mandatory for all employees, contractors, and volunteers)
- Review agency/office system notices for accuracy and validity. Correct notices where needed and provide guidance to agencies/offices.
- Provide oversight and reviews ensuring Agency Privacy Officers utilize best practices and standards in their work with systems documentation, privacy reporting, and other privacy concerns
- Review of System PIAs for Privacy requirements
- Review of web pages for Privacy compliance through reports provided by the Access Hawaii Committee

- Updating of the OIMT Privacy manuals and handbooks and writing new procedures and templates where needed
- Conduct Privacy technical evaluation and compliance reviews for the OS, agencies, and offices
- Develop role-based Privacy training
- Develop and conduct Privacy workshops and Privacy awareness campaigns
- Creation of a centralized risk assessment and PIA file collection across the Executive Branch
- Enterprise-wide examination of offices, in coordination with agencies, for PII coverage
- Enterprise-wide examination of offices, in coordination with Agencies, for PII Reviews
- Enterprise-wide examination of offices, in coordination with Agencies, for best practices in privacy protection in paper and electronic records
- Vigilantly keeping current with new privacy legislation and guidance, and promptly disseminating it and incorporating it into agency practices
- Increasing and stronger liaisons with external agencies, commissions, and working groups regarding government-wide privacy policies, initiatives, and matters
- Adoption of a very proactive stance regarding privacy guidance and implementation throughout the State to promote best practices and minimize risk while coordinating with other key programs
- Availability for providing ongoing privacy subject matter expertise for the highest offices within the State, as well as increased ongoing support for agencies including their Privacy Officers
- Provide assistance to the Information Privacy and Security Council

4.4 ASSUMPTIONS

Success is predicated on hiring requested staff, contractor support, fulfilling financial resources (e.g., procuring tools), implementing policies, authorities, and processes as requested.

4.5 TECHNICAL CONSTRAINTS

The Privacy Program will need new and more sophisticated tools to more effectively track, monitor, and analyze the outputs and performance of the program. It will be necessary to have these to better determine and analyze quantitative and qualitative measures for the effectiveness and overall performance of privacy compliance and quality at the department. To have this evaluative capability, there will need to be new metrics, analytics, and measures for privacy compliance and for privacy violations, as well as tools to assist in investigation of privacy performance. The data will provide value in measuring levels of compliance, quality assurance across the department, areas needing correction and enforcement, and provide for improved program management.

5. RISKS

5. RISKS

This section summarizes major program risks discovered at the start of the program. This program's risks will be monitored and reported as part of the Privacy Program Risk Register.

Table 6: Risks

ID	Description	Probability 1 = low 5 = high	Impact 1 = low 5 = high	Mitigation Plan
1	Personnel overcommitted due to other tasks, existing duties, illness, vacations, etc. may delay program	5	5	Ensure Agency/Office Privacy Officers have backups
2	Contracting delays for procurements may delay program or increase costs	4	4	Extend Program schedule, as necessary; keep CIO and OIMT Business Manager informed of anticipated cost issues
3	Failing to comply with State laws and the voluminous FISMA review and reporting requirements would be devastating to the Department.	5	5	Ensure Senior Managers are aware of potential fallout from non-compliance; and recommend personal liability insurance be required for all Privacy Officers
4	Failure to publish a PIA prior to collection of information covered by the Privacy Act	5	5	Use annual PII reviews to warn delinquent Agencies/offices about potential costs; ensure employee awareness of requirements
5	Failure to draft a PIA for a system included in an agency's IT investment portfolio can subject the agency to non-approval by OIMT of its investment.	5	5	Ensure PIAs are conducted as regular part of annual review process
6	Failure to protect PII or SSNs could result in identify theft, Legislature inquiry, bad media coverage, loss of public confidence in the State government, financial loss to the individual and the State government, and may result in official Departmental reprimands or termination and may have budget consequences for the affected program.	5	5	Acquire software to capture unencrypted PII to prevent breaches; conduct annual survey/review for use of PII in conducting business to minimize use/risk
7	Remediating a major breach, for example, the loss of a laptop with unencrypted SSNs or PII of numerous citizens, could cost the State millions of dollars and thousands of work hours	5	5	Get PLMS approved and ensure agencies commit to it; consider methods for determining where money to pay costs will come from, and control use of laptops

6. STAFFING PLAN

6. STAFFING PLAN

6.1 FY 2014-15 TEAM STRUCTURE (NOTIONAL)

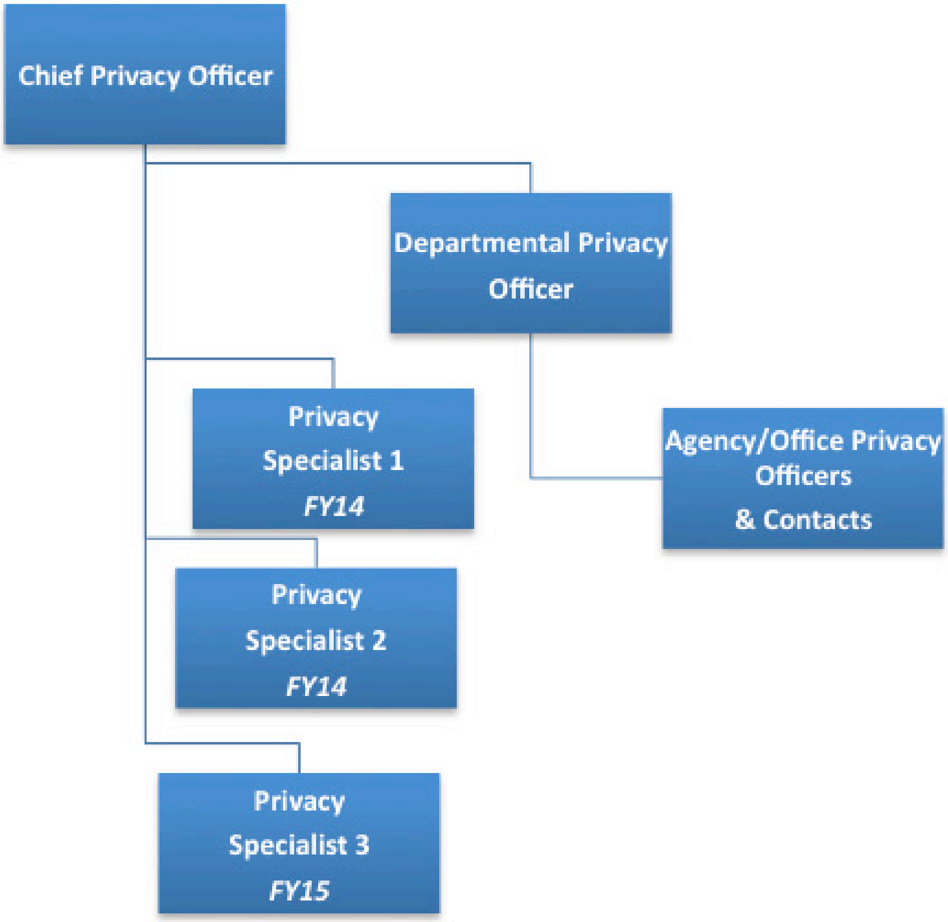

Chief Privacy Officer
Departmental Privacy Officer
Privacy Specialist 1 FY14
Agency/Office Privacy Officers & Contacts
Privacy Specialist 2 FY14
Privacy Specialist 3 FY15

Figure 3: Privacy Program Team Organization Fiscal Year 2014-15

7. RESOURCE REQUIREMENTS

7. RESOURCE REQUIREMENTS

7.1 ROLES AND RESPONSIBILITIES

Table 7: Roles and Responsibilities

Role	Responsibilities
Sponsor(s): Senior Agency Official for Privacy/Chief Information Office Assistant Secretaries, Agency/Office heads, and Budget Officers	• Commit to the scope of this Plan • Authorize program funding/resources required to successfully meet objectives of this Plan, including full compliance with State privacy laws and policies • Be accountable for the success/failure of agency/office compliance • Participate in Identity Theft Task Force meetings, as appropriate • Ensure acquisitions comply with State privacy requirements • Facilitate resolution of OIMT and OIMT Privacy Office PII breaches and other issues outside of the program • Actively participate in progress reviews to ensure critical program information is communicated to Agency/office organizations • Facilitate resolution of program issues in agency/office organizations
OIMT Privacy Officer–Program Manager/Team Leader	• Manage the day-to-day work of the program • Provide program oversight and monitoring of agency privacy programs for compliance • Define and manage program risks • Lead, coordinate, and facilitate Program team's planning and execution of tasks and deliverables • Accountable for the success/failure of program/team tasks and deliverables • Ensure appropriately skilled program participants are available when needed • Prepare and present program reports to appropriate levels of management • Facilitate resolution of issues and elevated risks • Manage acquisitions
OIMT Privacy Specialists	• Provide leadership, expert technical assistance and training for agency/office SMEs and Privacy Officers • Attend all scheduled meetings • Assist OIMT Privacy Officer in providing program oversight/monitoring of agency/office privacy programs for compliance • Actively participate in progress reviews to ensure critical program information is communicated to all agency/office organizations • Facilitate resolution of program issues, elevated risks, e.g., PII breach investigations, in agency/office organizations • Be accountable for the success/failure of OIMT program tasks and deliverables

Role	Responsibilities
	• Ensure appropriately skilled program participants are available when needed • Complete assigned tasks and deliverables based on agreed schedule. • Provide status updates including issues and risks • Communicate openly and assertively • Respect opinions of others • Agree to work toward consensus
Agency/Office Privacy Officers–Team Leaders	• Participate in agency/office process to ensure compliance with applicable privacy requirements, e.g., preparation of PIAs, etc. • Anticipate/prepare to mitigate privacy risks within the agency/office • Present program results to senior agency/office management and others • Be accountable for the success/failure of agency/office compliance • Attend all scheduled meetings • Prepare and present agency/office reports to appropriate levels of management • Designate/train back-up personnel • Ensure appropriately skilled program participants are available when needed • Develop/issue agency/office-specific procedures for compliance, as appropriate • Investigate/report on PII breaches within the agency/office • Keep OIMT Privacy Officer informed of status/outcomes of breach investigations • Provide technical assistance/training to agency/office personnel • Ensure all employees are aware of statutory/regulatory/policy responsibilities • Complete assigned tasks and deliverables based on agreed schedule • Act as SME for appropriate organizational function • Be prepared to take some responsibility to educate others • Communicate openly and assertively • Respect opinions of others • Agree to work toward consensus
OIMT Finance and Procurement Staff	• Oversee contracts • Manage task order solicitation • Administer contracts • Administer competitive procurements • Facilitate OIMT Privacy Program Procurement staff processing of acquisitions

Role	Responsibilities
Internal Stakeholders: Program Team Agency/Office Privacy Officers Agency/Office CIOs Sponsors All Other OIMT Employees **External Stakeholders:** The Public Legislature	• Understand legal, regulatory, and policy requirements for handling data as covered in HRS §487(N), HRS §487(R), and federal standards where required • Ensure compliance with privacy laws, regulations, and policies • Report potential and actual breaches to appropriate officials • Take annual privacy training • Provide feedback regarding OIMT implementation of privacy laws, regulations, and policies via audits, reports, Legislature inquiries, correspondence, appeals/litigation, etc. • Legislature amends the law and State policies to improve privacy safeguards and compliance

7.2 PROGRAM STAFFING PLAN

OIMT is investing 4.83 Full-time Equivalents (FTEs) of effort by FY-2014 via employees and contractors to complete this program's tasks and deliverables. The breakdown by organization is as follows:

Table 8: Program Staffing Plan by OIMT Entity

OIMT Entity	FTEs
Privacy Officer	1
Business Manager	0.125
Business Staff	0.25
Privacy Specialist (first/third FTE)	0.33
Privacy Specialist (FY-2014)	3
Program Total	4.83

This table shows an estimated percentage of scheduled work hours needed for the program to be successful.

Table 9: Minimum Program Staffing Plan

Resource Name or Role (if not staffed)	Minimum Needed for this program (%)	OIMT Entity
EM05+	100	Privacy Officer
	0.125	Business Manager
	0.25	Business Staff
SR-24	0.33	Privacy/508/Quality Assurance Specialist
SR-22/24	100	Privacy Specialist
SR-22/24	100	Privacy Specialist
SR-22/24	100	Privacy Specialist

7.3 CONTRACT SERVICES REQUIREMENTS

Table 10: Contractor Requirements

Role	Skills	Experience	Duration
Develop Privacy role-based training modules and no less than six workshops	Planning, developing, and presenting computer-based and classroom training	Governmental Privacy experience, CIPP/G Certification	Greater than one year
Plan, develop compliance standards, conduct compliance audits and training to meet requirements	Planning, developing privacy compliance standards, and conducting compliance audits, evaluations, etc.	Governmental Privacy experience; CIPP/G Certification	Greater than one year

7.4 STAFFING PLAN FOR ONGOING OPERATIONS

In addition to the Staffing Plan for this program, the following the organizational OIMT roles, skills, and experience will be needed to operate and maintain the resulting solution.

Table 11: Operational Support Requirements

Role	Skills	Experience
Two Privacy Specialist (FY-2014) One Privacy Specialist (FY-2015) for all skills identified	Development of policy, procedures, manuals, handbooks, and directives to large organizations on the Privacy Program (e.g., PIAs, PII, SSN Reduction, DEAR, PLMS, Breach, etc.) Provision of oversight to Privacy Program Development/Presentation of Privacy training Privacy Compliance	One year at next lower grade

8. DELIVERABLES

8. DELIVERABLES

8.1 PROGRAM DELIVERABLES

Verification methods include: analysis, inspection, demonstration, and testing.

Table 12: Program Deliverables

Deliverable	Objective	Primary Audience	Reviewers	Approvers
Agency/Office Identity Theft Task Force (ITTF) Charters	Codify roles and responsibilities of task force and task force members	Each Agency/Office	OIMT Privacy Officer/ Privacy Specialists Agency/Office Managers and CISOs	OIMT Privacy Officer
Scorecards; FISMA Annual Report; assist in compliance reviews use of SSNs/PII, DEAR, CSAM, and Privacy websites; and Privacy Impact Assessments	Comply with various laws and State privacy requirements	Public, OIMT Privacy Office	OIMT Privacy Specialists Agency/Office Managers	OIMT Privacy Officer

8.2 PROGRAM MANAGEMENT DELIVERABLES

Verification methods include: analysis, inspection, demonstration, and testing.

Table 13: Program Management Deliverables

Deliverable	Objective	Primary Audience	Reviewers	Approvers
Program Plan	Acquire resources required for full OIMT compliance with privacy laws and State policies	All agencies and offices	OIMT Privacy Officer ICSD Administrator	OIMT PMB Budget Officers
Update OIMT Privacy Manual and Handbook (need requested FTE to complete)	Provide guidance needed to ensure OIMT compliance with privacy laws and related State policies	All agencies and offices	OIMT Privacy Officer ICSD Administrator	OIMT PMB
Privacy Loss Mitigation Strategy (PLMS) (need requested FTE to complete)	Provide guidance to Agencies/ offices needed to ensure appropriate OIMT response/ handling of breaches of PII	All agencies and offices	OIMT Privacy Officer ICSD Administrator	OIMT PMB
OIMT Identity Theft Task Force (ITTF) Charter (need requested FTE to complete)	Codify roles and responsibilities of task force and task force members	All agencies and offices	OIMT Privacy Officer ICSD Administrator	OIMT PMB

Deliverable	Objective	Primary Audience	Reviewers	Approvers
OIMT Privacy Policies and Procedures (in addition to Privacy Manual and Handbook) (need requested FTE to complete)	Enable awareness of scheduled tasks	All agencies and offices	OIMT Privacy Officer ICSD Administrator	OIMT PMB
Role-Based Trainings & Workshops (need requested FTE to complete)	Identify strengths, areas for improvement, and recommendations	All agencies and offices	OIMT Privacy Team	OIMT Privacy Officer
Technical Evaluations (need requested FTE to complete)	Ensure compliance with privacy requirements	All agencies and offices	OIMT Privacy Team	OIMT Privacy Officer

9. PROGRAM CONTROLS

9. PROGRAM CONTROLS

9.1 SCORECARDS (QUARTERLY AND ANNUALLY)

Agency/Office Privacy Officers are responsible for preparing quarterly PIA and annual PIA/PII reports to OIMT. These reports reflect level of agency/office/OIMT compliance with specified requirements.

9.2 FISMA PRIVACY ANNUAL REPORT (ANNUAL)

Agency/Office Privacy Officers are responsible for preparing their portion of the annual reports as set forth in the privacy plan. This report reflects level of agency/office/OIMT compliance with specified requirements.

9.3 ANNUAL REVIEW OF SYSTEM OF RECORDS NOTICES AND AUTOMATIC REQUIREMENT TO WRITE PIA FOR NEW SYSTEMS WITHIN 90 DAYS

The OIMT Privacy Office conducts an annual review of SRNs, in collaboration with the Agency/Office Privacy Officers, to ensure that existing PIAs are current and that all new Privacy Act systems have PIAs and any outdated PIAs must be revised as appropriate.

9.4 REVIEW AND PROCESSING OF PRIVACY IMPACT ASSESSMENTS (PIAS) FOR ALL ELECTRONIC SYSTEMS

As part of the review process, all systems that contain PII must have PIAs written and published. This step ensures that PIAs are incorporated into the system creation process.

9.5 ANNUAL SURVEY/REVIEW FOR REDUCING USE OF SSNS AND OTHER PII IN CONDUCTING OIMT BUSINESS

The OIMT Privacy Office conducts an annual survey and review of OIMT's use of SSNs and PII in conducting business, in collaboration with the agency/office Privacy Officers. This exercise ensures that the use of SSNs and PII in conducting OIMT business is minimal so that the risk of PII loss is as low as possible.

9.6 REVIEW DEPARTMENTAL ENTERPRISE ARCHITECTURE REPOSITORY (DEAR), CYBER SECURITY ASSESSMENT MANAGEMENT (CSAM) AND PRIVACY WEBSITES FOR COMPLIANCE ANNUALLY

These program controls are not currently being implemented due to lack of sufficient program resources. Implementation of controls will begin once staffing levels are reached.

9.7 PERFORM PRIVACY TECHNICAL EVALUATIONS ANNUALLY

These program controls are not currently being implemented due to lack of sufficient program resources. Implementation of controls will begin once staffing levels are reached.

9.8 PRIVACY AND SECURITY

All program documents will be labeled Sensitive But Unclassified - For Official Use Only in the header and footer. All Certification and Accreditation (C&A) tasks and deliverables required before this program's solution can be implemented in production are part of this program.

REFERENCES

REFERENCES

Major State Privacy statutes and authorities are located at:

http://ipsc.hawaii./gov

www.capitol.hawaii.gov/hrscurrent/

OIMT's Privacy website is located at:

http://oimt.hawaii.gov

For OIMT Privacy contacts:

See the listing maintained at http://oimt.hawaii.gov.

The OIMT Privacy Manual is located at:

http://oimt.hawaii.gov/Privacy

GLOSSARY OF ACRONYMS

GLOSSARY OF ACRONYMS

For definitions of terms and acronyms used in this document, see the OIMT Nomenclature Guide.

COMMUNICATIONS AND OUTREACH PLAN

TABLE OF CONTENTS

1.0 INTRODUCTION 3
1.1 Purpose....4
1.2 Scope 4
2.0 COMMUNICATIONS STRATEGY, GOALS, OBJECTIVES, AND PERFORMANCE MEASURES 5
2.1 Strategy 6
2.2 Goals 6
2.3 Objectives 6
3.0 STAKEHOLDERS 7
4.0 ROLES AND RESPONSIBILITIES....9
4.1 Chief Information Officer (CIO) 10
4.2 OIMT Staff....10
4.2.1 Senior Communications Manager 10
4.2.2 Program/Project Managers....10
5.0 KEY ELEMENTS....11
5.1 Consistency and Frequency of Messages 12
5.1.1 The Messages 12
5.2 Balancing Macro and Micro 12
5.3 Branding....12
6.0 COMMUNICATION CHANNELS, METHODS, AND TOOLS 13
6.1 Printed Materials....14
6.1.1 Governor and Legislative Briefings/Reports....14
6.1.2 Opinion-editorial Pieces 14
6.1.3 Earned Media Placements....14
6.2 Personal Interaction....15
6.2.1 Governance Committees....15
6.2.2 Face-to-face Town Hall Meetings and Coffee Hours (Internal Stakeholders)....15
6.2.3 Speaking Engagements (External Stakeholders)....15
6.3 Online Communications....15
6.3.1 OIMT Website and Blog 15
6.3.2 Electronic Newsletters 15

1.0 INTRODUCTION

1.0 INTRODUCTION

1.1 PURPOSE

As the State of Hawai‘i begins to transform its business processes and Information Technology (IT) and Information Resource Management (IRM) infrastructure, systems, services, and policies, it is important to communicate with all stakeholders, both internally and externally. The anticipated organizational change and the activities surrounding this may impact various audiences including State employees, contractors, vendors, and the citizens of Hawai‘i. The purpose of this document is to define the *Communications and Outreach Plan* for the transformation.

1.2 SCOPE

The scope of the communications and outreach plan is to:

- Define the communications strategy for the transformation initiative.
- Outline the messages to be communicated throughout the transformation initiative.
- Identify roles and responsibilities.
- Define communication mechanisms, engagement tools, and feedback options.

2.0 COMMUNICATIONS STRATEGY, GOALS, OBJECTIVES, AND PERFORMANCE MEASURES

2.0 COMMUNICATIONS STRATEGY, GOALS, OBJECTIVES, AND PERFORMANCE MEASURES

2.1 STRATEGY

The principles of this communications strategy are to:

- Build trust among internal and external stakeholders through open discussions throughout the transformation process.
- Provide stakeholders with the relevant information necessary to understand the need for change and how to comply with the new environment.
- Report progress or delays in progress so that stakeholders can continue to contribute to the success of the transformation initiative.

2.2 GOALS

As the Chief Information Officer (CIO) and the Office of Information Management and Technology (OIMT) develop and execute the statewide *Business and IT/IRM Transformation Plan,* the Communications and Outreach Plan aims to meet the following goals:

- Ensure accurate, consistent, and timely communication to appropriate audiences.
- Minimize the number of concerns which may naturally develop within the audiences.
- Engage internal and external stakeholders to participate in the planning and transformation process.
- Build advocacy and support for future funding and anticipated legislation.

2.3 OBJECTIVES

The objectives of this communications plan are to:

- Build credibility with internal and external audiences for the CIO and OIMT by establishing expectations, executing, and reporting on activities and progress.
- Ensure accurate, consistent, and timely communication to appropriate audiences.
- Minimize the number of concerns which may naturally develop within the audiences.
- Provide multiple forums and opportunities for departments' leadership, IT staff, and other internal stakeholders to offer comments and feedback during the planning and execution processes.
- Ensure State employees are kept updated regarding the transformation activities and progress.
- Ensure State employees are aware of activities or issues that may affect them and alleviate concerns as best possible.
- Ensure State employees have multiple venues where they may raise issues and concerns, and have them addressed in a timely manner.
- Ensure that individual citizens and Hawai'i businesses are kept apprised of key transformation activities, successes, and opportunities for engagement.
- Ensure all media outlets have a defined, authoritative source of information regarding the State's IT/IRM.

3.0 STAKEHOLDERS

3.0 STAKEHOLDERS

When developing communications, all stakeholders must be considered. This is due to the fact that communications vary depending on who needs to be reached and what the audience needs to learn or take away from the communication.

The following internal and external stakeholders are important for the transformation initiative and must be taken into consideration for the *Communications and Outreach Plan*:

Internal	External
Executive Leadership	**General Public**
• Governor and Lieutenant Governor • Department Directors and Deputy Directors	• Businesses • Individuals
State Employees	**Media**
• Department-level CIOs and IT Managers • IT staff • Non-IT staff	• Local print, broadcast, and online media outlets • IT trade publications • Government trade publications
Other Government Branches	**Local Business Community**
• State Legislature • Judiciary • Office of Hawaiian Affairs • University of Hawai‘i	• Chambers of Commerce • Business roundtables • IT trade associations • Public/private partnerships
Union Leadership	**Other Government Organizations**
• Hawai‘i Government Employees Association (HGEA) • United Public Workers (UPW	• Federal government • City and county government leadership

4.0 ROLES AND RESPONSIBILITIES

4.0 ROLES AND RESPONSIBILITIES

The following describes the roles and responsibilities for the individuals and organizations involved in the *Communications and Outreach Plan.*

4.1 CHIEF INFORMATION OFFICER (CIO)

Depending on the goal of the specific communication, the role of the CIO will change. The primary roles of the CIO in the communications strategy are outlined below.

Communications Goal	Description	Role of CIO
Inform	Create awareness	Steward
Request	Encourage action	Motivator
Position	Create a placeholder for future action; put in context of larger vision	Change agent
Consult	Refine ideas	Consultant
Evangelize	Create an extension of the CIO communications process with a person who can act as a surrogate and becomes part of the communications team	Inspiration

4.2 OIMT STAFF

This section describes the role of the OIMT staff.

4.2.1 SENIOR COMMUNICATIONS MANAGER

The Public Information Officer (PIO) is the core individual responsible for communications within State agencies. Within OIMT, the Senior Communications Manager will be charged with the responsibilities of a PIO including, but not limited to:

- Identifying and developing implementation strategy for communication mechanisms, as well as maintenance and management of identified mechanisms
- Developing and ensuring delivery of consistent and accurate messaging
- Serving as the Office's spokesperson
- Writing and disseminating all OIMT releases (or reviewing and editing, as appropriate)
- Responding to inquiries from all media outlets and other public communications agencies (e.g., industry blogs, industry associations, etc.)
- Reviewing and approving articles drafted by third parties
- Drafting and coordinating internal OIMT communications (e.g., departmental memos, employee messages, etc.)
- Establishing and facilitating OIMT Communication Forums
- Developing policies, procedures, etc.

4.2.2 PROGRAM/PROJECT MANAGERS

The Program/Project Manager is responsible for completing the project template, including a clear explanation of the benefits of the project. The Project Manager is also responsible for identifying stakeholders, holding sessions with key stakeholders, and mapping any resistance.

5.0 KEY ELEMENTS

5.0 KEY ELEMENTS

For the *Communications and Outreach Plan* to be successful, there are several key elements that must be present..

Key Element	Impact
Involved leadership	Demonstrates support of transformation initiatives, reinforces credibility and authority of messages, and provides context and background for forthcoming activities and actions.
Deliverer and receiver alignment	Recognizes unique characteristics, needs, and motivations of stakeholder groups
Ownership of communications	Ensures understanding by top level management and communicated to subordinate staff
Effective feedback mechanisms	Allows for two-way dialog and engagement with stakeholders; provides method to understand that messages are being received
Credibility of messaging and content	Builds trust with stakeholders; dispels rumors and incorrect assumptions
Consistency and frequency of messages	Reinforces messages and re-emphasizes credibility
Balancing macro and micro communications	Provides specific messages for the overall transformation and the individual projects that will be implemented

5.1 CONSISTENCY AND FREQUENCY OF MESSAGES

As we communicate with both internal and external audiences, there are a number of themes that should frame our communications as much as possible. Emphasizing these themes will counter and dispel rumors that may occur, alleviate any concerns felt by State of Hawai'i employees, and quell sideline discussions about the transformation.

Not only is it important to provide consistent messages, but also to communicate these messages frequently. The more frequently someone hears a message, the more likely they are to fully absorb and process it.

5.1.1 THE MESSAGES

Message 1: The transformation will benefit State of Hawai'i citizens through improved delivery of services and programs (e.g., going online instead of waiting in line), a more transparent and responsive government, and increased access to information and data.

Message 2: The transformation will benefit State of Hawai'i employees with streamlined processes that allow more focus on serving customers and access to a wider range of new technologies to support departmental mission, programs, and services.

Message 3: The transformation will benefit the State of Hawai'i government through efficiently aligned services, reduced costs, and unnecessary redundancies, increased reliability and security, and improved outcomes and accountability.

5.2 BALANCING MACRO AND MICRO

It is important to actively communicate both the macro (overall transformation benefits, timeline, etc.) and the micro (individual projects and wins). Each transformation project should have a communication plan and a clear explanation of the benefits. Before launching a project, the Project Manager should identify the key stakeholders, meet with them, and identify any concerns. This information should be used to map the support/resistance for a given project.

5.3 BRANDING

As part of the activities that the State of Hawai'i will undergo, especially with the many communications activities that will be initiated, OIMT should create specific branding standards, logos, and templates to identify transformation communication vehicles. All items must be developed in accordance with identified State of Hawai'i standards. The branding items, logos, and templates will support various communications activities including, but not limited to:

- News releases
- Status reports (annual, weekly, ad-hoc, etc.)
- PowerPoint and keynote presentations
- Memorandums
- Printed newsletters
- Online communications (websites, blogs, e-newsletters, etc.)
- White papers
- User manuals
- Policies, procedures, and standards
- Educational, outreach, and marketing collateral materials (e.g., posters, brochures, flyers, etc.)

6.0 COMMUNICATION CHANNELS, METHODS, AND TOOLS

6.0 COMMUNICATION CHANNELS, METHODS, AND TOOLS

This Plan proposes a number of different communication vehicles to inform and stakeholders up to date with specific types of information. The three primary types of interaction recommended are:

- Printed material
- Personal interaction
- Online communications

Some of the communication vehicles are push: information is provided or pushed to individuals on a regular basis. In other cases, the communications are pulled by stakeholders interested in the information, but it remains OIMT's responsibility to ensure the information is available to be pulled.

This Plan will evolve as the transformation progresses to best suit the needs of OIMT and the stakeholders of this initiative. As transformation activities occur, it will be important to communicate with internal and external audiences to address and alleviate concerns and fears that may arise and to build momentum around the organizational and cultural changes that need to occur for the transformation to be successful. Thus the State of Hawai'i CIO, Business Transformation Executive, Senior Communications Manager, and other individuals will regularly review and evaluate the effectiveness of the existing Plan to ensure it is meeting the organization's needs.

6.1 PRINTED MATERIALS

The following types of printed materials are proposed.

6.1.1 GOVERNOR AND LEGISLATIVE BRIEFINGS/REPORTS

Briefings and written reports to the Governor and members of the State of Hawai'i legislature should provide updates on the transformation activities. It is also a forum where these stakeholders are informed and educated on the necessary resources needed to support an effective and efficient IT/IRM discipline, funding requirements, management and oversight needs, proposed legislative changes, etc.

Reports will include, but not be limited to:

- *Reports to the Governor* (monthly updates)
- *Reports to the Legislature* (quarterly and annual reports as required by statute)
- *State of Hawai'i Chief Information Officer Annual Report*

6.1.2 OPINION-EDITORIAL PIECES

Opinion-editorial (op-ed) pieces are bylined editorials that position the CIO, Business Transformation Executive, and other members of the staff as champions of transforming government services through business re-engineering and IT modernization.

6.1.3 EARNED MEDIA PLACEMENTS

Earned media placements, garnered through media relations, will generate more target audience exposure to OIMT's key messages. These placements will also ensure that opinion formers and stakeholders are aware and updated on the transformation initiative. Placements in daily papers as well as broadcast and online media outlets will amplify support of the transformation initiative.

6.2 PERSONAL INTERACTION

The following types of personal interactions are proposed as effective means of communication.

6.2.1 GOVERNANCE COMMITTEES

The CIO and support staff will have continued personal interaction with the governance bodies identified throughout this document including, but not limited to:

- IT Steering Committee
- Executive Leadership Council (ELC)
- CIO Council (CIOC)

6.2.2 FACE-TO-FACE TOWN HALL MEETINGS AND COFFEE HOURS (INTERNAL STAKEHOLDERS)

Town hall-type meetings can be held at various locations to allow the CIO and OIMT to engage with both IT and non-IT employees regarding the *Business and IT/IRM Transformation Plan*. Staff will have the opportunity to ask questions of the CIO and gain a better understanding of the benefits of the transformation.

6.2.3 SPEAKING ENGAGEMENTS (EXTERNAL STAKEHOLDERS)

Speaking engagements with the appropriate organizations, business/community groups, and industry associations provide the opportunity to engage external stakeholders throughout the transformation process. Key messages will focus on the progress the transformation is making and how it is impacting the community, industry, and businesses.

6.3 ONLINE COMMUNICATIONS

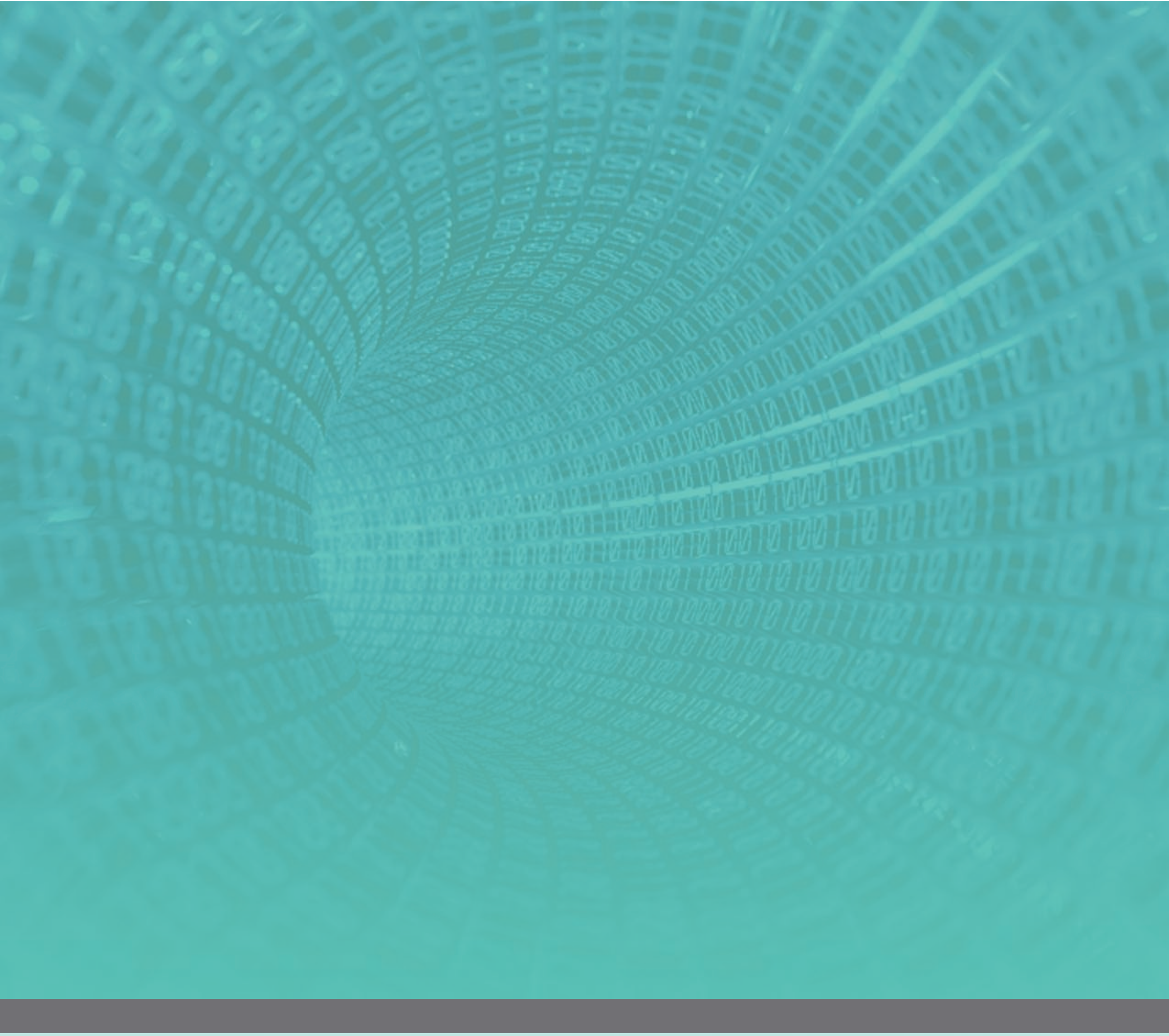
Online communications methods are outlined below.

6.3.1 OIMT WEBSITE AND BLOG

The OIMT website will be a primary online outlet to communicate with external audiences. The website will include a blog that can be authored by the CIO, Deputy CIOs, and other OIMT staff as appropriate.

6.3.2 ELECTRONIC NEWSLETTERS

Electronic newsletters, also known as e-newsletters, will allow subscribers to receive information on a regular basis from OIMT. The e-newsletter will provide a few key details on important projects, initiatives, and events, and drive readers to the OIMT website for more information. Users will be able to subscribe to the e-newsletter on the OIMT website and have it delivered directly to their inbox.



POLICY PLAN

TABLE OF CONTENTS

1. EXECUTIVE SUMMARY....4

2. INTRODUCTION....6

2.1 PURPOSE....7

2.2 SCOPE....7

3. BASIC PROGRAM ELEMENTS....8

3.1 MISSION....9

3.2 VISION....9

3.3 GOALS....9

3.4 OBJECTIVES....10

4. PROGRAM DELIVERABLES....11

4.1 FOUNDATIONAL POLICY CATEGORIES....12

4.2 WRITTEN DOCUMENTS WITH VERSION CONTROL....12

4.3 DEFINED MANAGEMENT STRUCTURE....13

4.4 TARGET USER GROUPS....13

4.5 POLICY COMMUNICATIONS AND EDUCATION PLAN....13

4.6 VERIFIED AUDIT TRAIL....13

4.7 WRITTEN EXCEPTION PROCESS....14

4.8 ENVISIONED PROCESS....14

5. MAJOR SCHEDULED EVENTS (MILESTONES AND REOCCURRING)....16

5.1 POLICY PROGRAM MILESTONES (NON-STAFFING)....17

5.2 POLICY PROGRAM MILESTONES (STAFFING)....17

6. COSTS....19

6.1 IDENTIFY PROGRAM COSTS (INCLUDING COSTS APPROVED BY THE OIMT)....20

6.2 CRITICAL SUCCESS FACTORS....20

6.3 ASSUMPTIONS....20

6.4 TECHNICAL CONSTRAINTS....21

7. RISKS......22

8. RESOURCE REQUIREMENTS......24

8.1 FY-2014 TEAM STRUCTURE (NOTIONAL)......25

9. ROLES, RESPONSIBILITIES, AND STAFFING......26

9.1 ROLES AND RESPONSIBILITIES......27

9.2 PROGRAM STAFFING PLAN......29

10. DELIVERABLES......30

10.1 PROGRAM DELIVERABLES......31

11. PROGRAM CONTROLS......32

11.1 POLICY AND SECURITY......33

12. ASSOCIATED DOCUMENTS......33

13. WORKS CITED......33

14. REFERENCES......33

15. GLOSSARY OF ACRONYMS......33

APPENDIX A: CROSSWALK OF POLICIES......34

FIGURES

FIGURE 1: POLICY GOVERNANCE PROCESS......14

FIGURE 2: POLICY PROGRAM TEAM ORGANIZATION FY-2014......25

TABLES

TABLE 1: MILESTONES (NON-STAFFING)......17

TABLE 2: MILESTONES (STAFFING)......17

TABLE 3: ANNUAL FY-2013 ESTIMATED OPERATING COSTS......20

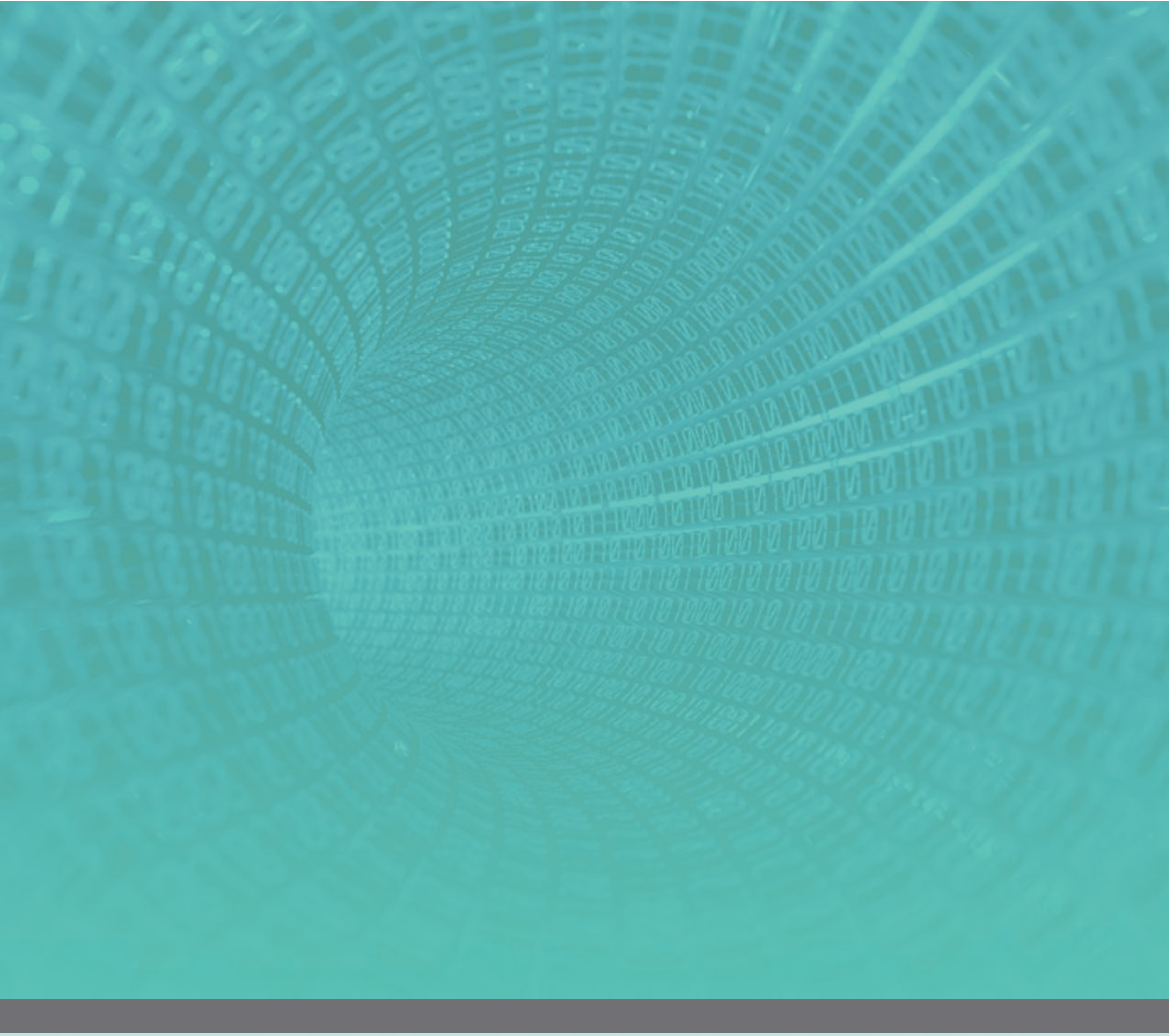
TABLE 4: RISKS......23

TABLE 5: ROLES AND RESPONSIBILITIES......27

TABLE 6: PROGRAM STAFFING PLAN BY OIMT ENTITY......29

TABLE 7: MINIMUM PROGRAM STAFFING PLAN......29

TABLE 8: PROGRAM MANAGEMENT DELIVERABLES......31



1. EXECUTIVE SUMMARY

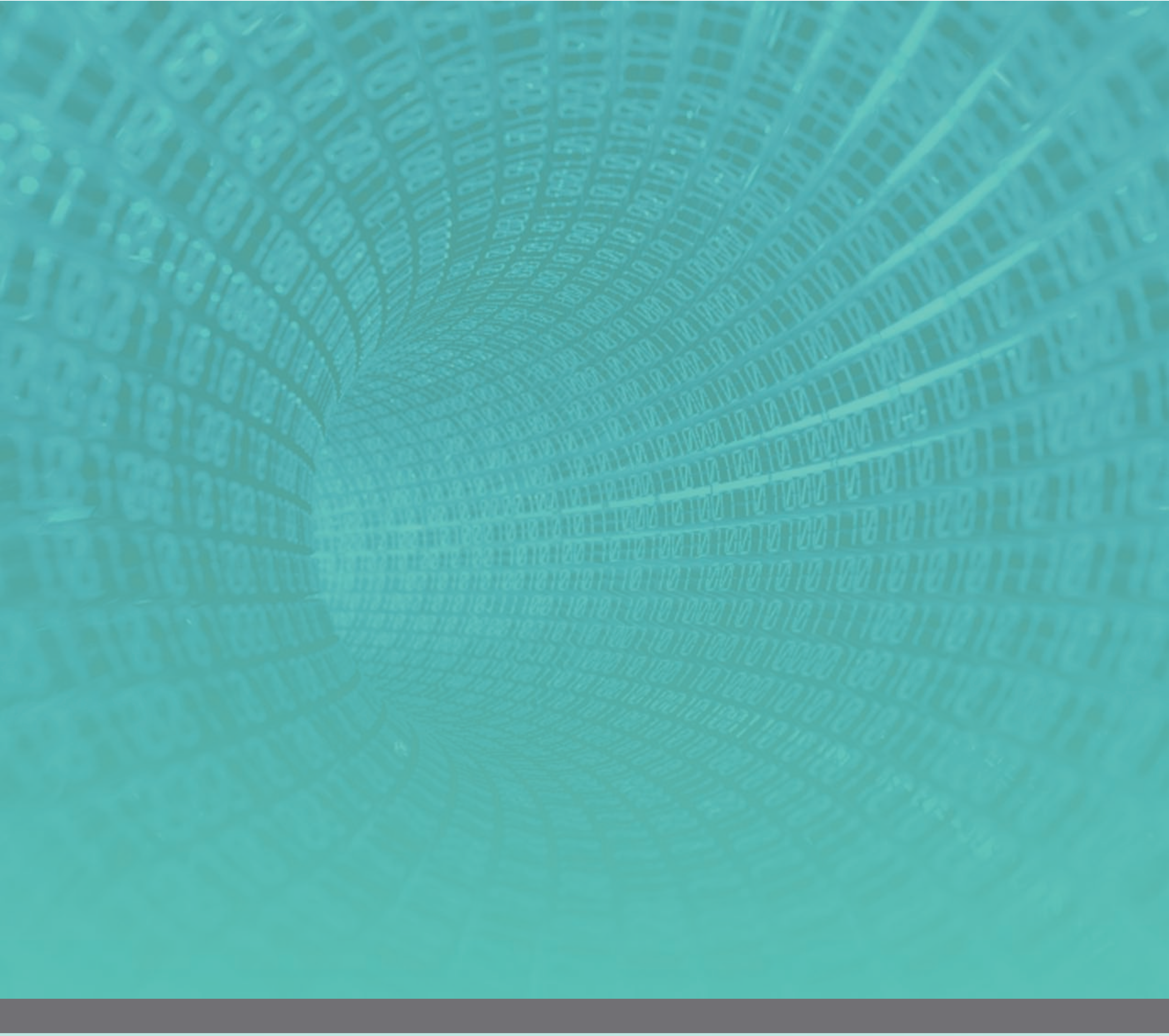
1. EXECUTIVE SUMMARY

A review of the State's fragmented Information Technology (IT) Policy Program by the Office of Information and Management Technology (OIMT) concluded that there is currently insufficient funding and staff support to meet today's policy requirements. Most agencies do not have a dedicated policy officer, nor are there consistent sets of policies used across the state.

The OIMT will soon provide governance and oversight for the IT infrastructure for a large portion of the state agencies as described in the Plan. In addition to guidance and directives regarding IT infrastructure the acting Chief Policy Officer (CPO), under the Chief Information Officer (CIO), also provides guidance, development, oversight, and assistance regarding policy.

The CPO is responsible for partnering with the Policy Working Group in formulating overarching State IT policy and overseeing agency/office implementation and achieving the State's strategic goals in support of the OIMT vision for enterprise IT policy. Policy will heavily rely on subject matter experts (SMEs) across the State as well as OIMT Working Groups to provide assistance with development and structure. Value to both the customer and the public is promoted through the use of State-approved standards, compliance requirements, and industry best practices.

It is envisioned that all enforcement and audit functionality will be defined as part of the governance development process contained in other sections of the Plan and will not be addressed in this document.



2. INTRODUCTION

2. INTRODUCTION

2.1 PURPOSE

Entities rely on policy to provide operating guidelines, and beyond that the business requires actual operating instructions. These instructions are delivered in the form of implementations of policy. It is imperative that a means of tying policy to its implementations be found, as well as measuring both policy and its implementations for effectiveness, so that the entity does not perceive its operating instructions as detached, irrelevant, contradictory, and ineffective. Policy governance ties policy and implementation formulation to measurements of usefulness to achieve better results for the State.

Policy governance, by definition, is a cyclic process that not only creates policy and its implementation but also measures policy and implementations for efficacy. It is the intention of the State of Hawai`i to provide proper attention to the measurement aspects of policy governance, ensuring its effectiveness. Furthermore, it is the objective of the State to be consistent in the mapping of policy and its implementations and enable enterprise transparency initiatives while increasing enterprise institutional knowledge. Policy governance is both applicable and needed in identity management and privacy settings.

This document will define the future requirements that will strengthen the framework on how the State develops, articulates, and implements IT policy for the Executive Branch and also defines the steps needed to build a consistent and comprehensive policy program.

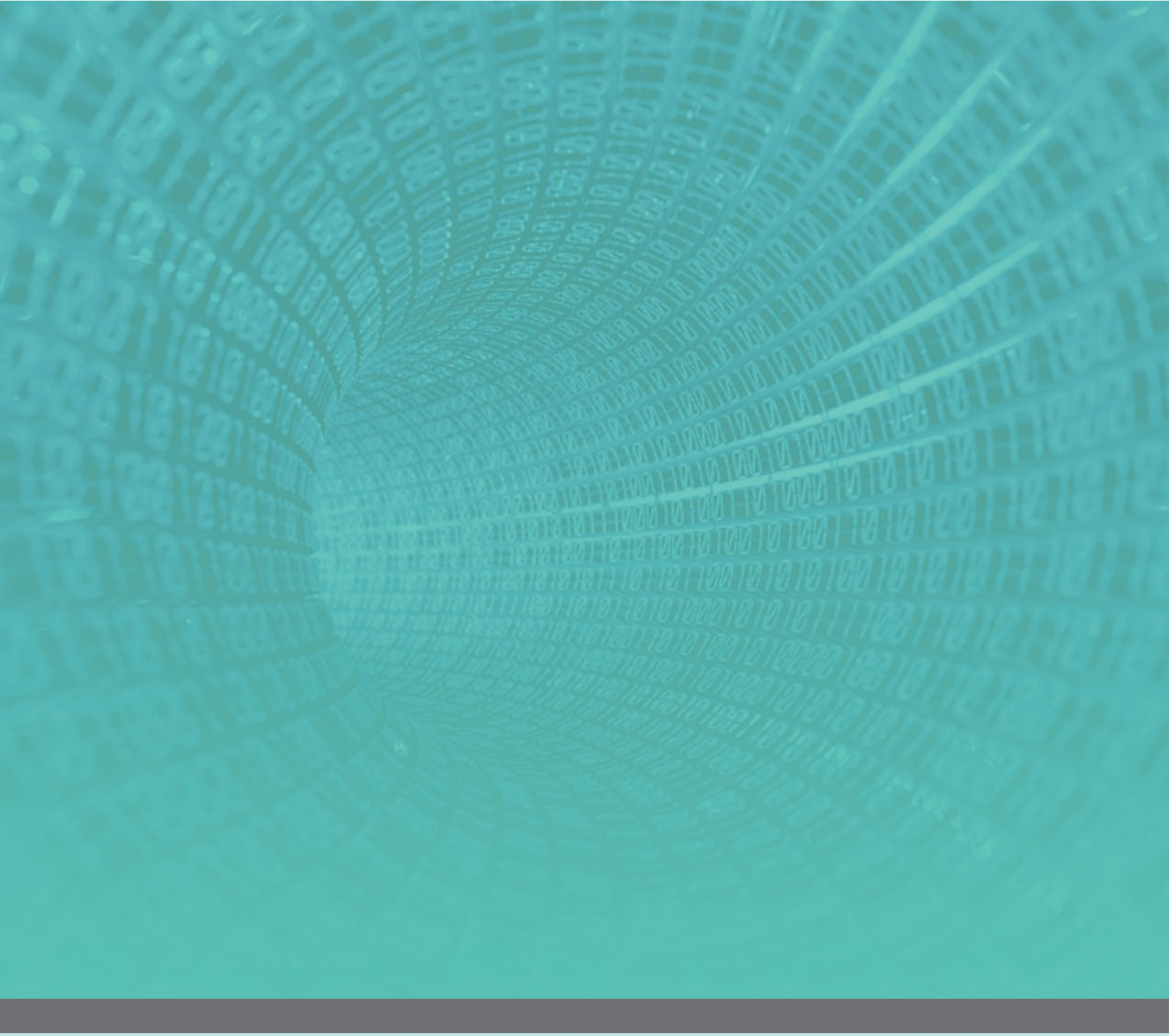
This document is a living document that will be kept current throughout the course of the program.

2.2 SCOPE

This document will define the scope and structure for the policy program for all Executive Branch agencies. In the future, this program may extend to other branches ensuring consistency of IT policies across the State.

In concert with the Policy Working Group, the Policy Specialists identified to be hired FY-2014 will accomplish the following in FY-2015:

- Better synchronization between the Policy Working Group, State Agencies, and the CIO Council (CIOC) in the development, provisioning, and implementation among the agencies in support of consistent and clear enterprise policies
- Proactive and relationship-building steps with auditing agencies
- Develop and update a policy program to educate staff on the policies and make an easily navigable web page where they can be housed to ensure both understanding and compliance
- Develop common nomenclature to be used across all policies and procedures
- Review agency/office additional requirements for accuracy and validity and incorporate them into the main policy library
- Updating of the OIMT Policy manuals and handbooks and writing new policy and templates where needed
- Provide oversight and reviews ensuring Agency Policy Officers utilize best practices and standards in their work with systems documentation, policy reporting, and other policy concerns
- Conduct policy technical evaluation and compliance reviews for agencies and offices
- Develop role-based policy training
- Develop and conduct policy workshops and policy awareness campaigns
- Creation of a centralized policy website for use across the Executive Branch
- Vigilantly keeping current with new policy legislation and guidance, and promptly disseminating it and incorporating it into Agency practices
- Increasing and stronger liaisons with external agencies, commissions and working groups regarding government-wide policy policies, initiatives, and matters
- Adoption of a very pro-active stance regarding policy guidance and implementation throughout the State to promote best practices and minimize risk while coordinating with other key programs
- Availability for providing ongoing policy subject matter expertise for the highest offices within the State, as well as increased ongoing support for Agencies including their Policy Officers
- Development of non-agency specific templates and guidelines for procedures, supply of best standards for application of policies



3. BASIC PROGRAM ELEMENTS

3. BASIC PROGRAM ELEMENTS

This section defines the mission, vision, goals, and objectives of the policy program.

3.1 MISSION

The Policy Working Group shall define and execute the process for establishing enterprise IT standards for Hawai`i State government entities. Enterprise IT standards provide several benefits to the State. These benefits include reduced costs, increased productivity, increased shared solutions, simplification of processes, and increased employee understanding and compliance. Standards may define or limit the tools, proprietary product offerings, or technical solutions which may be used, developed, or deployed by state government entities and their service providers. They may also define limitations, structure, methods, operational restrictions or processes, and obsolescence.

The policies developed will be ever-evolving—developed and maintained in such a way that they can be nimble and responsive to changes in Federal regulations and requirements as well as the requirements of Hawai`i State law.

The policies recommended and roughed by subject matter experts and the OIMT Working Groups with final development by the Policy Specialists will ensure:

- The State deploys and operates systems and technical solutions with uniformity in technology standards, process, methods, and protection of information
- The OIMT lays a solid policy framework to be used by agencies to successfully meet or exceed audit requirements
- The CIO maintains oversight in the development of the State policy structure
- That technology standards and systems reflect the collective input, technical knowledge, and programmatic expertise of State government entities
- A solid framework ensuring protection of confidential and personal information instills public confidence in government
- There is promotion of opportunities and standards for more seamless intra-agency common solutions
- A process of continuous improvement is in place and has a direct effect on the implementation of policy

3.2 VISION

The OIMT must proactively implement policy that will provide a statewide standard to ensure uniformity in technology standards, process, methods, and system. The OIMT must ensure that these policies are implemented to include recommendations and requirements associated with Federal Information Security Management Act (FISMA), the National Institute of Standards and Technology (NIST), the Federal Bureau of Investigation (FBI), the Criminal Justice Information Services (CJIS) Security Policy, Health Insurance Portability and Accountability Act (HIPAA), PCI Data Security Standard (PCI DSS), Americans with Disabilities Act (ADA), Internal Revenue Service Publication 1075, and other standards, agency audit requirements, guidelines, and best practices to comply with numerous laws and reporting requirements concerning policy. The vision is a lofty one that will take concentrated effort and cooperation across the State for many years. Substantial parts of the vision will require not only funding, but also dedicated staff and ongoing training for employees. By putting solid and consistent policies in place, we will build trust in government by the public in being good and secure stewards of their information, make it easier for staff to understand and meet expectations, and develop standardized procedures that streamline processes.

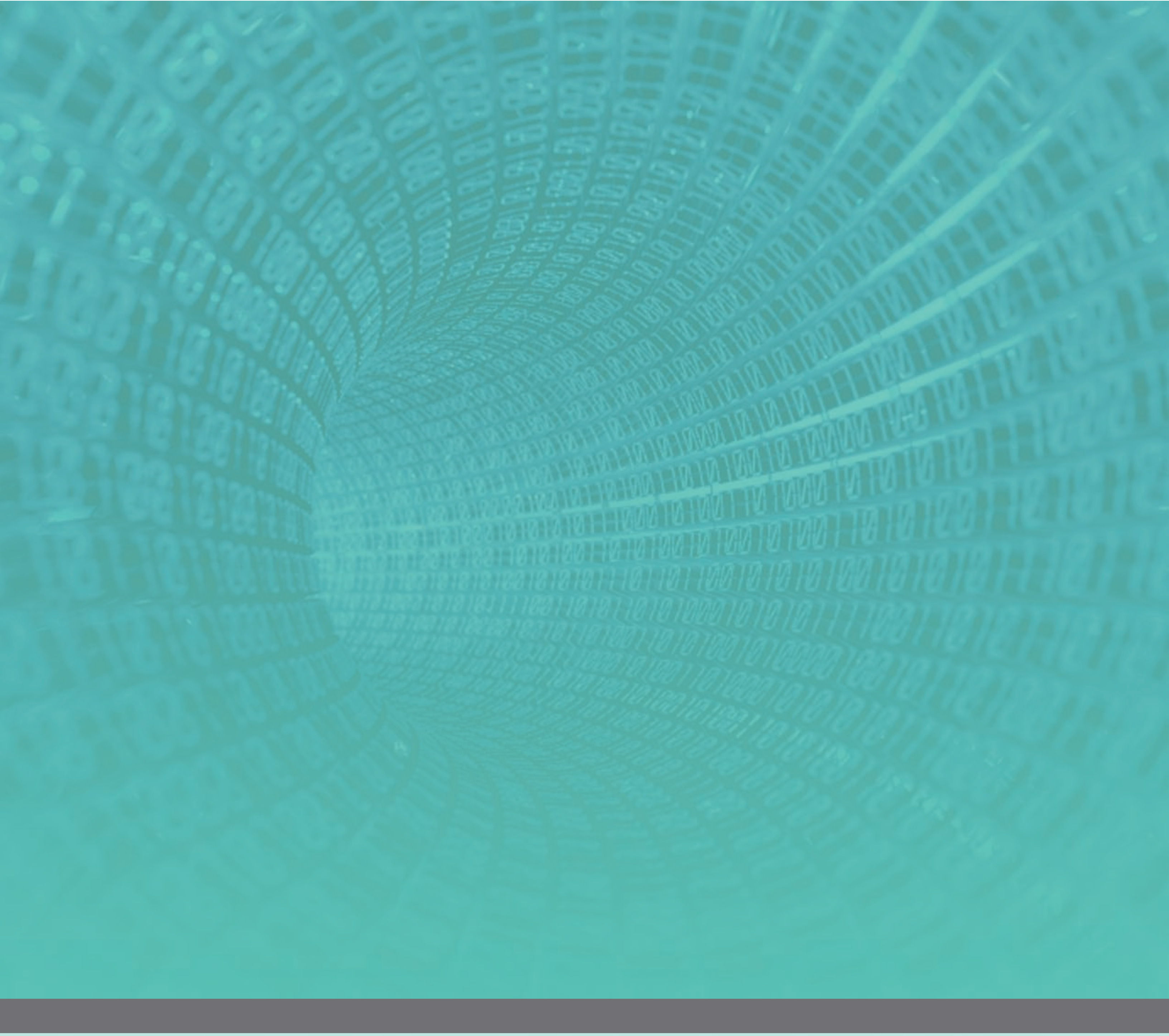
Establishment of a consistent policy governance structure is critical to streamlining policy development and implementation. Policy must also be differentiated from standards and procedures. Policy documents will contain the overarching governance concepts whereas standards and procedure documents contain the operational practices. As an example, a Password Policy defines the high level goals to build and sustain strong passwords. It would refer to a Password Standards document that defines the detailed rules and controls that make up a strong password such as password length, complexity, and history. Policy documents are intended to change less frequently than procedure documents that would be updated more frequently in response to rapid changes in technology.

3.3 GOALS

The goal of the OIMT Policy Program is to achieve excellence in IT policy establishment and compliance. Risks of not having a comprehensive policy structure in place can result in adverse findings during a Federal audit potentially resulting in fines or the loss of federal funds. Such risks involve general compliance issues with wide-ranging and very serious ramifications: We must work to ensure public trust, to ensure the minimization of negative media exposure; continuity of government, and to guarantee compliance with State and Federal requirements in order to prevent funding issues, additional scrutiny, and loss of State or public confidence.

3.4 OBJECTIVES

Program staff will be utilized to provide coordination, oversight, and comprehensive policy program direction for policy matters across the Executive Branch. This will support OIMT mission goals by increasing accountability, and enhancing functional integration. This will result in increased alignment between OIMT policies across the Executive Branch with OIMT enterprise initiatives. We will also utilize program staff to assist in updating procedures and training. Staff will conduct improved oversight of the new procedures and training, which will decrease State risk and provide support in conjunction with privacy and security staff to Executive Branch agencies for successfully passing audit and swift and comprehensive resolution of any adverse policy or procedural findings. Efforts can be undertaken to promote greater policy and security awareness throughout the State.



4. PROGRAM DELIVERABLES

4. PROGRAM DELIVERABLES

This section will outline the steps that will be taken, processes to be used, documentation to be developed, and procedure that will be put in place in the delivery of the Policy Program.

4.1 FOUNDATIONAL POLICY CATEGORIES

The Policy Working Group has established the following major policy categories in which the individual specific policies will be aligned with:

- Access Control
- Configuration Management
- Contingency Planning
- Incident Response
- Media Protection
- Physical and Environmental Protection
- Security and Privacy Awareness Training
- System and Information Integrity
- System and Services Acquisition

In addition to the above, a common set of terms and definitions will be developed and used across all policies as well as a standard set of classification labels.

4.2 WRITTEN DOCUMENTS WITH VERSION CONTROL

Even though it seems apparent, nearly every security standard and framework explicitly requires information security policies to be written. Since policies define management's expectations and stated goals for protecting information, policies cannot be implied, but must be documented. Having a written policy document helps to ensure standards are clear and concise, as well as ensures consistency and fairness. A written policy is the first key control established within the international standard ISO/IEC 1-7799:2005 which is currently the globally accepted best practice standard for information security, and is essential to performing both internal and external audits as it standardizes operations for conformity.

Policy documents need to be written in plain and simple language ensuring it is easy for both IT professionals and end-users to read, understand, and comply with. Since user education and training is a key component of all information security frameworks, clear, user-oriented language is critical.

Development of a standard template and format to be used across the State is essential so that policies can be effectively managed and updated. The standard format not only imposes consistency among documents, it ensures that each document contains key components that facilitate the overall management of the information security policies, such as the owner/author, title, scope, and effective dates of the policy. Each policy shall contain the following critical elements:

Title: The name of the policy should be as specific as possible—not more than six words.

Reference number: A reference number or code to assist with filing and identification.

Summary: Including a one or two-line summary of the policy is particularly useful when an index of policies is to be posted on the intranet.

Policy objective: This states the objective of the policy. It should also briefly explain the intent, making it clear despite potential complexities of detail later in the document.

Intended audience: A brief statement of the roles and/or locations chiefly targeted by this policy.

Exceptions: A brief statement if exceptions to the policy will be allowed and for what reasons and length of time.

Policy statement: The main content of the policy. This may have several subsections. It may also include diagrams and charts to promote better understanding.

Background material and references to other documents: References to other material that is essential to understanding the policy. It is important to ensure that these references are kept up to date, particularly when the policy is on an intranet and the references are hyperlinks that may change. This also helps to avoid too much background material into the policy document itself.

Compliance statement or reference to compliance framework: Each policy should contain, or be associated with a compliance statement saying who it affects and how (compulsory, advisory, or indicative). If the compliance statement is complex or will change frequently, it should be kept separate from the policy itself for reasons of simplicity and focus.

Roles and responsibilities for the policy: This section includes the job titles, names, and contact details of the people or group who have specific roles within the policy (for example, the people who have data protection and data privacy responsibilities).

Contact names for further information: This may be the author of the policy or others who can give explanations or guidance on what it means or how to apply it.

Policy dates, version number and change history: This includes the date the policy was approved and issued. It may include the date it comes into force if different from the issue date. There may also be an expiry date if the policy is intended to be of finite duration (for example, a special limit on hardware purchase while changing suppliers). Include a change history with dates and references to previous versions. Not only is this helpful for understanding what policy was in force at some specific time in the past, but it may be essential for legal or regulatory reasons to maintain such an audit trail. It must include a version number, following the enterprise standard.

Review timetable: This says when and by whom the policy will be reviewed or if the policy will remain in force without time limit and without review.

Policy owner: This is the job title, name, and contact details of the person or group responsible for the implementation and enforcement of the policy.

Change authority: This includes the job title, name and contact details of the person or group who has authority to change the policy or give exception waivers to it. If appropriate, also include a summary of the process for requesting and authorizing changes

References: Optionally, include references to related documents (as paper documents or hyperlinks) both internally and externally (for example, to ISO, NIST, COBIT, or ITIL documents).

4.3 DEFINED MANAGEMENT STRUCTURE

To help keep IT policies understandable and manageable, it is important to keep the information level steady among the various document types. In other words, it is not advisable to mix policies, procedures, standards, and guidelines into policy documents.

A policy governance structure will be developed which breaks information into separate documents for policies, standards, and procedures. For example, a Password Policy would state the high-level organizational goals to build and sustain strong passwords. It can refer to a Password Standard document, which defines the detailed controls that make up strong passwords, such as password length, complexity, and history. Keeping these structural elements separate will allow updating of standards and procedures as new technologies or processes are introduced, while updating higher-level policy documents less frequently.

Documents will be placed into groups based on subject matter. Since many agencies are subject to Federal audits as a requirement of them receiving federal program funds, the choice has been made to structure policy elements under the NIST/FISMA control numbers. This same structure will be used in the organizing of documents on the OIMT Web Portal.

The Policy Working Group is a standing investigative group that will act as an ongoing advisory body to the policy staff as well as to take input from the CIOC and other councils and boards. They will assist in the development and final editing of policy, ensuring that input from agencies and SMEs is incorporated as needed.

4.4 TARGET USER GROUPS

Not all IT policies are suitable for every role in the state. Therefore, written IT policy documents will be based on the lowest common need as an example defined by NIST or FISMA concepts. Some agencies (such as Health, Labor, Tax, and Welfare) will be able to add appendices specific to their agencies to strengthen policy where required, with those added requirements being applicable to their staff or those in possession of their data or access to their systems.

For example, all users might need to review and acknowledge Internet Acceptable Use policies. However, perhaps only a subset of users would be required to read and acknowledge a Mobile Computing Policy that defines the obligatory controls for working at home or on the road. It is felt that most employees are already faced with information overload, so the goal is to organize the framework in such a way where it is easy for staff to determine what is applicable to them.

4.5 POLICY COMMUNICATIONS AND EDUCATION PLAN

Communications will follow the Communications Strategy outlined in the Governance section of the Plan. For policy communications, the following would be emphasized:

- The policy framework
- How the specific policy fits in to the framework
- If the policy has been revised, a simple way to tell what has been changed
- Clear definition of individual responsibilities as a result of the policy
- A method for simply and easily providing feedback

4.6 VERIFIED AUDIT TRAIL

Policy documents will not be effective unless they are read and understood by all members of the target audience. It is envisioned that a working group specializing in training will develop an overall IT education program that will assist in this process.

A deliverable of the Policy Team with assistance from the other working groups will be defining a proposed audit mechanism which will indicate that users have read and acknowledged specific versions of policy documents, including the date of acknowledgement with our goal to be able to verify that each person handling information within our organization has read and understood the IT policies that apply to them.

4.7 WRITTEN EXCEPTION PROCESS

It may be impossible for every part of an agency to completely follow all of the IT policies at all times due to funding constraints or other circumstance. Rather than assuming there will be no exceptions to policy, a documented process for requesting and approving exceptions to policy and clearly documenting the associated risks will be developed. Written exception requests will require the approval of senior management within the organization and also at OIMT, and have a defined time frame after which the exceptions will be reviewed again.

Policy exceptions will be managed within the same framework as the policy documents themselves. In other words, exception will be documented, have a clear owner, and can be organized by topic area.

4.8 ENVISIONED PROCESS

The process of operationalizing privacy is analogous to the enterprise policy governance in which policies are formulated, implemented, measured, and then refined and re-implemented. Although the previous statement is recognizable as a governance process (specifically a Boyd cycle), there are common behaviors that prevent this process from being continuous and thus prevent it from becoming a true governance process.

It is to be understood that policy revision and creation stem largely from influencing factors including, but not limited to: business initiatives, emerging technologies, paradigm shifts, and mandated governmental changes. It is also important to recognize that in some cases the State may need to act quickly to create or revise items within the governance framework to facilitate and expedite the process of compliance.

Ideally, the goal is that the framework that is constructed for enterprise policy governance processes follows the flow illustrated in Figure 1 and reflects the anticipated regular methodology for new IT policy development. OIMT and the CIO may abbreviate and/or expedite the process when operationally required.

Initiation: At the Information Technology Steering Committee (ITSC), the CIO will table the goal and objective for proposed new IT policies and recommended updates to existing policies or additions. Subject matter experts or OIMT Working Groups may also submit changes for consideration to the policy team.

Initial Draft: The designated individual/group will conduct sufficient research and consultation with stakeholders and technical experts to craft an initial draft and suggest a classification as IT policy, standard, or guideline. The CIO will table the initial draft for review and comment by the ITSC, prior to publishing and circulating to the State at large.

Circulation and Comment: Subsequent to comments and recommended revisions to the initial draft, the draft document will be circulated among a larger group comprised of selected individuals in the affected units/departments/communities. Comments are to be returned to the development team for review within the specified deadline.

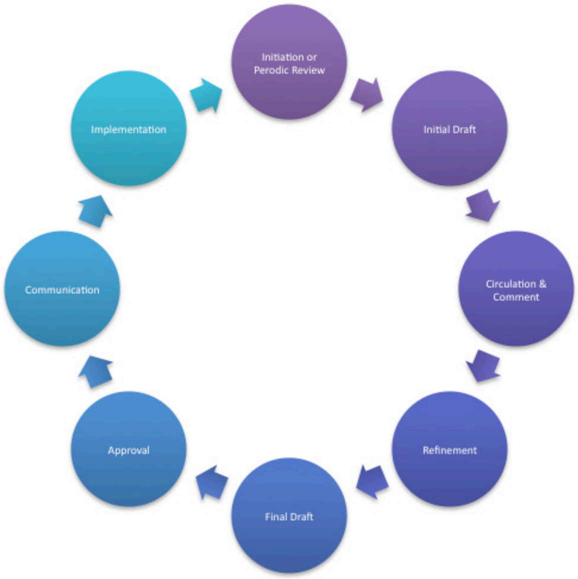


Figure 1: Policy Governance Process

Refinement: Based on comments gained during the circulation phase, modifications will be made to the policy. If significant or potentially controversial changes are made, another round of circulation and comment will occur. Further development of this process will further define when another round of circulation and comment is needed.

Final Draft: The CIO will liaise with affected stakeholders and the community at large as necessary and prior to submission of a final draft to the leadership of the affected unit/department/community for information and comment. Final drafts will be posted for information on the CIO's web site. Final drafts will include clear accountabilities, monitoring provisions, and any required reporting for compliance. A suggested timeline for review/updating will be included.

Approval: The finalized document will be submitted for approval. Following approval, the document will be posted on the CIO's website and clearly show the date it will become active.

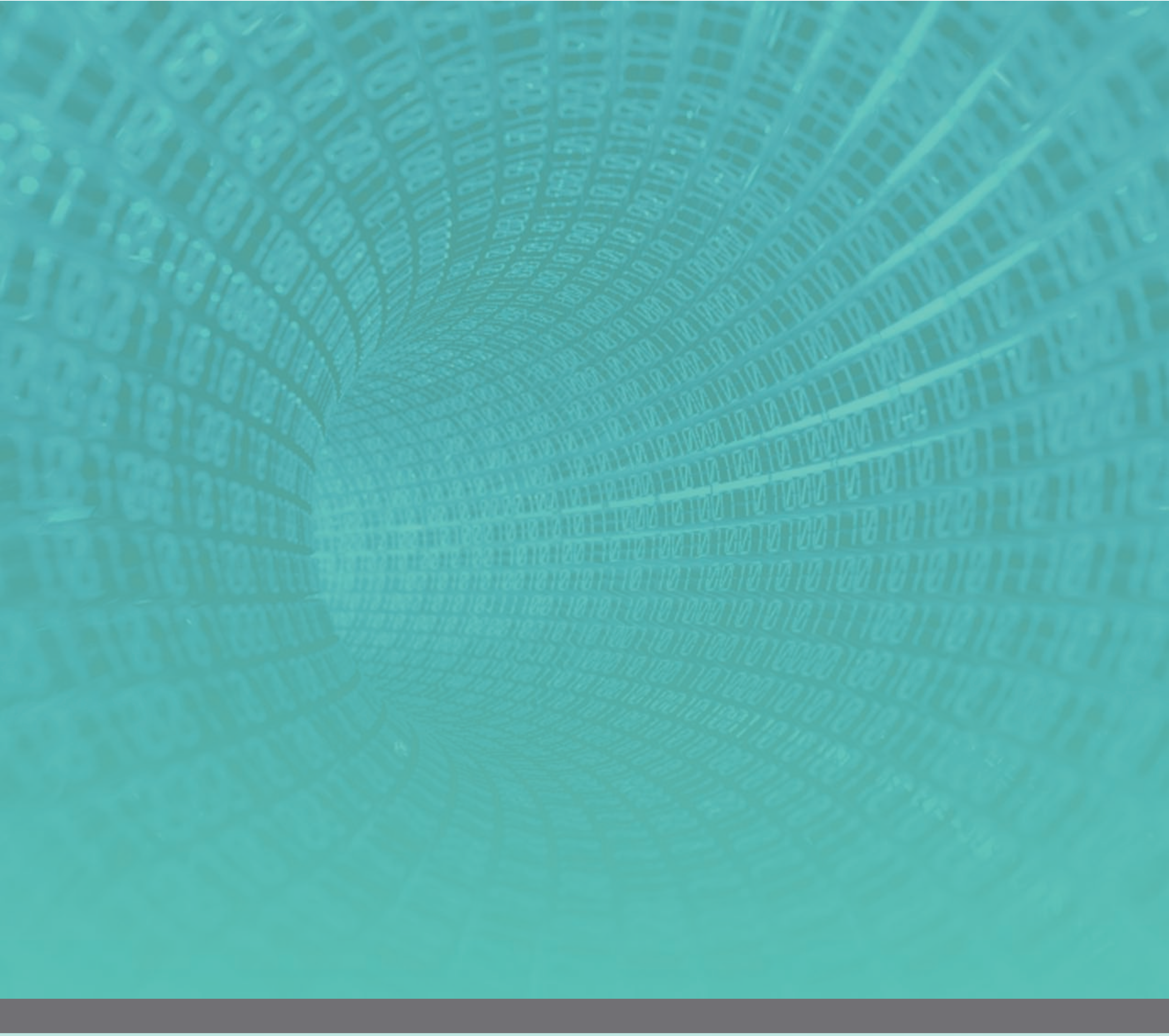
Communications: The policy will be suitably advertised/promoted ensuring affected staff is informed of and understands the policy. Multiple communication methods should be considered when promulgating any new or revised policy. Communications should include written notification (email, websites, paper memos, etc.) and face-to-face meetings of constituency groups to allow for clarification and responses to any questions. As an example, policies affecting personnel officers would be presented at meetings of personnel officers.

Implementation: A policy will become effective on the date stated in the policy document. The date shall allow at least thirty days for communication to staff and allow for any temporary exemptions to be applied for and vetted for approval or denial.

Periodic Review: Each policy should be reviewed at least bi-annually to ensure that it is still relevant with current technology, follows established best practices, and is compliant with audit requirements. Review may also take place as part of an agency Federal audit ensuring compliance.

Training: As each new policy is approved or existing one revised, each agency will be encouraged to participate in a training process that ensures that the policy is properly understood and adequately followed by procedures and guidelines, while expediting the targeted compliance.

The Continuous Improvement process will be employed as defined in the Service Management section of the Plan as elements of the policy development and review cycles.



5. MAJOR SCHEDULED EVENTS (MILESTONES AND REOCCURRING)

5. MAJOR SCHEDULED EVENTS (MILESTONES AND REOCCURRING)

5.1 POLICY PROGRAM MILESTONES (NON-STAFFING)

Table 1: Milestones (Non-staffing)

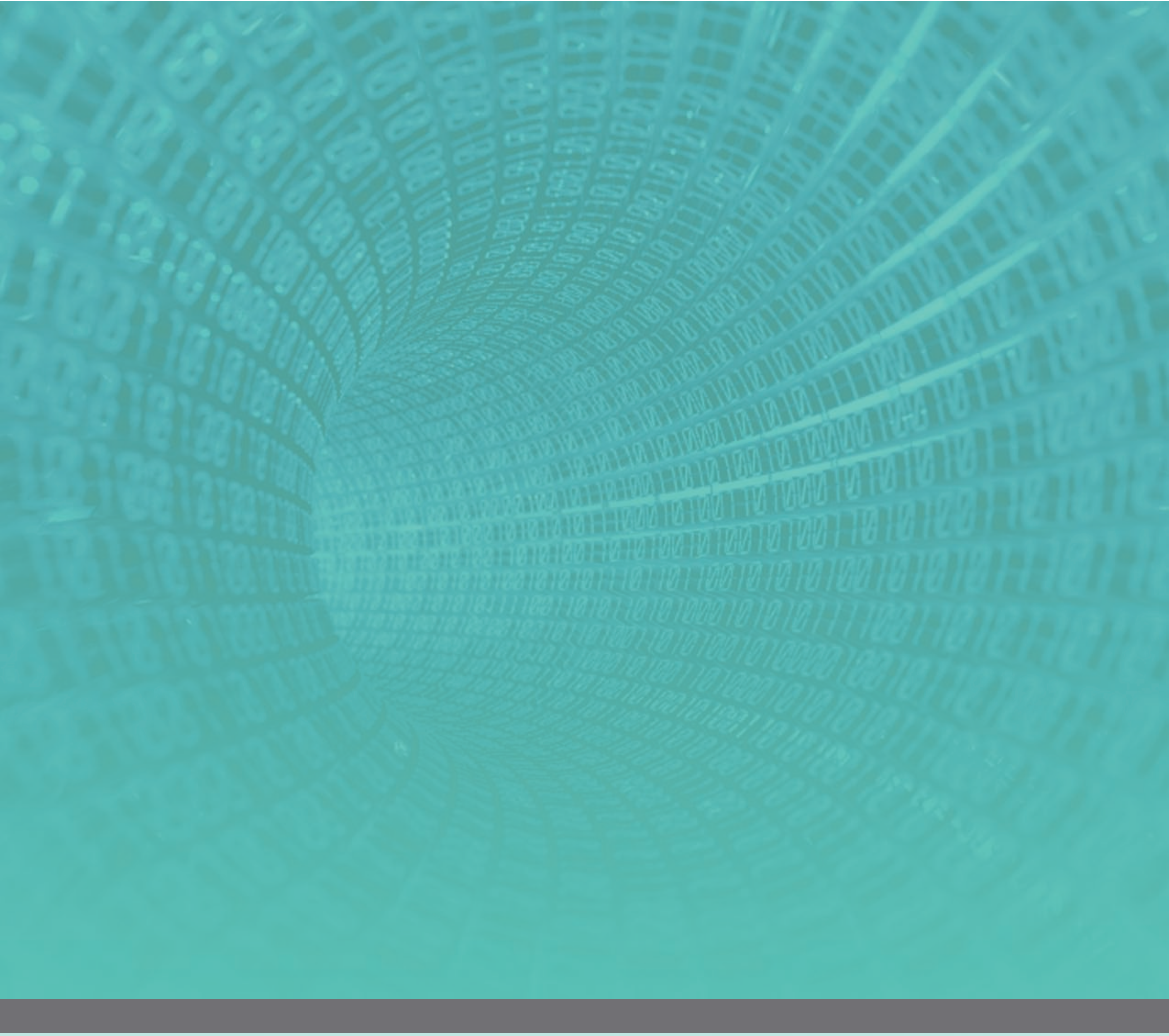
Milestones	Person or Team Responsible	Planned Completion Date
OIMT Directive on Administration Policy	Policy Officer, Information Management Chief, OIMT	FY-2015 (need FTE on board)
Complete and deploy Executive Branch policy website	Policy Officer	FY-2015 (need FTE on board)
Employee awareness and outreach to Agencies/Offices	Policy Officer	FY-2015 (need FTE on board)
Monitoring/oversight of Agency/Office Policy implementation	Departmental Policy Officers	FY-2015 (need FTE on board)
Update OIMT Policy Sections	Policy Officer and Policy Working Group	FY-2015 (need FTE on board)
Definition of training program requirements for all staff	Policy Officer and Policy Working Group	FY-2015 (need FTE on board)

5.2 POLICY PROGRAM MILESTONES (STAFFING)

Table 2: Milestones (Staffing)

Milestones	Person or Team Responsible	Planned Completion Date
Meet with Human Resources	Privacy Office, Information Management Chief, OIMT Business Manager	
Write PD	Privacy Officer	
Classify PD	OIMT HR	
Advertise vacancies (open continuously)	OIMT HR, OIMT Business Manager	
Pull first set of applicants (SR-24/26)	OIMT HR	
Set up interviews	CIO Business Manager, Privacy Officer	
Finalize interviews, give cert and recommendations to CIO for approval	Privacy Officer	
Pull second set of applicants (if needed)	OIMT HR	
Approval from CIO	Information Management Division Chief, Dept CIO, CIO	
Provide cert to OIMT HR for processing	OIMT Business Manager	
Set up interviews for second set of applicants (if needed)	OIMT Business Manager, Privacy Officer	

Milestones	Person or Team Responsible	Planned Completion Date
Make first and second offers	OIMT HR	
Meet with Human Resources	Privacy Officer	
Hire first and second applicants (on-board)	OIMT HR	
Using hiring sequence/procedures/milestones above, additional hiring in FY-2015 to cover shortfalls in hiring in FY-2014 up to two positions	OIMT Business Manager, Privacy Officer, CIO, Information Management Division Chief, OIMT HR	



6. COSTS

6. COSTS

6.1 IDENTIFY PROGRAM COSTS (INCLUDING COSTS APPROVED BY THE OIMT)

Table 3: Annual FY-2013 Estimated Operating Costs

Description	Estimated Annual Budget (Starting in FY-2014 – 4 % Increase for Each Out Year) (in Thousands $)	Basis of Estimates (Formulation Method and Source)
Personal Costs:		
Ongoing FTE expenses for two SR-26 Policy Specialists	Pending Review	Estimate of salaries
Travel:		
Travel to agency locations for Policy Compliance and training	Pending Review	Based on contractual expenses for no less than four trips/annually (includes transporting supporting documentation)
Training:		
Technical writing or focus area training	Pending Review	Based on estimates provided by previous procurement and contracts
Equipment:		
Scanners, printers, laptops, docking stations, monitors, projector, etc.	Pending Review	Based on estimates provided by previous procurement and contracts
Supplies/Printing/Minor Misc. Contracts:		
Print pamphlets, supplies, and minor contracts for updating CBTs	Pending Review	Based on estimates from OIMT, current supply expenditures, and policy pamphlets.
Total	**Pending Review**	

Note: Conferences are currently not included in these estimates. It is anticipated that SMEs will bring back injects to the policy team when they attend training or conferences as part of the continuous improvement cycle.

6.2 CRITICAL SUCCESS FACTORS

Critical Success Factors (CSFs) increase the probability of success when management focuses attention in these areas. This program's CSFs are as follows:

- Timely commitment of funds and processing of required acquisitions
- Hiring and availability of appropriately skilled staff and contractors to complete program tasks and deliverables
- Participation and commitment of program team to complete their tasks and deliverables on schedule
- Active agency participation on the Policy Working Group
- Active policy development participation by the OIMT Working Groups and SMEs

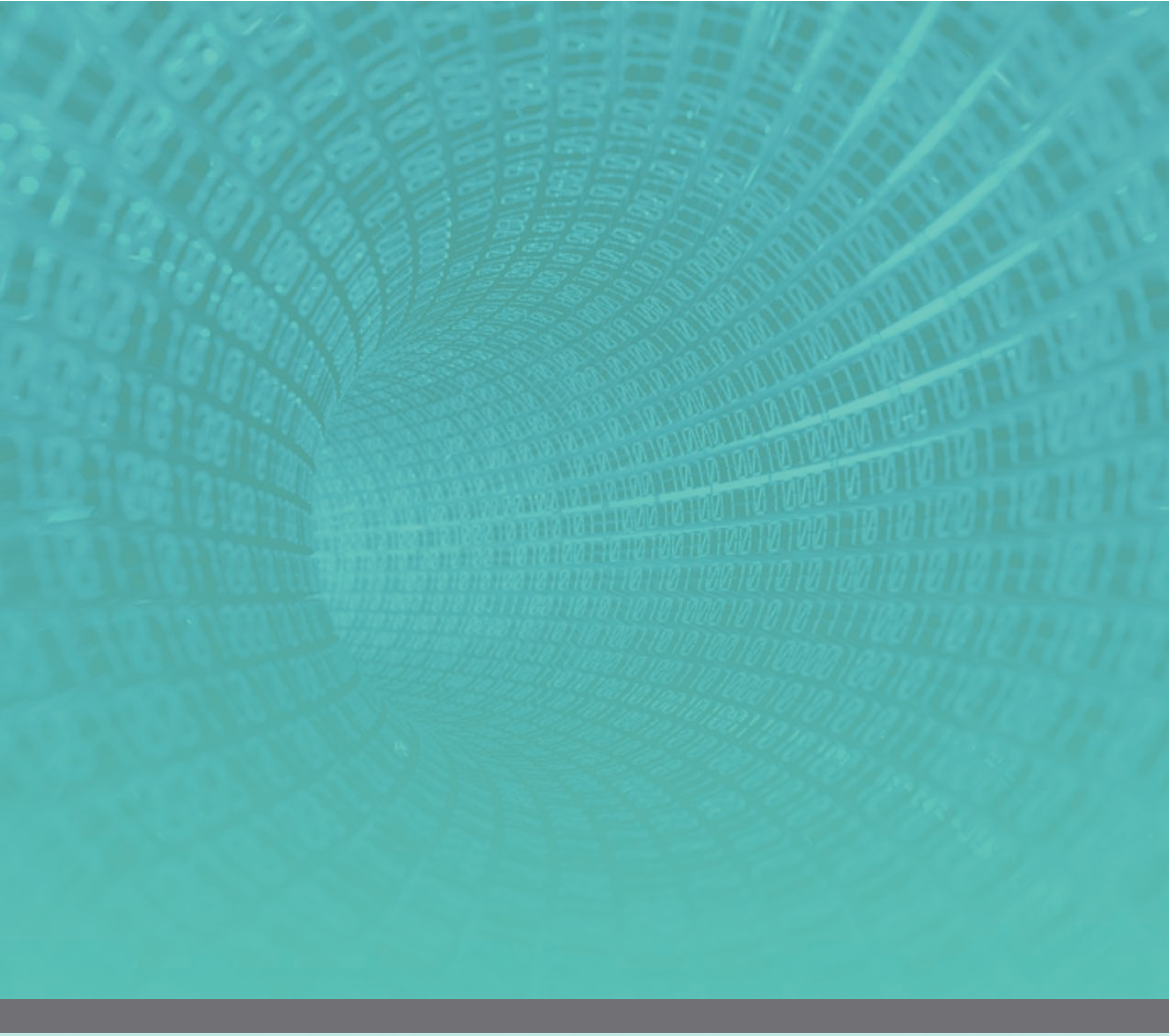
6.3 ASSUMPTIONS

Success is predicated on hiring requested staff, contractor support; fulfilling financial resources (e.g., procuring tools), implementing policies, authorities, and processes as requested.

Training tools and methodology will be developed and implemented by one of the other working groups that can implement the training needs developed.

6.4 TECHNICAL CONSTRAINTS

The Policy Program will need new and more sophisticated tools than the state currently has to more effectively track, monitor, and analyze the outputs and performance of the program. It will be necessary to have these tools to better determine and analyze quantitative and qualitative measures for the effectiveness and overall performance of policy compliance and quality at the Department. To have this evaluative capability, there will need to be new metrics, analytics, and measures for policy compliance and for policy violations, and tools to assist in investigation of policy performance. The data will provide value in measuring levels of compliance, quality assurance across the Department, areas needing correction and enforcement, and provide for improved program management.



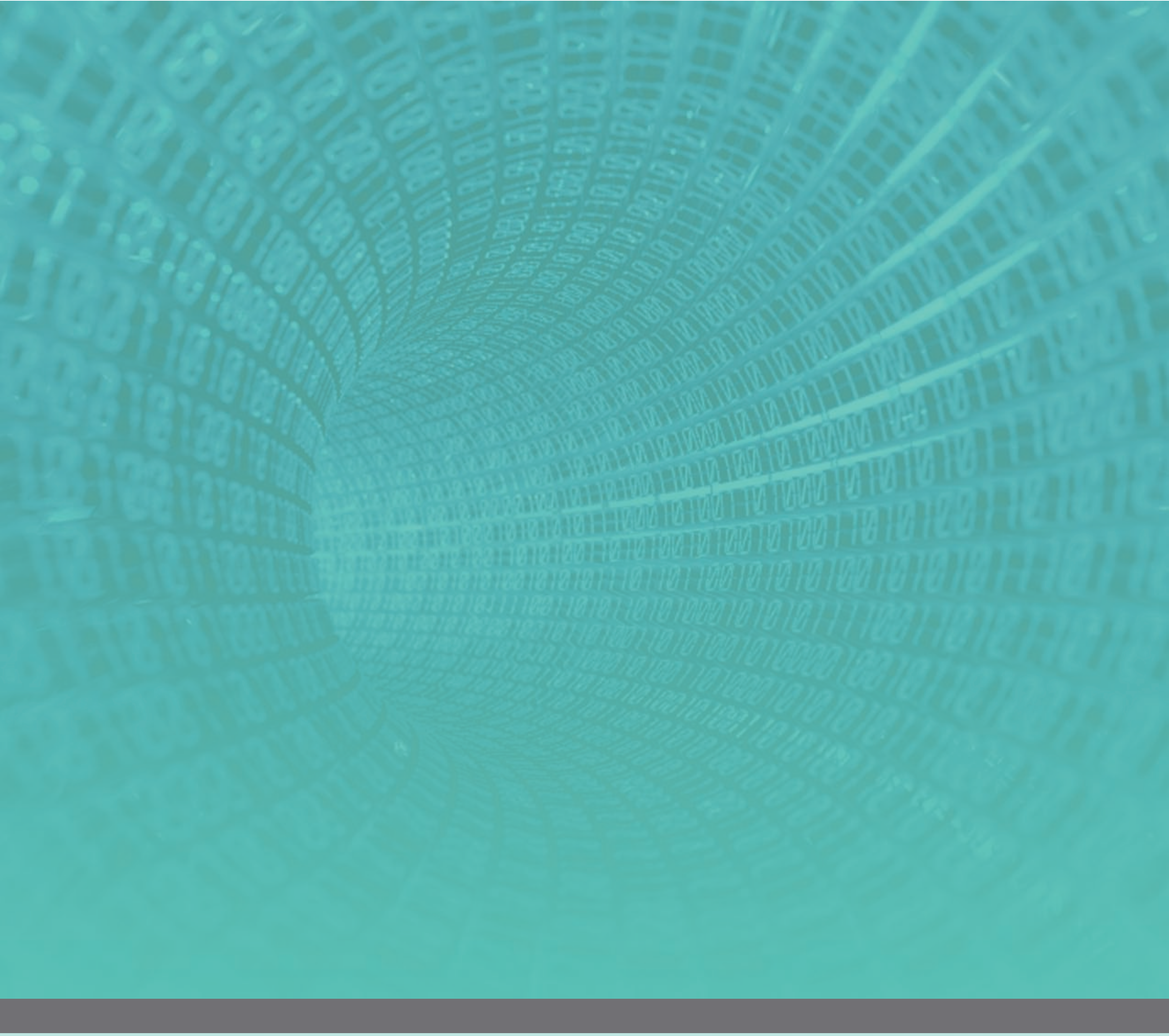
7. RISKS

7. RISKS

This section summarizes major program risks discovered at the start of the program. This program's risks will be monitored and reported as part of the Policy Program Risk Register.

Table 4: Risks

ID	Description	Probability 1 = low 5 = high	Impact 1 = low 5 = high	Mitigation Plan
1	Personnel overcommitted due to other tasks, existing duties, illness, vacations, etc. may delay program	5	5	There are only two OIMT staff members with this function. Management will need to act as the backup.
2	Contracting delays for procurements may delay program or increase costs	4	4	Extend the Program schedule, as necessary, and keep the CIO and OIMT Business Manager informed of anticipated cost issues
3	Contradictory policies across the Executive Branch	4	3	Policies will need to be combined to ensure a single policy is in effect.
4	Staff knowledge of the policy in effect	5	5	Training and awareness programs must be put in place as well as an easy navigable website and log-in banners.
5	Training of staff ensuring new policies are well understood	5	5	A working group should be formed focusing on how an IT training program can be put in place and the costs of the equipment, software, and consultants required.
6	Operational procedures and processes are developed and documented by the SMEs and technical team members once policies are developed	3	5	Assistance will be provided by the two policy specialists to guide the development of the documents and to tie them back into the main policy framework.



8. RESOURCE REQUIREMENTS

8. RESOURCE REQUIREMENTS

8.1 FY-2014 TEAM STRUCTURE (NOTIONAL)

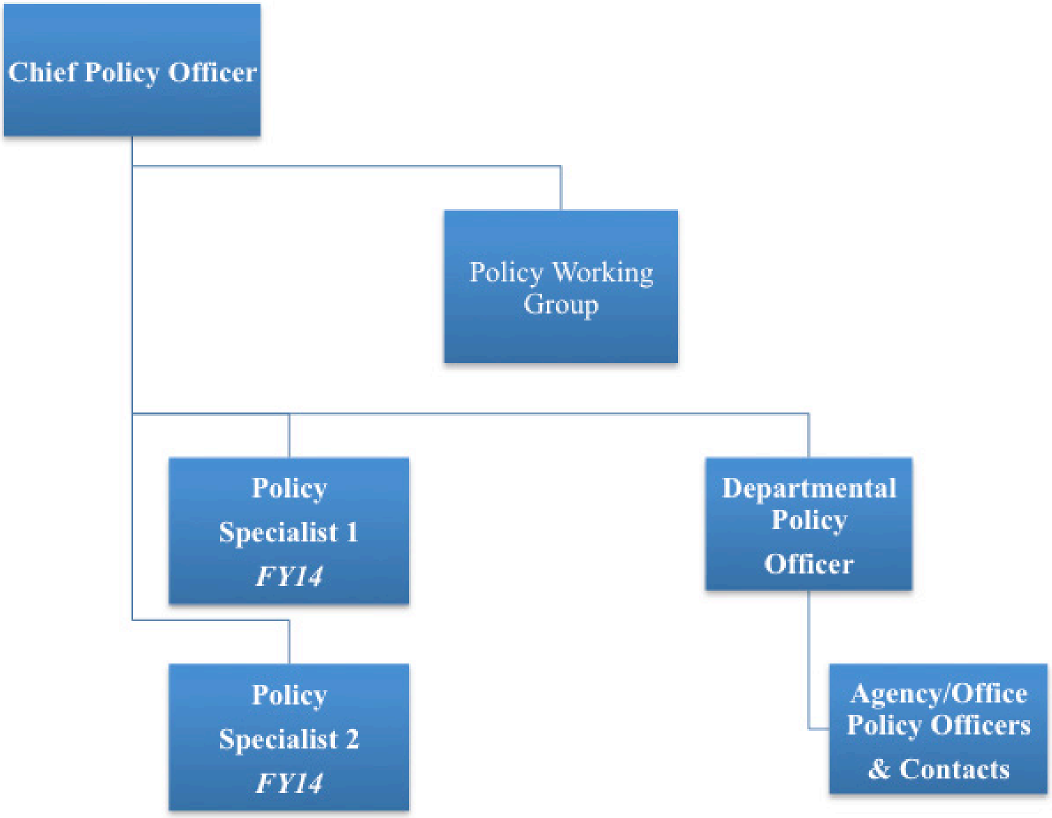
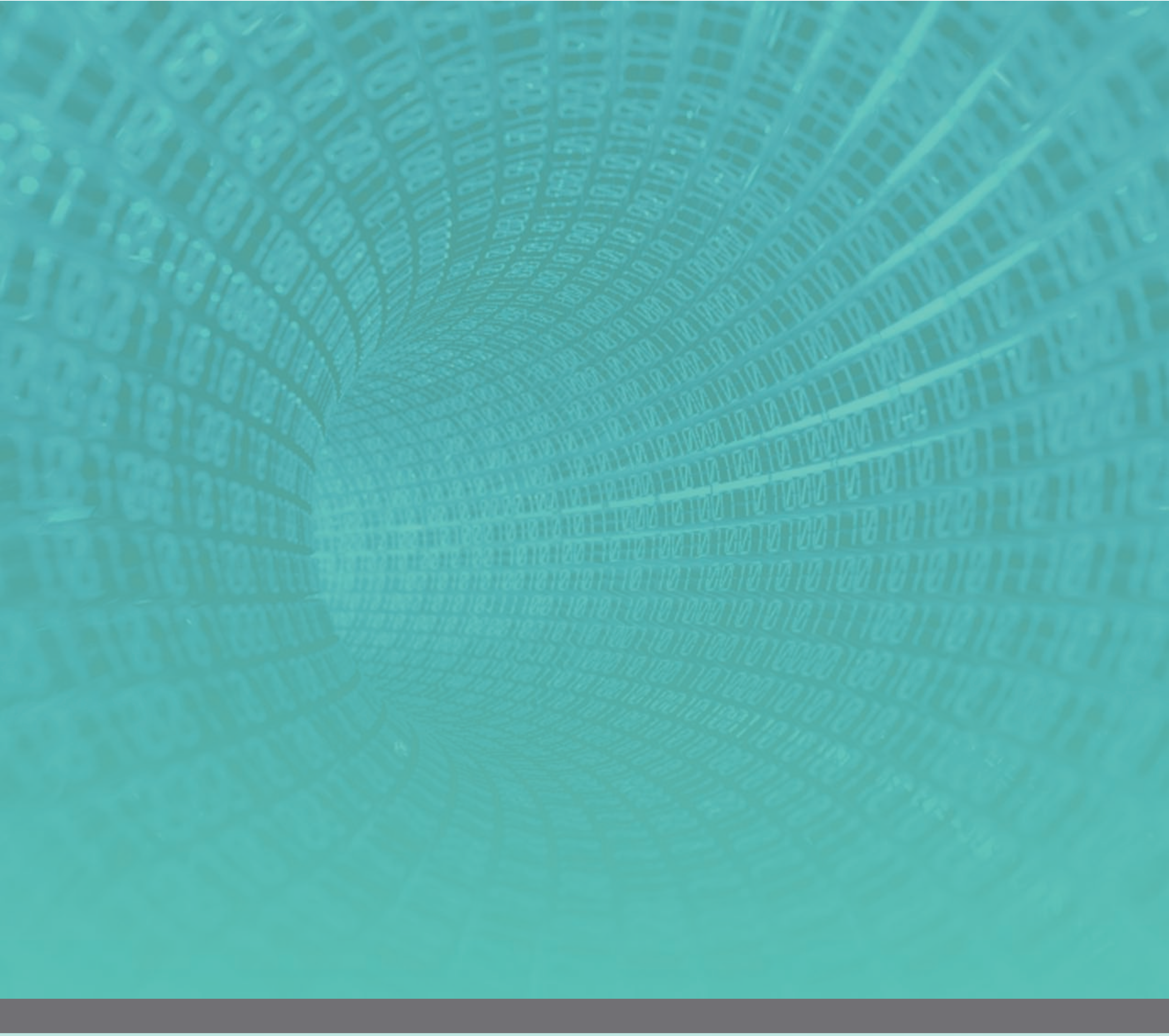


Figure 2: Policy Program Team Organization FY-2014



9. ROLES, RESPONSIBILITIES, AND STAFFING

9. ROLES, RESPONSIBILITIES, AND STAFFING

9.1 ROLES AND RESPONSIBILITIES

Table 5: Roles and Responsibilities

Role	Responsibilities
Sponsor(s): Senior Agency Official for Policy/Chief Information Office Assistant Secretaries, Agency/Office Heads and Budget Officers	• Commit to the scope of this Plan • Authorize program funding/resources required to successfully meet objectives of this Plan, including full compliance with State policy laws and policies • Be accountable for the success of agency/office compliance • Ensure acquisitions comply with State policy requirements • Actively participate in progress reviews to ensure critical program information is communicated to agency/office organizations • Facilitate resolution of program issues in agency/office organizations
OIMT Policy Officer–Program Manager/Team Leader	• Manage the day-to-day work of the program • Provide program oversight and monitoring of agency policy programs for compliance • Define and manage program risks • Lead, coordinate, and facilitate Program Team's planning and execution of tasks and deliverables • Accountable for the success of program/team tasks and deliverables • Ensure appropriately skilled program participants are available when needed • Prepare and present program reports to appropriate levels of management • Facilitate resolution of issues and elevated risks • Manage acquisitions • Chair the OIMT Policy Working Group
OIMT Policy Specialist	• Provide leadership, expert technical assistance and training for agency/office SMEs and Policy Officers • Attend all scheduled meetings • Assist OIMT Policy Officer in providing program oversight/monitoring of Agency/office policy programs for compliance • Actively participate in progress reviews to ensure critical program information is communicated to all agency/office organizations • Develop and maintain a website containing all policies • Develop communications plan to educate staff of policies and changes • Be accountable for the success/failure of OIMT program tasks and deliverables • Ensure appropriately skilled program participants are available when needed • Complete assigned tasks and deliverables based on agreed schedule.

Role	Responsibilities
	• Provide status updates including issues and risks • Communicate openly and assertively • Respect opinions of others • Agree to work toward consensus
Agency/Office Policy Officers–Team Leaders	• Participate in agency/office process to ensure compliance with applicable policy requirements. • Present program results to senior agency/office management and others • Be accountable for the success of agency/office compliance • Attend all scheduled meetings • Prepare and present agency/office reports to appropriate levels of management • Designate/train back-up personnel • Ensure appropriately skilled program participants are available when needed • Develop/issue agency/office-specific procedures for compliance, as appropriate • Provide technical assistance/training to agency/office personnel • Ensure all employees are aware of statutory/regulatory/policy responsibilities • Complete assigned tasks and deliverables based on agreed schedule • Act as SME for appropriate organizational function • Be prepared to take some responsibility to educate others • Communicate openly and assertively • Respect opinions of others • Agree to work toward consensus
OIMT Finance and Procurement Staff	• Oversee contracts • Manage task order solicitation • Administer contracts • Administer competitive procurements • Facilitate OIMT Policy Program Procurement staff processing of acquisitions
Internal Stakeholders: Program Team Agency/Office Policy Officers Agency/Office CIOs Sponsors All Other OIMT Employees	• Ensure compliance with policy laws, regulations, and policies • Report potential and actual breaches to appropriate officials • Take annual policy training • Provide feedback regarding OIMT implementation of policy laws, regulations and policies via audits, reports, Legislature inquiries, correspondence, appeals/litigation, etc.

9.2 PROGRAM STAFFING PLAN

OIMT is investing 1.5 Full-time Equivalents (FTEs) of effort by FY- 14 via employees and contractors to complete this program's tasks and deliverables. The breakdown by organization is as follows:

Table 6: Program Staffing Plan by OIMT Entity

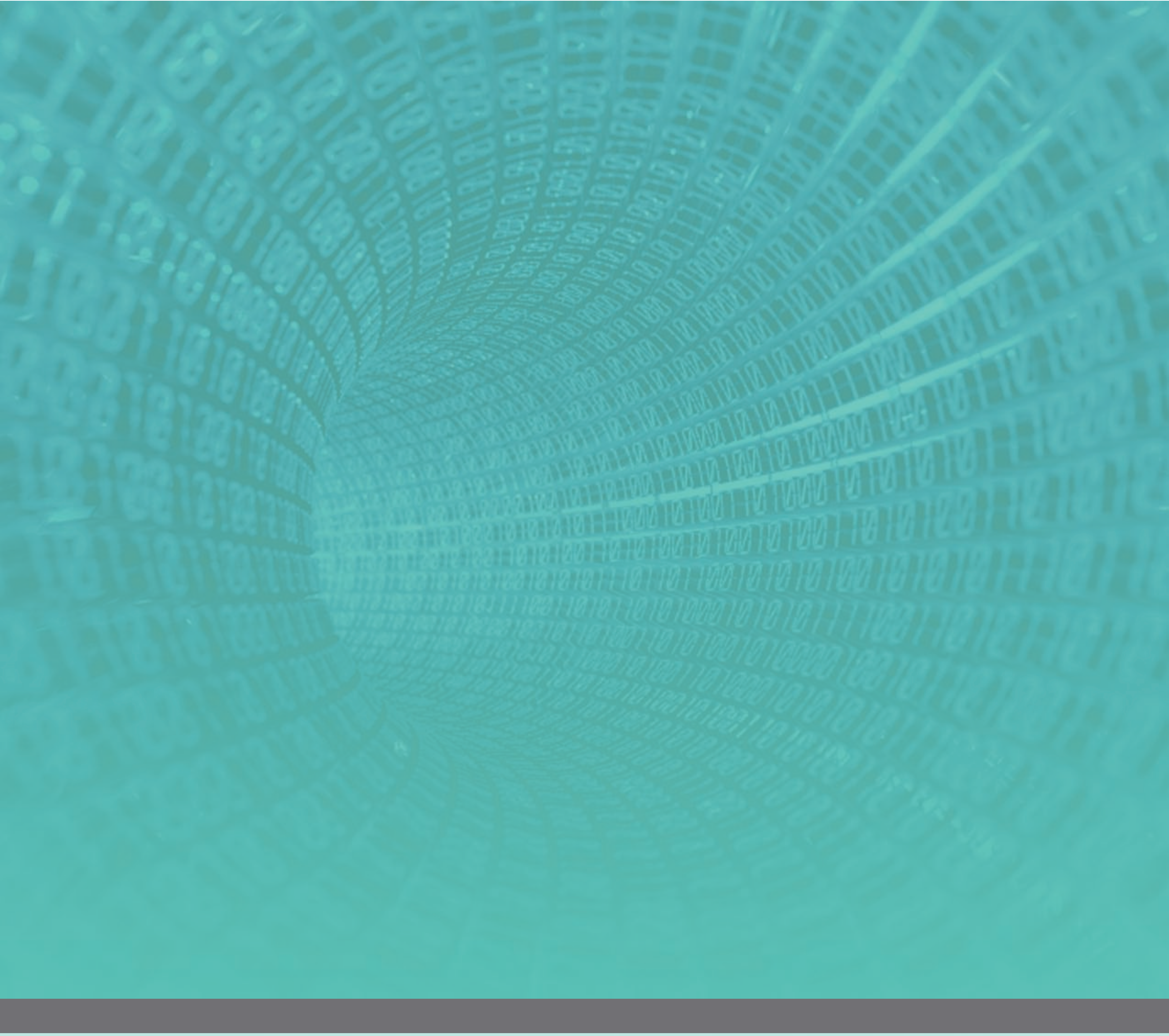
OIMT Entity	FTEs
Policy Officer	0.25
Other OIMT Staff	0.25
SMEs and OIMT WGs	1
Policy Specialist (second in FY-2014)	2
Program Total	3.5

Table 7 shows an estimated percentage of scheduled work hours need for the program to be successful.

Table 7: Minimum Program Staffing Plan

Resource Name or Role (if not staffed)	Minimum Needed for this Program (%)	OIMT Entity
EM05	0.25	Policy Officer
Other OIMT Staff assistance	0.25	
SR-24/26	2	Policy Specialist

Note that this does not take into account hours required within an agency or hours required for a successful Policy Working Group which the agencies participate in.



10. DELIVERABLES

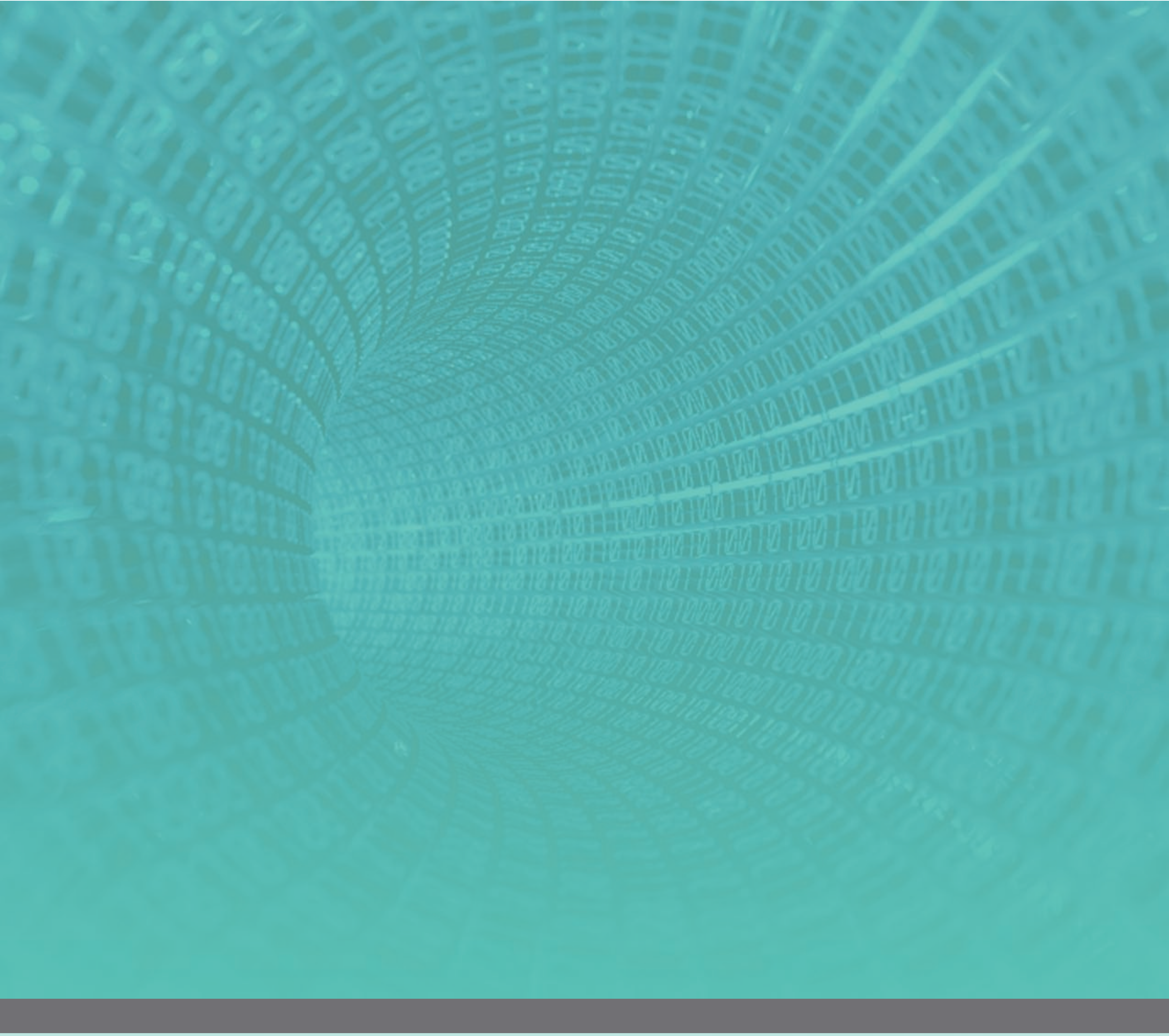
10. DELIVERABLES

10.1 PROGRAM DELIVERABLES

Verification methods include: analysis, inspection, demonstration, and testing requirements. Governance over policy implementation and verification will be overseen by the Governance team, and thus is not included in this document.

Table 8: Program Management Deliverables

Deliverable	Objective	Primary Audience	Reviewers	Approvers
Program Plan	Acquire resources required for full OIMT compliance with policy laws and State policies	All agencies and offices	OIMT Policy Officer, CIO, Policy WG	CIO, Budget Officers
Update OIMT Policy set (need requested FTE to complete)	Provide guidance needed to ensure OIMT compliance with policy laws and related State policies	All agencies and offices	OIMT Policy Officer, Policy WG	OIMT PO
OIMT Policy Policies and Procedures (in addition to Policy Manual and Handbook) (need requested FTE to complete)	Enable awareness of scheduled tasks	All agencies and offices	OIMT Policy Officer, Policy WG	OIMT PO
Role-based Trainings and Workshops (need requested FTE to complete)	Identify strengths, areas for improvement, and recommendations	All agencies and offices	OIMT Policy Officer, Policy WG	OIMT PO
Technical Evaluations (need requested FTE to complete)	Ensure compliance with policy requirements	All agencies and offices	OIMT Policy Officer, Policy WG	OIMT PO



11. PROGRAM CONTROLS

12. ASSOCIATED DOCUMENTS

13. WORKS CITED

14. REFERENCES

15. GLOSSARY OF ACRONYMS

11. PROGRAM CONTROLS

11.1 POLICY AND SECURITY

All program sensitive documents will be labeled **Sensitive But Unclassified - For Official Use Only** in the header and footer. All Certification and Accreditation (C&A) tasks and deliverables required before this program's solution can be implemented in production are part of this program.

12. ASSOCIATED DOCUMENTS

- State of Hawai`i Business Transformation Strategy and IT/IRM Strategic Plan, 2012 (referred to as the Plan)
- Baseline of Information Management and Technology and Comprehensive View of State Services (referred to as the Final Report) prepared by SAIC
- Internal Revenue Service Publication 1075
- National Institute of Standards Special Publications (800 Series)

13. WORKS CITED

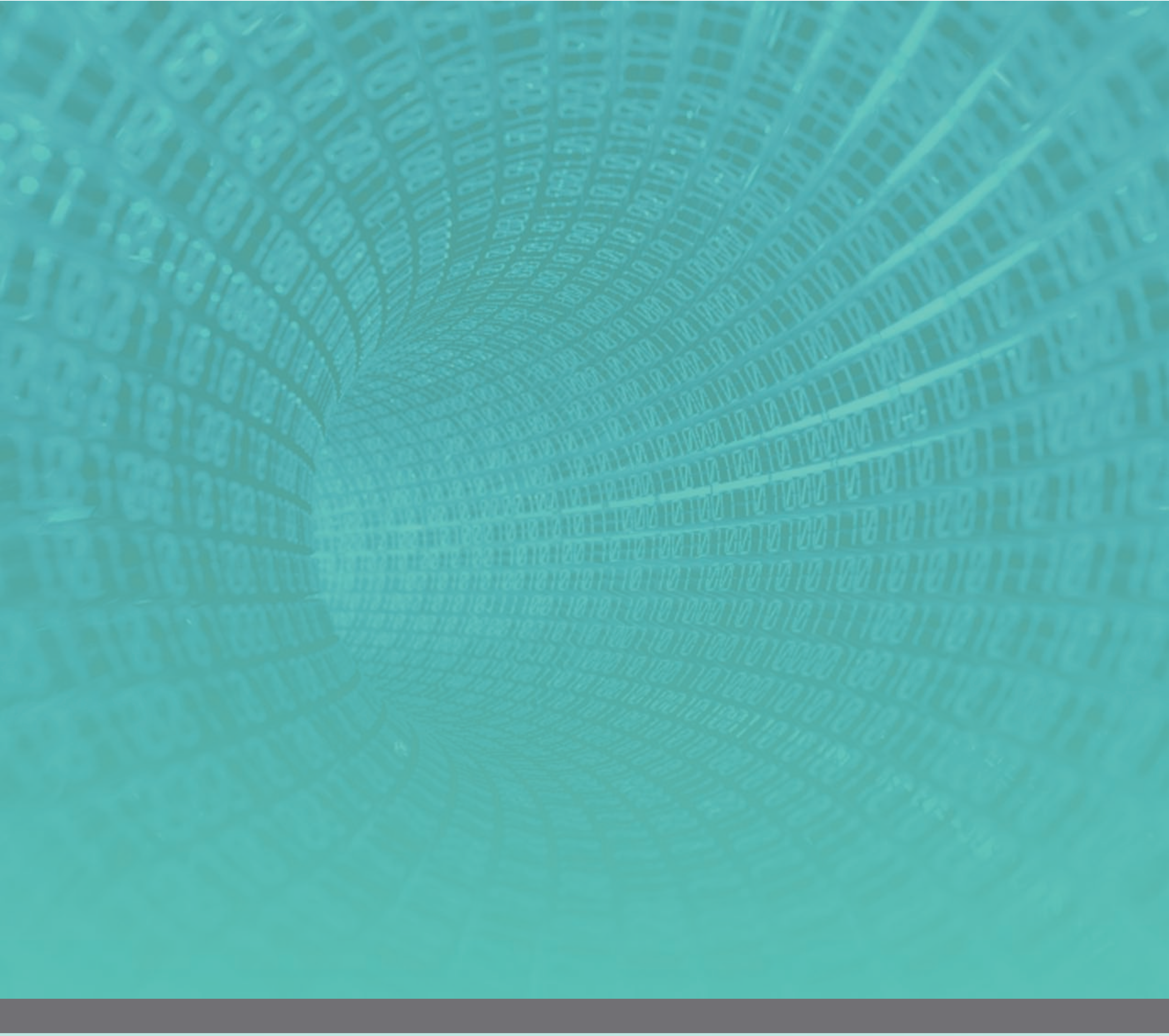
Gartner, Governance Processes to Support Effective Implementations of Policy. 2010.

14. REFERENCES

OIMT's Policy website is located at: http://oimt/higov.net

15. GLOSSARY OF ACRONYMS

For definitions of terms and acronyms used in this document, see the OIMT Nomenclature Guide.



APPENDIX A: CROSSWALK OF POLICIES

APPENDIX A: CROSSWALK OF POLICIES

The Tables that follow illustrate existing policies that were collected from State agencies and aligned into the new Policy Framework as devised by OIMT and the Policy Working Group. Policy will be developed for each on the coverage areas noted in the first column, incorporating existing Agency policy then aligning and incorporating established and proven Federal Policy or other best practices.

POLICY & PROCEDURE CROSSWALK

Key: ▨ Collateral exists 🟥 Good collateral example

P Procedure O Other type of collateral (e.g., best practice, guideline, etc.)

Policy	C-C Honolulu	CSEA	DCCA	DLNR	DOE	DOH	DHR	DOT	ICSD	HCJDC	DAGS	IPSC	Privacy	PSD	UH			
RECORDS MANAGEMENT																**Laws**	**Notes**	**Other State Collateral**
Records Management Policy			▨					▨ P	▨			▨				Act 137	DCCA's Office of Information Practice's Records Reporting System	
Records Management Retention Schedule				▨ O				▨ P			▨					487R	DAGS general record schedules (http://dlnri.higov.net/intranet/Documents/IT/Policies/GRS%202002%20-%20revised%205-06.pdf & http://dlnri.higov.net/intranet/Documents/IT/Policies/Comp%20Cir%202001-02.pdf)	
Digital/Paperless Environment																		
ACCESS																		
General		▨	▨	▨ O		▨			▨	▨	▨			▨			MFP_Security_FINAL.pdf	
Remote		▨	▨	▨ O					▨	▨	▨	▨		▨			HCJDC Remote Access Agreement	
Wireless		▨		▨ O	▨	▨			▨								Wireless LAN Security Policy (authorized use/security)	
Revoking Privileges After Termination		▨	▨	▨ O	▨				▨									
Consultant and Contractor Access																		
Policy for Interfacing with non State of Hawaii Entities (DOH)																		
Publicly Accessible Systems Policy																		Maryland
ACCEPTABLE USE																		
Acceptable Use		▨		▨ O	▨	▨	▨			▨				▨	▨		DHR Acknowledgement Form; ICSD Smartphone Agreement	Maryland (E Comm); New York
User-owned Device Mgmt			▨							▨								
Use of State Telephones																		Ohio
Loss of physical asset									▨									
SECURITY																		
General Security														▨			UH Sys Admin rules (good); HCJDC LAN Workstation and Server Policy; CJIS Security Policy; Maryland Agency Self-Evaluation Tool; DHS Cyber Security Evaluation Tool	
Security Incident Management		▨ P	▨			▨			▨			▨			▨	487N, Act 10	ICSD Incident Response Cklist	

POLICY & PROCEDURE CROSSWALK

Key:				
	▨	Collateral exists	🟥	Good collateral example
	P	Procedure	O	Other type of collateral (e.g., best practice, guideline, etc.)

Policy	C-C Honolulu	CSEA	DCCA	DLNR	DOE	DOH	DHR	DOT	ICSD	HCJDC	DAGS	IPSC	Privacy	PSD	UH			
Security Training and Awareness						▨											CSEA Policy on Employee Orientation	
Security Testing Policy									▨									
Password Policy and Guidance		▨	▨	▨ O	▨					▨					▨			Maryland
Physical Security	▨			▨ O		▨			▨									
Personal Identification Information (PII)		▨	▨					🟥 P	▨	▨	▨	▨ O	▨			Act 10, Acts 135 - 137, 139 of 2006, HRS 487N, 487J and 487R (7/1/07)	Best practice from IPSC; UH General Confidentiality Notice (agreement)	
Classification			▨			▨			▨						▨			Maryland (Standards for Security Categorization of Information Systems)
Screen Procedure						▨												
User-owned Device Mgmt			▨							▨								
Risk Assessment		▨ P				▨												
HIPAA		▨				▨												Connecticut
Certification and Accreditation		▨							▨									
Internet Privacy Policy																		New York
Digital Signature Policy																		New York
Virus Software Policy		▨	▨	▨ O		▨				▨								
Hard Drive Encryption Policy			▨									▨						
SOCIAL MEDIA																		
Social Media Policy				▨ O					▨								DAGS April 2009 Cyber Security Tips Newsletter (http://hawaii.gov/dags/icsd/cst/newsletters/2009/april_social_networking); SOH Social Networking Policy.pdf; New York Social Media Legal Guidance Toolkit; New York Social Media Tutorial	Maine; New York
EMAIL/INTERNET/MOBILE																		
Email Usage		▨		▨ O		▨ P			▨									

POLICY & PROCEDURE CROSSWALK

Key:	▨	Collateral exists	🟥	Good collateral example
	P	Procedure	O	Other type of collateral (e.g., best practice, guideline, etc.)

Policy	C-C Honolulu	CSEA	DCCA	DLNR	DOE	DOH	DHR	DOT	ICSD	HCJDC	DAGS	IPSC	Privacy	PSD	UH			
Wireless Email				▨ O					▨								Wireless policy (address rogue access points and endure agencies have deployed full wireless solutions which meet security req'ts and monitoring for unauthorized access)	
Web site Mgmt					▨				▨								EM 00-03; State Agency Website Common Template; need State Agency Website Deployment Policy (format, URL structure, domain names, advertisements/endorsements, etc.)	Connecticut; West Virginia
Wireless Communication					▨				▨									Maryland
Electronic Communications					▨				▨									Maryland
eCommerce Policy																		
Mobile Device Policy			🟥					▨			▨	▨				Act 10	HCJDC Mobile Device Use Agreement; ICSD Smartphone Agreement	Maryland
Interfacing with non State Entities						▨												
Instant Messaging																		
SOFTWARE/HARDWARE																		
Development									▨									
Application Development									▨								ICSD System Requirements for Computer Application Systems; ICSD Standard Systems Development Methodology (SSDM)	
Database Development									▨								ICSD Database/Data Dictionary Overview (includes System Development Checklist for DB tasks)	
Change Management						▨			▨									
Tivoli									▨									
VM									▨								Cloud/Virtualization Policy	
Configuration Management		▨				▨												
Software Maintenance		▨	▨	▨ O					▨	▨								California 4846 (legally procured & used in compliance with licenses, copyright laws, etc., inventory, etc.)
OS									▨									
Power Management Policy				▨ O														California 4819.31.13

POLICY & PROCEDURE CROSSWALK

Key: ▨ Collateral exists 🟥 Good collateral example

P Procedure O Other type of collateral (e.g., best practice, guideline, etc.)

Policy	C-C Honolulu	CSEA	DCCA	DLNR	DOE	DOH	DHR	DOT	ICSD	HCJDC	DAGS	IPSC	Privacy	PSD	UH			
Hardware						▨			▨	▨								
Network									▨								ICSD 8.04 Network Security	
Monitoring									▨									
OUTAGE MANAGEMENT																		
Outage									▨								Centralized Support Priority Support Policy (DLIR)	
PROPERTY CONTROL																		
State IT Property Control				▨ O		▨												Connecticut
Inventory Policy			▨								▨						DLIR uses a $600 inventory tool	
Disposal of IT Equipment		▨	▨	▨ O		▨	▨			▨		▨			▨			Ohio
CBA/ROI/Feasibility Planning																		California 4819.35
Cost Threshold																		California 4819.39
IT Equipment Depreciation																		
System Inventory and Modernization																		
POLICY DEVELOPMENT																		
Procedure and Process for Creating, Reviewing and Approving IT Policies, Procedures, and Guidelines			▨						▨		▨						Guidelines for Writing Standards (http://hawaii.gov/dags/icsd/standards/pdf_standards/ITS_0101.pdf); DAGS Policy Exception Request Form	
Exception Management						▨												
Definitions						▨												California 4819.2
PROJECT MANAGEMENT																	-	
Project Management Policy																		Connecticut
PROCUREMENT																		
IT Procurement (including Technology Review)			▨						▨		▨						Executive Memorandum 94-08 8/31/94; B&F Memo 10/18/94; CS Circular 90-1 9/14/90; ICSD T-205 Approval Process; EM 08-05; AD 87.1; CM 2011-14 & 2011-05	New York
Service Contract Information Technology (SCIT) Certification Policy																		California 4819.31
DISASTER RECOVERY																		
Disaster Recovery Planning Policy		▨		▨ O														California 4819.31

POLICY & PROCEDURE CROSSWALK

Key: ▨ Collateral exists 🟥 Good collateral example

P Procedure O Other type of collateral (e.g., best practice, guideline, etc.)

Policy	C-C Honolulu	CSEA	DCCA	DLNR	DOE	DOH	DHR	DOT	ICSD	HCJDC	DAGS	IPSC	Privacy	PSD	UH			
IT Business Continuity Planning Guideline																		
STORAGE/BACKUP																		
Storage/Backup Policy				▨ O	▨				▨	▨					▨			
TELECOMMUTING																		
Telecommuting Policy							🟥										DHR MOU	
STRATEGIC PLAN																		
Agency Strategic Plan																		California 4900.2
Information Management Strategic Planning Process																		California 4819.31
IT Capital/Portfolio Planning																		California 4819.31/4904
IT Performance Management																		
IT Project Oversight Framework (including reporting and project criticality classification)																		California 4819.31.10/4800
OTHER																		
Data Entry Policy									▨									

* Include social media, email, etc. (See Maryland's.)

BUSINESS AND IT/IRM

GLOSSARY, ACRONYMS & REFERENCE GUIDE

TABLE OF CONTENTS

1. FORWARD 3

2. GLOSSARY 4

0 - 9 4

A 4

B 6

C 7

D 11

E 13

F 14

G 15

H 16

I 17

J 20

K 20

L 20

M 21

N 22

O 23

P 23

Q 26

R 26

S 29

T 34

U 36

V 36

W 37

X, Y 38

Z 38

3. STATE OF HAWAIʻI EXECUTIVE BRANCH DEPARTMENTS, DIVISIONS, BRANCHES, OFFICES, BOARDS, COMMISSIONS & COUNCILS 39

4. CIO COUNCIL ADVISORY WORKING GROUPS 40

5. COMMONLY USED TECHNICAL ABBREVIATIONS AND ACRONYMS 41

NOTES 44

REFERENCES 48

1. FORWARD

The Office of Information Management and Technology (OIMT) implemented State of Hawaiʻi Business and Information Technology (IT) and Information Resource Management (IRM) Glossary, Acronyms, and Reference Guide, dated July 2012, as a standalone document for assisting in development of documentation related to IT/IRM and business processes.

This guide is intended to be a companion document in collaboration with the Office of Information Management & Technology Business IT/IRM Transformation Plan to restructure the business processes and information technologies serving the employees and citizens of the State of Hawaiʻi.

Most of the terms in this document are derived from various federal, state, local, educational and private sector sources, but a number of them have been examined for consistency in order to remove inconsistencies among the departments and the State IT & business community.

This glossary, acronyms and reference document is intended to fulfill several overall objectives:

- Resolve differences between the definitions of terms used by the State, Local, Federal to enable all departments to use the same source of information (and move towards shared documentation and processes).
- Accommodate the transition from multiple information technology organizations to a single statewide information technology organization in current use to the terms now appearing in documents produced by the State IT Transformation initiative.
- Ensure consistency among related and dependent terms.
- Identify terms and acronyms which have multiple meanings depending on the situation or document(s) where the term or acronym appears
- Include terms that are important to the support of goals of State Departments and to the concept of information sharing.
- Review existing definitions to reflect, as appropriate a broader enterprise perspective vice a system perspective.
- Strike an appropriate balance between macro terms and micro terms (i.e., include terms that are useful in writing and understanding documents dealing with business or IT/IRM policies, directives, instructions, and guidance, and strike terms that are useful only to specific business or IT/IRM subspecialties).

Many technology and business terms come and go into vogue and OIMT has attempted to include significant examples that have a useful distinction when compared to existing Information Assurance terms. A number of terms recommended for inclusion in the glossary were not added – often because they appeared to have a narrow application.

When glossary terms have common acronyms, they have been noted the acronym with the term and added the acronym to the acronym list. In some instances, there may be several meanings for the same acronym, and in those cases OIMT has tried to list all the common meanings. Note that some acronyms are self-explanatory, and so there is no definition of these acronyms in the glossary itself.

OIMT is creating this document has attempted to include as many information technology and information assurance definitions, many other terms have been overlooked for a specific reasons or were simply overlooked, or not relevant, and some terms are newly identified, If there is a term or definition that is either not included in this glossary or should be identified as a Candidate For Deletion (C.F.D.) in future versions of this document, please submit the term with a definition based on the following criteria: 1) specific relevance to Information Assurance; 2) economy of words; 3) accuracy; 4) broad applicability; and 5) clarity. Use these same criteria to recommend any changes to existing definitions or to suggest new terms (definitions must be included with any new terms). When recommending a change to an existing definition, please note how that change might affect other terms. In all cases, send your suggestions to the State of Hawaiʻi Office of Information Management & Technology via e-mail address listed below.

OIMT recognizes that, to remain useful, a glossary must be in a continuous state of coordination, and encourages reviews and welcome comments as new terms become significant and old terms fall into disuse or change meaning. The goal of OIMT is to keep this document relevant and a useful tool for commonality among the State's IT community.

State of Hawaiʻi
Office of Information Management and Technology

RE: Business and IT/IRM – Glossary, Acronyms &
Reference Guide

mailto: oimt@hawaii.gov

2. GLOSSARY

This instruction applies to all State of Hawai'i Executive Branch Departments, Agencies, Divisions, Bureaus and Offices; supporting contractors and agents; that collect, generate process, store, display, transmit or receive state sensitive information or that operate, use, or connect to the State managed Network or information technology systems, as defined herein. Private industry, educational institutions, citizens, etc. can use the terms and acronyms herein as a guideline when dealing with the State's IT/IRM infrastructure or reference documentation.

0 – 9

3rd Generation (3G) – used to represent the 3rd generation of mobile telecommunications technology. This is a set of standards used for mobile devices and mobile telecommunication services and networks that comply with the International Mobile Telecommunications-2000 (IMT-2000) specifications by the International Telecommunication Union.[1] 3G finds application in wireless voice telephony, mobile Internet access, Fixed Wireless Internet access, video calls and mobile TV.

4th Generation (4G) – 4G is the fourth generation of cell phone mobile communications standards. It is a successor of the third generation (3G) standards. A 4G system provides mobile ultra-broadband Internet access, for example to laptops with USB wireless modems, to smartphones, and to other mobile devices. Conceivable applications include amended mobile web access, IP telephony, gaming services, high-definition mobile TV, video conferencing and 3D television.

6 Sigma (6σ) – A widely used business management strategy, originally developed by Motorola during the 1980s, made popular by Jack Welch at General Electric during the 1990s. 6 Sigma attempts to improve the quality of the outputs of a process by identifying and removing the causes of errors and minimizing the variability in manufacturing and business processes. (See also Lean Six Sigma.)

A

access – Opportunity to make use of an information system (IS) resource.

access control – Limiting access to information system resources only to authorized users, programs, processes, or other systems.

Access Control List (ACL) – 1. A list of permissions associated with an object. The list specifies who or what is allowed to access the object and what operations are allowed to be performed on the object.
2. A mechanism that implements access control for a system resource by enumerating the system entities that are permitted to access the resource and stating, either implicitly or explicitly, the access modes granted to each entity.

access list – Roster of individuals authorized admittance to a controlled area.

accountability – Principle that an individual is entrusted to safeguard and control equipment, keying material, and information and is answerable to proper authority for the loss or misuse of that equipment or information.

accreditation - Formal declaration by State Authorized Accrediting Authority (SAAA) that an information system is approved to operate at an acceptable level of risk, based on the implementation of an approved set of technical, managerial, and procedural safeguards.

[1] *Clint Smith, Daniel Collins. "3G Wireless Networks", page 136. 2000.*

Accrediting Authority – Synonymous with Designated Accrediting Authority (DAA). See also Authorizing Official.

accreditation package – Product comprised of a System Security Plan (SSP) and a report documenting the basis for the accreditation decision.

Active Directory (AD) – A directory service created by Microsoft for Windows domain networks. It is included in most Windows Server operating systems.

Active Directory provides a central location for network administration and security. Server computers that run Active Directory are called domain controllers. An AD domain controller authenticates and authorizes all users and computers in a Windows domain type network—assigning and enforcing security policies for all computers and installing or updating software. For example, when a user logs into a computer that is part of a Windows domain, Active Directory checks the submitted password and determines whether the user is a system administrator or normal user.[2]

Advanced Encryption Standard (AES) – A U.S. Government-approved cryptographic algorithm that can be used to protect electronic data. The AES algorithm is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information.

Advanced Persistent Threat (APT) – Refers to a group, such as a foreign government, with both the capability and the intent to persistently and effectively target a specific entity. The term is commonly used to refer to cyber threats, in particular that of Internet-enabled espionage using a variety of intelligence gathering techniques to access sensitive information[3], but applies equally to other threats such as that of traditional espionage or attack.[4] Other recognized attack vectors include infected media, supply chain compromise, and social engineering. Individuals, such as an individual hacker, are not usually referred to as an APT as they rarely have the resources to be both advanced and persistent even if they are intent on gaining access to, or attacking, a specific target.[5]

advisory – Notification of significant new trends or developments regarding the threat to the information systems of an organization. This notification may include analytical insights into trends, intentions, technologies, or tactics of an adversary targeting information systems.

Agile – Refers to software development as a group methods based on iterative and incremental development, where requirements and solutions evolve through collaboration between self-organizing, cross-functional teams. It promotes adaptive planning, evolutionary development and delivery, a time-boxed iterative approach, and encourages rapid and flexible response to change. It is a conceptual framework that promotes foreseen interactions throughout the development cycle. The Agile Manifesto[6] introduced the term in 2001.

air-gapped system – Two or more computer systems that are physically, electrically, and electromagnetically isolated from one another, in order to create a more secure set of systems.

applet – Any small application that performs one specific task within the scope of a larger program, often as a plug-in.

application – Software program that performs a specific function directly for a user and can be executed without access to system control, monitoring, or administrative privileges.

[2] *"Active Directory on a Windows Server 2003 Network". Active Directory Collection. Microsoft. 13 March 2003. http://technet.microsoft.com/en-us/library/cc780036(WS.10).aspx#w2k3tr_ad_over_qbjd. Retrieved 20 July 2012.*

[3] *"Anatomy of an Advanced Persistent Threat (ATP)". Dell SecureWorks. http://go.secureworks.com/advancedthreats. Retrieved 21 July 2012.*

[4] *"Are you being targeted by an Advanced Persistent Threat?". Command Five Pty Ltd. http://www.commandfive.com/apt.html. Retrieved 21 July 2012.*

[5] *"The changing threat environment…". Command Five Pty Ltd. http://www.commandfive.com/threats.html. Retrieved 21 July 2012.*

Approval to Operate (ATO) – The official management decision issued by a SAAA to authorize operation of an information system and to explicitly accept the residual risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals.

anti forensics –

asset – A major application, general support system, high impact program, physical plant, mission critical system, personnel, equipment, or a logically related group of systems. (see also – investment, portfolio)

assurance – Measure of confidence that the security features, practices, procedures, and architecture of an information system accurately mediates and enforces the security policy.

attack – Any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself.

audit – Independent review and examination of records and activities to assess the adequacy of system controls and ensure compliance with established policies and operational procedures.

audit log – A chronological record of system activities. Includes records of system accesses and operations performed in a given period.

audit reduction tools – Preprocessors designed to reduce the volume of audit records to facilitate manual review. Before a security review, these tools can remove many audit records known to have little security significance. These tools generally remove records generated by specified classes of events, such as records generated by nightly backups.

audit trail – A chronological record that reconstructs and examines the sequence of activities surrounding or leading to a specific operation, procedure, or event in a security relevant transaction from inception to final result.

authenticate – To verify the identity of a user, user device, or other entity.

authentication – The process of verifying the identity or other attributes claimed by or assumed of an entity (user, process, or device), or to verify the source and integrity of data. Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.

authenticator – The means used to confirm the identity of a user, process, or device (e.g., user password or token).

uthenticity – The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator.
See Authentication.

authorization – Access privileges granted to a user, program, or process or the act of granting those privileges.

availability – The property of being accessible and useable upon demand by an authorized entity. Ensuring timely and reliable access to and use of information.

Average Rate of Occurrence (ARO) – The annualized rate at which a particular event or incident occurs. Used in qualitative risk management, in order to develop a risk assessment.

B

back door – Typically unauthorized hidden software or hardware mechanism used to circumvent security controls.

backup – Copy of files and programs made to facilitate recovery, if necessary.

banner – Display on an information system that sets parameters for system or data use.

baseline – Hardware, software, databases, and relevant documentation for an information system at a given point in time.

biometrics – Measurable physical characteristics or personal behavioral traits used to identify, or verify the claimed identity, of an individual. Facial images, fingerprints, and handwriting samples are all examples of biometrics.

blended attack – A hostile action to spread malicious code via multiple methods.

bot – Modified term for "robot", is a compromised computer system on the Internet which is being used as part of an overall 'botnet' to perform attacks against other Internet resources, but hides the identity of the actual attacker.

botnet – A botnet is a collection of compromised computers connected to the Internet (each compromised computer is known as a 'bot'). When a computer is compromised by an attacker, there is often code within the malware that commands it to become part of a botnet.

boundary – Physical or logical perimeter of a system.

boundary protection – Monitoring and control of communications at the external boundary of an information system to prevent and detect malicious and other unauthorized communications, through the use of boundary protection devices (e.g., proxies, gateways, routers, firewalls, guards, encrypted tunnels).

breach – A breach is an incident in which sensitive, protected or confidential data has potentially been viewed, stolen or used by an individual unauthorized to do so. Data breaches may involve personal health information (PHI), personally identifiable information (PII), trade secrets or intellectual property.

buffer overflow – A condition at an interface under which more input can be placed into a buffer or data holding area than the capacity allocated, overwriting other information. Attackers exploit such a condition to crash a system or to insert specially crafted code that allows them to gain control of the system.

Business Continuity Plan (BCP) – The documentation of a predetermined set of instructions or procedures that describe how an organization's business functions will be sustained during and after a significant disruption.

Business Impact Analysis (BIA) – The documentation of a predetermined set of instructions or procedures that describe how an organization's business functions will be sustained during and after a significant disruption.

Business Process Reengineering (BPR) – A business management strategy originally pioneered in the early 1990s, focusing on the analysis and design of workflows and processes within an organization. BPR aimed to help organizations fundamentally rethink how they do their work in order to dramatically improve customer service, cut operational costs, and become world-class competitors. In the mid-1990s, as many as 60% of the Fortune 500 companies claimed to either have initiated reengineering efforts, or to have plans to do so.

C

Certificate – A digitally signed representation of information that

1) identifies the authority issuing it
2) identifies the subscriber
3) Identifies its valid operational period (date issued / expiration date).

community certificate usually implies public key certificate and can have the following types:

1) cross certificate; 2) encryption certificate; & 3) identity certificate

Certificate management – Process whereby certificates (as defined above) are generated, stored, protected, transferred, loaded, used, and destroyed.

Certificate Policy (CP) – A specialized form of administrative policy tuned to electronic transactions performed during certificate management. A Certificate Policy addresses all aspects associated with the generation, production, distribution, accounting, compromise recovery, and administration of digital certificates. Indirectly, a certificate policy can also govern the transactions conducted using a communications system protected by a certificate-based security system. By controlling critical certificate extensions, such policies and associated enforcement technology can support provision of the security services required by particular applications.

Certificate Revocation List (CRL) – A list of revoked public key certificates created and digitally signed by a Certification Authority.

Certificate Status Authority (CSA) – A trusted entity that provides on-line verification to a relying party of a subject certificate's trustworthiness, and may also provide additional attribute information for the subject certificate.

chain of custody – A process that tracks the movement of evidence through its collection, safeguarding, and analysis lifecycle by documenting each person who handled the evidence, the date/time it was collected or transferred, and the purpose for the transfer.

chain of evidence – A process and record that shows who obtained the evidence; where and when the evidence was obtained; who secured the evidence; and who had control or possession of the evidence. The "sequencing" of the chain of evidence follows this order: collection and identification; analysis; storage; preservation; presentation in court; return to owner.

ciphertext – Is the result of encryption performed on plaintext using an algorithm, called a cipher. Ciphertext is also known as encrypted or encoded information because it contains a form of the original plaintext that is unreadable by a human or computer without the proper cipher to decrypt it.

clearing – The removal of sensitive data from storage devices in such a way that there is assurance that the data may not be reconstructed using normal system functions or software file/data recovery utilities. The data may still be recoverable, but not without special laboratory techniques.

Clearing is typically an administrative protection against accidental disclosure within an organization. For example, before a hard drive is re-used within an organization, its contents may be cleared to prevent their accidental disclosure to the next user.

cloud computing – A model for enabling on-demand network access to a shared pool of configurable IT capabilities/ resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. It allows users to access technology-based services from the network cloud without knowledge of, expertise with, or control over the technology infrastructure that supports them. This cloud model is composed of five essential characteristics (on-demand self-service, ubiquitous network access, location independent resource pooling, rapid elasticity, and measured service); three service delivery models (Cloud Software as a Service (SaaS), Cloud Platform as a Service (PaaS), and Cloud Infrastructure as a Service (IaaS)); and four models for enterprise access (Private cloud, Community cloud, Public cloud and Hybrid cloud).
Note: Both the user's data and essential security services may reside in and be managed within the network cloud.

coeverity – The level of magnetic field used to read/write data to a data storage device.

cold site – Backup site that can be up and operational in a relatively short time span, such as a day or two. Provision of services, such as telephone lines and power, is taken care of, and the basic office furniture might be in place, but there is unlikely to be any computer equipment, even though the building might well have a network infrastructure and a room ready to act as a server room. In most cases, cold sites provide the physical location and basic services.

Common Vulnerabilities and Exposures (CVE) – A dictionary of common names for publicly known information system vulnerabilities.

compensating security control – A management, operational, and/or technical control (i.e., safeguard or countermeasure) employed by an organization in lieu of a recommended security control in the low, moderate, or high baselines that provides equivalent or comparable protection for an information system.

compromise – Disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred.

computer cryptography – Use of a crypto-algorithm program by a computer to authenticate or encrypt/decrypt information.

Computer Forensics – The practice of gathering, retaining, and analyzing computer-related data for investigative purposes in a manner that maintains the integrity of the data.

Computer Network Attack (CNA) – Actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves.

Computer Network Defense (CND) – Actions taken to defend against unauthorized activity within computer networks. CND includes monitoring, detection, analysis (such as trend and pattern analysis), and response and restoration activities.

Computer Network Exploitation (CNE) – Enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary information systems or networks.

Computer Security – Measures and controls that ensure confidentiality, integrity, and availability of information system assets including hardware, software, firmware, and information being processed, stored, and communicated.

computer security incident – See Incident.

Computer Security Incident Response Team (CSIRT) – Group of individuals usually consisting of Security Analysts organized to develop, recommend, and coordinate immediate mitigation actions for containment, eradication, and recovery resulting from computer security incidents. Also called a Computer Security Incident Response Team (CSIRT) or a CIRC (Computer Incident Response Center, Computer Incident Response Capability or Cyber Incident Response Team).

computer security object – A resource, tool, or mechanism used to maintain a condition of security in a computerized environment. These objects are defined in terms of attributes they possess, operations they perform or are performed on them, and their relationship with other objects.

computer security subsystem – Hardware/software designed to provide computer security features in a larger system environment.

computing environment – Workstation or server (host) and its operating system, peripherals, and applications.

confidentiality – The property that information is not disclosed to system entities (users, processes, devices) unless they have been authorized to access the information.

configuration control – Process of controlling modifications to hardware, firmware, software, and documentation to protect the information system against improper modifications prior to, during, and after system implementation.

Configuration Control Board (CCB) – A group of qualified people with responsibility for the process of regulating and approving changes to hardware, firmware, software, and documentation throughout the development and operational lifecycle of an information system.

contingency plan – Management policy and procedures used to guide an enterprise response to a perceived loss of mission capability. The Contingency Plan is the first plan used by the enterprise risk managers to determine what happened, why, and what to do. It may point to the COOP or Disaster Recovery Plan for major disruptions.

Continuity of Government (COG) – A coordinated effort within the Federal Government's executive branch to ensure that national essential functions continue to be performed during a catastrophic emergency.

Continuity of Operations Plan (COOP) – Management policy and procedures used to guide an enterprise response to a major loss of enterprise capability or damage to its facilities. The COOP is the third plan needed by the enterprise risk managers and is used when the enterprise must recover (often at an alternate site) for a specified period of time. Defines the activities of individual departments and agencies and their sub-components to ensure that their essential functions are performed. This includes plans and procedures that delineate essential functions; specifies succession to office and the emergency delegation of authority; provide for the safekeeping of vital records and databases; identify alternate operating facilities; provide for interoperable communications, and validate the capability through tests, training, and exercises. See also Disaster Recovery Plan and Contingency Plan.

continuous monitoring – The process implemented to maintain a current security status for one or more information systems or for the entire suite of information systems on which the operational mission of the enterprise depends. The process includes: 1) The development of a strategy to regularly evaluate selected IA controls/metrics, 2) Recording and evaluating IA relevant events and the effectiveness of the enterprise in dealing with those events, 3) Recording changes to IA controls, or changes that affect IA risks, and 4) Publishing the current security status to enable information sharing decisions involving the enterprise.

controlled access area – Physical area (e.g., building, room, etc.) to which only authorized personnel are granted unrestricted access. All other personnel are either escorted by authorized personnel or are under continuous surveillance.

controlled interface – A boundary with a set of mechanisms that enforces the security policies and controls the flow of information between interconnected information systems.

cookie – Data exchanged between an HTTP server and a browser (a client of the server) to store state information on the client side and retrieve it later for server use.

countermeasure – Actions, devices, procedures, or techniques that meet or oppose(i.e., counters) a threat, a vulnerability, or an attack by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that corrective action can be taken.

covert channel – An unauthorized communication path that manipulates a communications medium in an unexpected, unconventional or unforeseen way in order to transmit information without detection by anyone other than the entities operating the covert channel.

credential – Evidence or testimonials that support a claim of identity or assertion of an attribute and usually are intended to be used more than once.

critical infrastructure – System and assets, whether physical or virtual, so vital to the U.S. that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.

cross-certificate – A certificate used to establish a trust relationship between two Certification Authorities.

cracker – Cracking is the act of breaking into a computer system, often on a network. A cracker can be doing this for profit, maliciously, for some altruistic purpose or cause, or because the challenge is there. Some breaking-and-entering has been done ostensibly to point out weaknesses in a site's security system. See hacker.

cross certificate – A certificate issued from a CA that signs the public key of another CA not within its trust hierarchy that establishes a trust relationship between the two Cas.

cryptography – Art or science concerning the principles means, and methods for rendering plain information unintelligible and for restoring encrypted information to intelligible form.

cryptology – The mathematical science that deals with cryptanalysis and cryptography.

cyber attack – An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information.

cyber cartel – A criminal organization developed with the primary purpose of promoting, controlling and profiting from the exploitation of individuals and computer systems on the Internet.

Cybersecurity – The ability to protect or defend the use of cyberspace from cyber-attacks.

cyberspace – A global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.

D

data – A subset of information in an electronic format that allows it to be retrieved or transmitted.

data asset –
1. Any entity that is comprised of data. For example, a database is a data asset that is comprised of data records. A data asset may be a system or application output file, database, document, or web page. A data asset also includes a service that may be provided to access data from an application. For example, a service that returns individual records from a database would be a data asset. Similarly, a web site that returns data in response to specific queries (e.g., www.weather.com) would be a data asset.
2. An information-based resource.

data integrity – The property that data has not been changed, destroyed, or lost in an unauthorized or accidental manner.

Data At Rest (DAR) – The term used to describe all data in storage but excludes any data that frequently traverses the network or that which resides in temporary memory. Data at rest includes but is not limited to archived data, data which is not accessed or changed frequently, files stored on hard drives, USB thumb drives, files stored on backup tape and disks, and also files stored off-site or on a storage area network (SAN).

Data In Motion (DIM) – Is data being transferred between two nodes in a network. This data can be regarded as secure if and only if (a) both hosts are capable of protecting the data in the previous two classifications and (b) the communication between the two hosts is identified, authenticated, authorized, and private, meaning no third host can eavesdrop on the communication between the two hosts.

Data In Use (DIU) – Is data not in an at rest state, that is on only one particular node in a network (for example, in resident memory, or swap, or processor cache or disk cache, etc. memory). This data can be regarded as "secure" if and only if (a) access to the memory is rigorously controlled (the process that accessed the data off of the storage media and read the data into memory is the only process that has access to the memory, and no other process can either access the data in memory, or man-in-the-middle the data while it passes through I/O), and (b) regardless of how the process terminates (either by successful completion, or killing of the process, or shutdown of the computer), the data cannot be retrieved from any location other than the original at rest state, requiring re-authorization.

data loss – Data loss is an error condition in information systems in which information is destroyed by failures or neglect in storage, transmission, or processing. Information systems implement backup and disaster recovery equipment and processes to prevent data loss or restore lost data.

Data Loss Prevention (DLP) – Refers to systems that identify, monitor, and protect data in use (e.g. endpoint actions), data in motion (e.g. network actions), and data at rest (e.g. data storage) through deep content inspection, contextual security analysis of transaction (attributes of originator, data object, medium, timing, recipient/destination and so on) and with a centralized management framework. Systems are designed to detect and prevent unauthorized use and transmission of confidential information.
(See also data in use, data in motion and data at rest.)

Data owner – The head of the organization that has final statutory and operational authority for specified information. (In the government community, the Data Owner is usually the department head who establishes the controls used for the collection, processing, and dissemination of specified information.)

decrypt – Generic term encompassing decodes and decipher.

Defense-in-Breadth – A planned, systematic set of multi-disciplinary activities that seek to identify, manage, and reduce risk of exploitable vulnerabilities at every stage of the system, network, or sub-component lifecycle (system, network, or product design and development; manufacturing; packaging; assembly; system integration; distribution; operations; maintenance; and retirement).

Defense-in-Depth – Information Security strategy integrating people, technology, and operations capabilities to establish variable barriers across multiple layers and missions of the organization.

degauss – Procedure to reduce the magnetic field on a data storage device (E.g. hard disk drive) to virtual zero by applying a reverse magnetizing field.
Also called demagnetizing.

deleted file – A file that has been logically, but not necessarily physically, erased from the operating system, perhaps to eliminate potentially incriminating evidence. Deleting files does not always necessarily eliminate the possibility of recovering all or part of the original data.

Demilitarized Zone (DMZ) – Perimeter network segment that is logically between internal and external networks. Its purpose is to enforce the internal network's Information Assurance policy for external information exchange and to provide external, untrusted sources with restricted access to releasable information while shielding the internal networks from outside attacks.

Denial of Service (DoS) – The prevention of authorized access to resources or the delaying of time-critical operations. (Time-critical may be milliseconds or it may be hours, depending upon the service provided.)

Disaster Recovery Plan (DRP) – Management policy and procedures used to guide an enterprise response to a major loss of enterprise capability or damage to its facilities. The DRP is the second plan needed by the enterprise risk managers and is used when the enterprise must recover (at its original facilities) from a loss of capability over a period of hours or days. See Continuity of Operations Plan and Contingency Plan.

Discretionary Access Control (DAC) – A means of restricting access to objects (e.g., files, data entities) based on the identity and need-to-know of subjects (e.g., users, processes) and/or groups to which the object belongs. The controls are discretionary in the sense that a subject with certain access permission is capable of passing that permission (perhaps indirectly) on to any other subject (unless restrained by mandatory access control).

disruption – An unplanned event that causes the general system or major application to be inoperable for an unacceptable length of time (e.g., minor or extended power outage, extended unavailable network, or equipment or facility damage or destruction).

Distributed Denial of Service (DdoS) – A Denial of Service technique that uses numerous hosts to perform the attack.

Domain Name Service (DNS) – A hierarchical distributed naming system for computers, services, or any resource connected to the Internet or a private network. It associates various pieces of information with domain names assigned to each of the participating entities. Most importantly, it translates domain names meaningful to humans into the numerical identifiers associated with networking equipment for the purpose of locating and addressing these devices worldwide.

Domain Name Service Security Extensions (DNSSEC) – A suite of Internet Engineering Task Force (IETF) specifications for securing certain kinds of information provided by the Domain Name System (DNS) as used on Internet Protocol (IP) networks. It is a set of extensions to DNS which provide to DNS clients (resolvers) origin authentication of DNS data, authenticated denial of existence, and data integrity, but not availability or confidentiality.

dumpster diving – The practice of sifting through commercial or residential trash containers to find items of useful in identity theft, social engineering, or for items of value that have been discarded without proper destruction of the information contained.

E

electronic signature – The process of applying any mark in electronic form with the intent to sign a data object. (See also digital signature.)

enclave – Collection of information systems connected by one or more internal networks under the control of a single authority and security policy. The systems may be structured by physical proximity or by function, independent of location.

encryption – The process of changing plaintext into ciphertext for the purpose of security or privacy.

encryption certificate – A certificate containing a public key that can encrypt or decrypt electronic messages, files, documents, or data transmissions, or establish or exchange a session key for these same purposes. Key management sometimes refers to the process of storing protecting and escrowing the private component of the key pair associated with the encryption certificate. (See also certificate)

end-to-end encryption – Encryption of information at its origin and decryption at its intended destination without intermediate decryption.

end-to-end security – Safeguarding information in an information system from point of origin to point of destination.

Enterprise Architecture (EA) – The description of an enterprise's entire set of information systems: how they are configured, how they are integrated, how they interface to the external environment at the enterprise's boundary, how they are operated to support the enterprise mission, and how they contribute to the enterprise's overall security posture.

Enterprise Resource Planning (ERP) – A system(s) integrating internal and external management information across an entire organization, embracing finance/accounting, manufacturing, asset management, sales and service, customer relationship management, etc. ERP systems automate this activity with an integrated software application. The purpose of ERP is to facilitate the flow of information between all business functions inside the boundaries of the organization and manage the connections to outside stakeholders.

enterprise risk management – The methods and processes used by an enterprise to manage risks to its mission and to establish the trust necessary for the enterprise to support shared missions. It involves the identification of mission dependencies on enterprise capabilities, the identification and prioritization of risks due to defined threats, the implementation of countermeasures to provide both a static risk posture and an effective dynamic response to active threats; and it assesses enterprise performance against threats and adjusts countermeasures as necessary.

Evaluation Assurance Level (EAL) – Set of assurance requirements that represent a point on the Common Criteria predefined assurance scale.

event – Any observable occurrence in a system and/or network. Events sometimes provide indication that an incident is occurring.

external information system – An information system or component of an information system that is outside of the authorization boundary established by the organization and for which the organization typically has no direct control over the application of required security controls or the assessment of security control effectiveness.

extranet – A private network that uses Web technology, permitting the sharing of portions of an enterprise's information or operations with suppliers, vendors, partners, customers, or other enterprises.

F

failover – The capability to switch over automatically (typically without human intervention or warning) to a redundant or standby information system upon the failure or abnormal termination of the previously active system.

false acceptance – In biometrics, the instance of a security system incorrectly verifying or identifying an unauthorized person. It typically is considered the most serious of biometric security errors as it gives unauthorized users access to systems that expressly are trying to keep them out.

False Acceptance Rate (FAR) – The measure of the likelihood that the biometric security system will incorrectly accept an access attempt by an unauthorized user. A system's false acceptance rate typically is stated as the ratio of the number of false acceptances divided by the number of identification attempts.

false rejection – In biometrics, the instance of a security system failing to verify or identify an authorized person. It does not necessarily indicate a flaw in the biometric system; for example, in a fingerprint-based system, an incorrectly aligned finger on the scanner or dirt on the scanner can result in the scanner misreading the fingerprint, causing a false rejection of the authorized user.

False Rejection Rate (FRR) – The measure of the likelihood that the biometric security system will incorrectly reject an access attempt by an authorized user. A system's false rejection rate typically is stated as the ratio of the number of false rejections divided by the number of identification attempts.

Federal Information Processing Standard (FIPS) – A standard for adoption and use by Federal agencies that has been developed within the Information Technology Laboratory and published by the National Institute of Standards and Technology, a part of the U.S. Department of Commerce. A FIPS covers some topic in information technology in order to achieve a common level of quality or some level of interoperability.

Federal Information Security Management Act (FISMA) – A statute (Title III, P.L. 107-347) that requires agencies to assess risk to information systems and provide information security protections commensurate with the risk. FISMA also requires that agencies integrate information security into their capital planning and enterprise architecture processes, conduct annual information systems security reviews of all programs and systems, and report the results of those reviews to OMB.

file protection – Aggregate of processes and procedures designed to inhibit unauthorized access, contamination, elimination, modification, or destruction of a file or any of its contents.

firewall – A hardware/software capability that limits access between networks and/or systems in accordance with a specific security policy.

flooding – An attack that attempts to cause a failure in a system by providing more input than the system can process properly.

forensics copy – An accurate bit-for-bit reproduction of the information contained on an electronic device or associated media, whose validity and integrity has been verified using an accepted algorithm.

forensics – The practice of gathering, retaining, and analyzing computer-related data for investigative purposes in a manner that maintains the integrity of the data.

File Transfer Protocol (FTP) – A standard network protocol used to transfer files from one host to another host over a TCP-based network, such as the Internet.

fault tolerant – The property that enables a system (often computer-based) to continue operating properly in the event of the failure of (or one or more faults within) some of its components. If its operating quality decreases at all, the decrease is proportional to the severity of the failure, as compared to a naïvely-designed system in which even a small failure can cause total breakdown. Fault-tolerance is particularly sought-after in high-availability or life-critical systems.

G

gateway – Interface providing compatibility between networks by converting transmission speeds, protocols, codes, or security measures.

general user – An authorized user of a computer, system or application. General users make up the largest portion of all users of system; general users are granted the concept of least-privilege and are only granted access to systems and data in order to perform normal work duties.

General Users Guide (GUG) – A set of standards, guidelines and procedures used by general users of a computer system to perform their daily work assignments.

Global Information Grid (GIG) – The globally interconnected, end-to-end set of information capabilities for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel. The GIG includes owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services, and National Security Systems. Non-GIG IT includes stand-alone, self-contained, or embedded IT that is not, and will not be, connected to the enterprise network.

group authenticator – Used, sometimes in addition to a sign-on authenticator, to allow access to specific data or functions that may be shared by all members of a particular group.

Guard (system) – A mechanism limiting the exchange of information between information systems or subsystems.

H

hacker – Unauthorized user who attempts to or gains access to an information system.

Hacktivism – (a morphing of the words of hack and activism) is the use of computers and computer networks as a means of protest to promote political ends. The term was first coined in 1996 by a member of the Cult of the Dead Cow hacker collective named Omega. If hacking as "illegally breaking into computers" is assumed, then hacktivism could be defined as "the use of legal and/or illegal digital tools in pursuit of political ends". These tools include web site defacements, redirects, denial-of-service attacks, information theft, web site parodies, virtual sit-ins, typosquatting and virtual sabotage. If hacking as "clever computer usage/programming" is assumed, then hacktivism could be understood as the writing of code to promote political ideology: promoting expressive politics, free speech, human rights, and information ethics through software development. Acts of hacktivism are carried out in the belief that proper use of code will be able to produce similar results to those produced by regular activism or civil disobedience.

hacktivist – An individual who uses computers and computer networks as a means of protest to promote political ends.

hardware – The physical components of an information system.

Health Information Privacy Accountability Act(HIPAA) – Federal legislation enacted on August 21, 1996 by the United States Congress. Title I of HIPAA protects health insurance coverage for workers and their families when they change or lose their jobs. Title II of HIPAA, known as the Administrative Simplification (AS) provisions, requires the establishment of national standards for electronic health care transactions and national identifiers for providers, health insurance plans, and employers.

high impact – The loss of confidentiality, integrity, or availability that could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, individuals, other organizations, or the national security interests of the United States; (i.e., 1) causes a severe degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; 2) results in major damage to organizational assets; 3) results in major financial loss; or 4) results in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.)

high-impact system – An information system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a potential impact value of high.

honeypot – A system (e.g., a web server) or system resource (e.g., a file on a server) that is designed to be attractive to potential crackers and intruders and has no authorized users other than its administrators.

honeynet – A honeynet is a network set up with intentional vulnerabilities; its purpose is to invite attack, so that an attacker's activities and methods can be studied and that information used to increase network security. A honeynet contains one or more honey pots, which are computer systems on the Internet expressly set up to attract and "trap" people who attempt to penetrate other people's computer systems. Although the primary purpose of a honeynet is to gather information about attackers' methods and motives, the decoy network can benefit its operator in other ways, for example by diverting attackers from a real network and its resources.

hot site – Backup site that includes phone systems with the phone lines already connected. Networks will also be in place, with any necessary routers and switches plugged in and turned on. Desks will have desktop PCs installed and waiting, and server areas will be replete with the necessary hardware to support business-critical functions. Within a few hours, a hot site can become a fully functioning element of an organization.

Hypertext Markup Language (HTML) – The main markup languages for creation of web pages, the elements of HTML are the basic building blocks of webpages.

Hypertext Transfer Protocol (HTTP) – Is the application protocol for distributed, collaborative, hypermedia information systems. HTTP is the foundation of data communication for the World Wide Web.

Hypertext Transfer Protocol Secure (HTTPS) – Is the combination of Hypertext Transfer Protocol (HTTP) with SSL protocol. It provides encrypted communication and secure identification of a network web server.

identification – An act or process that presents an identifier to a system so that the system can recognize a system entity (e.g., user, process, or device) and distinguish that entity from all others.

identifier – A data object – often, a printable, non-blank character string – that definitively represents a specific identity of a system entity, distinguishing that identity from all others.

identity – The set of attribute values (i.e., characteristics) by which an entity is recognizable and that, within the scope of an identity manager's responsibility, is sufficient to distinguish that entity from any other entity.

identity token – Smart card, metal key, or other physical object used to authenticate identity.

identity-based access control – Access control based on the identity of the user (typically relayed as a characteristic of the process acting on behalf of that user) where access authorizations to specific objects are assigned based on user identity.

identity certificate – A certificate that provides authentication of the identity claimed. Within the NSS PKI, identity certificates may be used only for authentication or may be used for both authentication and digital signatures. (See also certificate.)

impact level – The magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability.

inadvertent disclosure – Type of incident involving accidental exposure of information to an individual not authorized access.

incident – An assessed occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system; or the information the system processes, stores, or transmits; or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

incident response plan – The documentation of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of an incident against an organization's IT systems(s).

indicator – Recognized action, specific, generalized, or theoretical, that an adversary might be expected to take in preparation for an attack.

individual accountability – Ability to associate positively the identity of a user with the time, method, and degree of access to an information system.

information – Any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual.

Information Assurance (IA) – Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. While focused dominantly on information in digital form, the full range of IA encompasses not only digital but also analog or physical form. Information assurance as a field has grown from the practice of information security which in turn grew out of practices and procedures of computer security.

Information Assurance Vulnerability Alert (IAVA) – Notification that is generated when an Information Assurance vulnerability may result in an immediate and potentially severe threat to DoD systems and information; this alert requires corrective action because of the severity of the vulnerability risk.

IA architecture – A description of the structure and behavior for an enterprise's security processes, information security systems, personnel and organizational sub-units, showing their alignment with the enterprise's mission and strategic plans.

IA infrastructure – The underlying security framework that lies beyond an enterprise's defined boundary, but supports its IA and IA-enabled products, its security posture and its risk management plan.

Industrial Control System (ICS) – A term describing the control systems used in industrial production. E.g. Power, water or manufacturing systems. (See also Supervisory Control and Data Acquisition.)

Information Resources Management (IRM) – The planning, budgeting, organizing, directing, training, controlling, and management activities associated with the burden, collection, creation, use, and dissemination of information by agencies.

Information Security (IS) – The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

information security policy – Aggregate of directives, regulations, rules, and practices that prescribe how an organization manages, protects, and distributes information.

Information System (IS) – A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
Note: Information systems also include specialized systems such as industrial/process controls systems, telephone switching and private branch exchange (PBX) systems, and environmental control systems.

information system life cycle – The phases through which an information system passes, typically characterized as initiation, development, operation, and termination (i.e., sanitization, disposal and/or destruction).

Information Technology (IT) – Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which 1) requires the use of such equipment or 2) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term information technology includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources.

Infrastructure As A Service (IaaS) – Delivers cloud computer infrastructure services, typically in the form of platform virtualization environments. A customer purchase services in the form of a utility and includes all resources necessary to satisfy client computing requirements.

inside acquisition threat – An entity with authorized access (i.e., within the security domain) that has the potential to harm an information system or enterprise through destruction, disclosure, modification of data, and/or denial of service.

integrity – The property whereby an entity has not been modified in an unauthorized manner.

intellectual property – Creations of the mind such as musical, literary, and artistic works; inventions; and symbols, names, images, and designs used in commerce, including copyrights, trademarks, patents, and related rights. Under intellectual property law, the holder of one of these abstract "properties" has certain exclusive rights to the creative work, commercial symbol, or invention by which it is covered.

Interconnection Security Agreement (ISA) – A document that regulates security-relevant aspects of an intended connection between an agency and an external system. It regulates the security interface between any two systems operating under two different distinct authorities. It includes a variety of descriptive, technical, procedural, and planning information. It is usually preceded by a formal MOA/MOU that defines high-level roles and responsibilities in management of a cross-domain connection.

interface – Common boundary between independent systems or modules where interactions take place.

internal network – A network where 1) the establishment, maintenance, and provisioning of security controls are under the direct control of organizational employees or contractors; or 2) cryptographic encapsulation or similar security technology implemented between organization-controlled endpoints provides the same effect (at least with regard to confidentiality and integrity). An internal network is typically organization-owned, yet may be organization-controlled while not being organization-owned.

internal security controls – Hardware, firmware, or software features within an information system that restrict access to resources to only authorized subjects.

Internet – The Internet is the single, interconnected, worldwide system of commercial, governmental, educational, and other computer networks that share (a) the protocol suite specified by the IAB and (b) the name and address spaces managed by the Internet Corporation for Assigned Names and Numbers (ICANN).

Internet Protocol (IP) – Standard protocol for transmission of data from source to destinations in packet-switched communications networks and interconnected systems of such networks.

intranet – A private network that is employed within the confines of a given enterprise (e.g., internal to a business or agency).

intrusion – Unauthorized act of bypassing the security mechanisms of a system.

Intrusion Detection Systems (IDS) – Hardware or software products that gather and analyze information from various areas within a computer or a network to identify possible security breaches, which include both intrusions (attacks from outside the organizations) and misuse (attacks from with the organizations).

Intrusion Detection Systems (IDS) (host-based) – IDSs which operate on information collected from within an individual computer system. This vantage point allows host-based IDSs to determine exactly which processes and user accounts are involved in a particular attack on the Operating System. Furthermore, unlike network-based IDSs, host-based IDSs can more readily "see" the intended outcome of an attempted attack, because they can directly access and monitor the data files and system processes usually targeted by attacks.

Intrusion Detection Systems (IDS) (network-based) – IDSs which detect attacks by capturing and analyzing network packets. Listening on a network segment or switch, one network-based IDS can monitor the network traffic affecting multiple hosts that are connected to the network segment.

Intrusion Prevention System (IPS) – System that can detect an intrusive activity and can also attempt to stop the activity, ideally before it reaches its targets.

IP Security (IPSEC) – Suite of protocols for securing Internet Protocol (IP) communications at the network layer, layer 3 of the OSI model by authenticating and/or encrypting each IP packet in a data stream. IPSec also includes protocols for cryptographic key establishment.

IT Security awareness and training program – Explains proper rules of behavior for the use of agency information systems and information. The program communicates IT security policies and procedures that need to be followed.

J

K

keystroke monitoring – The process used to view or record both the keystrokes entered by a computer user and the computer's response during an interactive session. Keystroke monitoring is usually considered a special case of audit trails.

L

label – See Security Label

labeled security protections – Access control protection features of a system that use security labels to make access control decisions.

Lean Six Sigma – A synergized managerial concept of Lean and Six Sigma that results in the elimination of the seven kinds of wastes (classified as Defects, Overproduction, Transportation, Waiting, Inventory, Motion and Over-Processing) and provision of goods and service at a rate of 3.4 defects per million opportunities (DPMO) .

The Lean Six Sigma concepts were first published in the book titled "Lean Six Sigma: Combining Six Sigma with Lean Speed" authored by Michael George in the year 2002. Lean Six Sigma utilizes the DMAIC phases similar to that of Six Sigma. The Lean Six Sigma projects comprise the Lean's waste elimination projects and the Six Sigma projects based on the critical to quality characteristics. The DMAIC toolkit of Lean Six Sigma comprises all the Lean and Six Sigma tools. The training for Lean Six Sigma is provided through the belt based training system similar to that of Six Sigma. The belt personnel are designated as White Belts, Yellow Belts, Green Belts, Black Belts and Master Black Belts. See also Six Sigma

least privilege – The principle that security architecture should be designed so that each entity is granted the minimum system resources and authorizations that the entity needs to perform its function.

least trust – The principal that security architecture should be designed in a way that minimizes 1) the number of components that require trust and 2) the extent to which each component is trusted.

likelihood of occurrence – In Information Assurance risk analysis, a weighted factor based on a subjective analysis of the probability that a given threat is capable of exploiting a given vulnerability.

local access – Access to an organizational information system by a user (or process acting on behalf of a user) communicating through a direct connection without the use of a network.

local authority – Organization responsible for generating and signing user certificates in a PKI-enabled environment.

logic bomb – A piece of code intentionally inserted into a software system that will set off a malicious function when specified conditions are met.

logical perimeter – A conceptual perimeter that extends to all intended users of the system, both directly and indirectly connected, who receive output from the system. Without a reliable human review by an appropriate authority. The location of such a review is commonly referred to as an “air gap.”

Long Term Evolution – A mobile communication standard which allows for higher speeds in the transmission of data and voice to mobile devices such as cellular phones, tablet devices, etc. A standard associated with 3G and 4G communications. See 3rd and 4th Generation.

low impact – The loss of confidentiality, integrity, or availability that could be expected to have a limited adverse effect on organizational operations, organizational assets, individuals, other organizations, or the interests of the State of Hawai‘I; (i.e., 1) causes a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; 2) results in minor damage to organizational assets; 3) results in minor financial loss; or 4) results in minor harm to individuals.

low-impact system – An information system in which all three security properties (i.e., confidentiality, integrity, and availability) are assigned a potential impact value of low.

M

macro virus – A virus that attaches itself to documents and uses the macro programming capabilities of the document’s application to execute and propagate.

magnetic remanence – Magnetic representation of residual information remaining on a magnetic medium after the medium has been cleared. See clearing.

malicious applets – Small application programs that are automatically downloaded and executed and that perform an unauthorized function on an information system.

malicious code – Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. A virus, worm, Trojan horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malicious code.

malicious logic – Hardware, firmware, or software that is intentionally included or inserted in a system for a harmful purpose.

malware – See malicious code, malicious applets, and malicious logic.

management controls – Actions taken to manage the development, maintenance, and use of the system, including system-specific policies, procedures and rules of behavior, individual roles and responsibilities, individual accountability, and personnel security decisions.

management security controls – The security controls (i.e., safeguards or countermeasures) for an information system that focus on the management of risk and the management of information systems security.

Mandatory Access Control (MAC) – A means of restricting access to objects based on the sensitivity (as represented by a security label) of the information contained in the objects and the formal authorization (i.e., clearance, formal access approvals, and need-to-know) of subjects to access information of such sensitivity.

Man-in-the-Middle Attack (MitM) – A form of active wiretapping attack in which the attacker intercepts and selectively modifies communicated data to masquerade as one or more of the entities involved in a communication association.

masquerading – A type of threat action whereby an unauthorized entity gains access to a system or performs a malicious act by illegitimately posing as an authorized entity.

media – Physical devices or writing surfaces including but not limited to magnetic tapes, optical disks, magnetic disks, LSI memory chips, printouts (but not including display media) onto which information is recorded, stored, or printed within an information system.

media sanitization – The actions taken to render data written on media unrecoverable by both ordinary and extraordinary means.

Memorandum of Understanding/ Memorandum of Agreement (MOU/MOA) – A document established between two or more parties to define their respective responsibilities in accomplishing a particular goal or mission, e.g., establishing, operating, and securing a system interconnection.

message digest – A cryptographic checksum typically generated for a file that can be used to detect changes to the file. Synonymous with hash value/result.

mobile computing – Human–computer interaction by which a computer is expected to be transported during normal usage. Mobile computing involves mobile communication, mobile hardware, and mobile software. Communication issues include ad-hoc and infrastructure networks as well as communication properties, protocols, data formats and concrete technologies. Hardware includes mobile devices or device components

mobile code – Software programs or parts of programs obtained from remote information systems, transmitted across a network, and executed on a local information system without explicit installation or execution by the recipient.

moderate impact – The loss of confidentiality, integrity, or availability that could be expected to have a serious adverse effect on organizational operations, organizational assets, individuals, other organizations, or the State of Hawaiʻi; (i.e., 1) causes a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; 2) results in significant damage to organizational assets; 3) results in significant financial loss; or 4) results in significant harm to individuals that does not involve loss of life or serious life threatening injuries.

moderate impact system – An information system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a potential impact value of moderate and no security objective is assigned a potential impact value of high.

multi-factor authentication – An approach to security authentication, which requires that the user of a system provide more than one form of verification in order to prove their identity and allow access to the system.

Multi-factor authentication takes advantage of a combination of several factors of authentication; three major factors include verification by something a user knows (such as a password), something the user has (such as a smart card or a security token), and something the user is (such as the use of biometrics). Due to their increased complexity, authentication systems using a multi-factor configuration are harder to compromise than ones using a single factor of authentication.
See also strong authentication.

N

National Information Infrastructure (NII) – Nationwide interconnection of communications networks, computers, databases, and consumer electronics that make vast amounts of information available to users. It includes both public and private networks, the internet, the public switched network, and cable, wireless, and satellite communications.

National Vulnerability Database (NVD) – The U.S. Government repository of standards based vulnerability management data, enabling automation of vulnerability management, security measurement, and compliance (e.g., FISMA).

need-to-know – A method of isolating information resources based on a user’s need to have access to that resource in order to perform their job but no more. The terms ‘need-to know” and “least privilege” express the same idea. Need-to-know is generally applied to people, while least privilege is generally applied to processes.

need-to-know determination – Decision made by an authorized holder of official information that a prospective recipient requires access to specific official information to carry out official duties.

network – Information system(s) implemented with a collection of interconnected components. Such components may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices.

network access – Access to an organizational information system by a user (or a process acting on behalf of a user) communicating through a network (e.g., local area network, wide area network, Internet).

network resilience – A computing infrastructure that provides continuous business operation (i.e., highly resistant to disruption and able to operate in a degraded mode if damaged), rapid recovery if failure does occur, and the ability to scale to meet rapid or unpredictable demands.

non-repudiation – Assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender’s identity, so neither can later deny having processed the information.

O

object – Passive information system-related entity (e.g., devices, files, records, tables, processes, programs, domains) containing or receiving information. Access to an object implies access to the information it contains.

object reuse – Reassignment and reuse of a storage medium containing one or more objects after ensuring no residual data remains on the storage medium.

operational controls – The security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by people (as opposed to systems).

Operations Security (OPSEC) – Systematic and proven process by which potential adversaries can be denied information about capabilities and intentions by identifying, controlling, and protecting generally unclassified evidence of the planning and execution of sensitive activities. The process involves five steps: identification of critical information, analysis of threats, analysis of vulnerabilities, assessment of risks, and application of appropriate countermeasures.

outside acquisition threat – An unauthorized entity outside the security domain that has the potential to harm an information system through destruction, disclosure, modification of data, and/or denial of service.

overt channel – Communications path within a computer system or network designed for the authorized transfer of data. See covert channel.

overwrite procedure – A software process that replaces data previously stored on storage media with a predetermined set of meaningless data or random patterns.

P

packet sniffer – Software that observes and records network traffic.

passive attack – An attack that does not alter systems or data.

password – A secret string of letters, numbers and special characters used for accessing information systems. User supplied and maintained.

patch management – The systematic notification, identification, deployment, installation, and verification of operating system and application software code revisions. These revisions are known as patches, hot fixes, and service packs.

Payment Card Industry-Data Security Standard (PCI-DSS) – A widely accepted set of policies and procedures intended to optimize the security of credit, debit and cash card transactions and protect cardholders against misuse of their personal information.

penetration – See intrusion.

penetration testing (PenTest) – A test methodology in which assessors, typically working under specific constraints, attempt to circumvent or defeat the security features of an information system.

perimeter – A perimeter is the boundary between the private and locally managed-and-owned side of a network and the public and usually provider-managed side of a network.

Personally Identifiable Information (PII) – Information which can be used to distinguish or trace an individual’s identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother’s maiden name, etc.

As defined in State of Hawai‘i Acts 135 and 136 includes an individual’s first name (or initial) in combination with any one or more of the following additional data elements, in combination, when the all data elements are not sufficiently encrypted.

1. Social Security Number; or
2. Driver’s License number or Hawai‘i identification number; or
3. Account number, credit/debit card number, access code, or password that would permit access to an individual’s financial account. (NOTE: this includes pCard/credit/EBT/debit cards issued to state employees or citizens of the state.)

Personal information does not include publically available information that is lawfully made available to the general public from federal, state or local via governmental records. HRS §487N-1

Personal Identification Number (PIN) – A short numeric code used to confirm identity. Often used in a multi-factor authentication implementation.

phishing – Deceiving individuals into disclosing sensitive personal information through deceptive computer-based means.

plaintext – Unencrypted information.

Plan of Action and Milestones (POA&M) – A document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.

Platform As A Service (PaaS) – A category of cloud computing services that provide a computing platform and a solution stack as a service. In the classic layered model of cloud computing, the PaaS layer lies between the SaaS and the IaaS layers.

PaaS offerings facilitate the deployment of applications without the cost and complexity of buying and managing the underlying hardware and software and provisioning hosting capabilities, providing all of the facilities required to support the complete life cycle of building and delivering web applications and services entirely available from the Internet.

Post Office Protocol (POP) – An application-layer Internet standard protocol used by local e-mail clients to retrieve e-mail from a remote server over a TCP/IP connection.

port scanning – Using a program to remotely determine which ports on a system are open (e.g., whether systems allow connections through those ports).

Portable Electronic Device (PED) – Any non-stationary electronic apparatus with singular or multiple capabilities of recording, storing, and/or transmitting data, voice, video, or photo images. This includes but is not limited to laptops, personal digital assistants, pocket personal computers, palmtops, MP3 players, cellular telephones, video cameras, and pagers.

potential impact – The loss of confidentiality, integrity, or availability that could be expected to have a limited (low) adverse effect, a serious (moderate) adverse effect, or a severe or catastrophic (high) adverse effect on organizational operations, organizational assets, or individuals.

precursor – A sign that an attacker may be preparing to cause an incident. See indicator.

Privacy Impact Assessment (PIA) – An analysis of how information is handled 1) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; 2) to determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system; and 3) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

privilege – A right granted to an individual, a program, or a process.

privileged account – An information system account with approved authorizations of a privileged user.

privileged command – A human-initiated command executed on an information system involving the control, monitoring, or administration of the system including security functions and associated security-relevant information.

privileged process – A computer process that is authorized (and, therefore, trusted) to perform security-relevant functions that ordinary processes are not authorized to perform.

privileged user – A user that is authorized (and, therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform.

Privileged Users Guide (PUG) – document(s) intended to outline approved methodologies used by privileged users in maintaining and monitoring computer systems.

Privileged User Management (PUM) – The function of monitoring privileged access and usage of systems.

probability of occurrence – See likelihood of occurrence.

probe – A technique that attempts to access a system to learn something about the system.

profiling – Measuring the characteristics of expected activity so that changes to it can be more easily identified.

proprietary information – Material and information relating to or associated with the State's products, business, or activities, including but not limited to financial information; data or statements; trade secrets; product research and development; existing and future product designs and performance specifications; marketing plans or techniques; schematics; client lists; computer programs; processes; and know-how that has been clearly identified and properly marked by the state as proprietary information, trade secrets, or company confidential information. The information must have been developed by the company and not be available to the Government or to the public without restriction from another source.

protection level (PL) – Based on the Confidentiality of information contained with a system. Each Information System shall incorporate security features that will control the release of information commensurate with the sensitivity of the information being processed, as well as with the established access approval procedures, and need-to-know of the users of the IS, will determine the Protection Level assigned to the IS. For each IS, assurance commensurate with the Protection Level shall be provided.

protection philosophy – Informal description of the overall design of an information system delineating each of the protection mechanisms employed. Combination of formal and informal techniques, appropriate to the evaluation class, used to show the mechanisms are adequate to enforce the security policy.

protocol – Set of rules and formats, semantic and syntactic, permitting information systems to exchange information.

proxy – An application that "breaks" the connection between client and server. The proxy accepts certain types of traffic entering or leaving a network and processes it and forwards it.
Note: This effectively closes the straight path between the internal and external networks making it more difficult for an attacker to obtain internal addresses and other details of the organization's internal network. Proxy servers are available for common Internet services; for example, a Hyper Text Transfer Protocol (HTTP) proxy used for Web access, and a Simple Mail Transfer Protocol (SMTP) proxy used for e-mail.

proxy agent – A software application running on a firewall or on a dedicated proxy server that is capable of filtering a protocol and routing it between the interfaces of the device.

proxy server – A server that services the requests of its clients by forwarding those requests to other servers.

public domain software – Software not protected by copyright laws of any nation that may be freely used without permission of, or payment to, the creator, and that carries no warranties from, or liabilities to the creator.

public key – A cryptographic key that may be widely published and is used to enable the operation of an asymmetric cryptography scheme. This key is mathematically linked with a corresponding private key. Typically, a public key can be used to encrypt, but not decrypt, or to validate a signature, but not to sign.

public key certificate – See certificate.

Public Key Cryptography – Encryption system that uses a public-private key pair for encryption and/or digital signature.

Public Key Infrastructure (PKI) – The framework and services that provide for the generation, production, distribution, control, accounting and destruction of public key certificates. Components include the personnel, policies, processes, server platforms, software, and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, recover, and revoke public key certificates.

Q

3rd Generation (3G) – The measurable end-to-end performance properties of a network service, which can be guaranteed in advance by a Service Level Agreement between a user and a service provider, so as to satisfy specific customer application requirements.
Note: These properties may include throughput (bandwidth), transit delay (latency), error rates, priority, security, packet loss, packet jitter, etc.

R

rapid application development (RAD) – A software development methodology that uses minimal planning in favor of rapid prototyping. The "planning" of software developed using RAD is interleaved with writing the software itself. The lack of extensive pre-planning generally allows software to be written much faster, and makes it easier to change requirements. See also Agile.t reciprocity – Mutual agreement among participating enterprises to accept each other's security assessments in order to reuse information system resources and/or to accept each other's assessed security posture in order to share information.

records – In computer science, records (also called tuples, structs, or compound data) are among the simplest data structures. A record is a value that contains other values, typically in fixed number and sequence and typically indexed by names. The elements of records are usually called fields or members.

For example, a date could be stored as a record containing a numeric year field, a month field represented as a string, and a numeric day-of-month field. As another example, a Personnel record might contain a name, a salary, and a rank. As yet another example, a Circle record might contain a center and a radius. In this instance, the center itself might be represented as a Point record containing x and y coordinates.

Records are distinguished from arrays by the fact that their number of fields is typically fixed, each field has a name, and that each field may have a different type.

A record type is a data type that describes such values and variables. Most modern computer languages allow the programmer to define new record types. The definition includes specifying the data type of each field and an identifier (name or label) by which it can be accessed. In type theory, product types (with no field names) are generally preferred due to their simplicity, but proper record types are studied in languages such as System F-sub. Since type-theoretical records may contain first-class function-typed fields in addition to data, they can express many features of object-oriented programming.

Records can exist in any storage medium, including main memory and mass storage devices such as magnetic tapes or hard disks. Records are a fundamental component of most data structures, especially linked data structures. Many computer files are organized as arrays of logical records, often grouped into larger physical records or blocks for efficiency.

records management – The process for tagging information for records keeping requirements as mandated in the Federal Records Act and the National Archival and Records Requirements.

Registration Authority (RA) – A trusted entity that establishes and vouches for the identity of a subscriber to a Credentials Service Provider (CSP). The RA may be an integral part of a CSP, or it may be independent of a CSP, but it has a relationship to the CSP(s).

remanence – Residual information remaining on storage media after clearing. See magnetic remanence and clearing.

remediation – The act of mitigating vulnerability or a threat.

remote access – Access to an organization's nonpublic information system by an authorized user (or an information system) communicating through an external, non-organization-controlled network (e.g., the Internet).

removable media – Portable electronic storage media such as magnetic, optical, and solid state devices, which can be inserted into and removed from a computing device, and is used to store text, video, audio, and image information. Such devices have no independent processing capabilities. Examples include hard disks, floppy disks, zip drives, compact disks (CD), thumb drives, pen drives, and similar USB storage devices.

replay attacks – An attack that involves the capture of transmitted authentication or access control information and its subsequent retransmission with the intent of producing an unauthorized effect or gaining unauthorized access.

residual risk – Portion of risk remaining after security measures have been applied.

Risk – 1) Uncertain, unpredictable, or unplanned event that, if occurs, will affect the outcome negatively or positively.; 2) A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of

a. the adverse impacts that would arise if the circumstance or event occurs; and
b. The likelihood of occurrence.

Note: Information system-related security risks are those risks that arise from the loss of confidentiality, integrity, or availability of information or information systems and reflect the potential adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the State.

risk assessment – The process of identifying, prioritizing, and estimating risks. This includes determining the extent to which adverse circumstances or events could impact an enterprise. Uses the results of threat and vulnerability assessments to identify risk to organizational operations and evaluates those risks in terms of likelihood of occurrence and impacts if they occur. The product of a risk assessment is a list of estimated, potential impacts and unmitigated vulnerabilities. Risk assessment is part of risk management and is conducted throughout the Risk Management Framework (RMF).

Part of risk management, incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place. Synonymous with risk analysis.

risk management – The process of managing risks to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the nation resulting from the operation or use of an information system, and includes:

1) the conduct of a risk assessment;
2) the implementation of a risk mitigation strategy;
3) employment of techniques and procedures for the continuous monitoring of the security state of the information system; and
4) Documenting the overall risk management program.

Risk Management Framework (RMF) – A structured approach used to oversee and manage risk for an enterprise.

risk mitigation – Prioritizing, evaluating, and implementing the appropriate risk-reducing controls/ countermeasures recommended from the risk management process.

risk tolerance – The defined impacts to an enterprise’s information systems that an entity is willing to accept.

robustness – The ability of an Information Assurance entity to operate correctly and reliably across a wide range of operational conditions, and to fail gracefully outside of that operational range.

role – A group attribute that ties membership to function. When an entity assumes a role, the entity is given certain rights that belong to that role. When the entity leaves the role, those rights are removed. The rights given are consistent with the functionality that the entity needs to perform the expected tasks.

Role-Based Access Control (RBAC) – Access control based on user roles (i.e., a collection of access authorizations a user receives based on an explicit or implicit assumption of a given role). Role permissions may be inherited through a role hierarchy and typically reflect the permissions needed to perform defined functions within an organization. A given role may apply to a single individual or to several individuals.

Root Certification Authority – In a hierarchical Public Key Infrastructure, the Certification Authority whose public key serves as the most trusted datum (i.e., the beginning of trust paths) for a security domain.

rootkit – A set of tools used by an attacker after gaining root-level access to a host to conceal the attacker's activities on the host and permit the attacker to maintain root-level access to the host through covert means.

rule-based security policy – A security policy based on global rules imposed for all subjects. These rules usually rely on a comparison of the sensitivity of the objects being accessed and the possession of corresponding attributes by the subjects requesting access. Also known as discretionary access control (DAC).

S

safeguards – Protective measures prescribed to meet the security requirements (i.e., confidentiality, integrity, and availability) specified for an information system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices. Synonymous with security controls and countermeasures.

sandbox – A restricted, controlled execution environment that prevents potentially malicious software, such as mobile code, from accessing any system resources except those for which the software is authorized.

sanitization – A general term referring to the actions taken to render data written on media unrecoverable by both ordinary and, for some forms of sanitization, extraordinary means.

scanning – Sending packets or requests to another system to gain information to be used in a subsequent attack.

scavenging – 1. Searching through object residue to acquire data;
2. The act of rummaging through items thrown away in search of sensitive or confidential information. See Social Engineering.

secure communications protocol – A communication protocol that provides the appropriate confidentiality, authentication, and content integrity protection.

Secure Shell (SSH) – A network protocol for secure data communication, remote shell services or command execution and other secure network services between two networked computers that it connects via a secure channel over an insecure network.

Secure Socket Layer (SSL) – A protocol used for protecting private information during transmission via the Internet.
Note: SSL works by using a public key to encrypt data that's transferred over the SSL connection. Most web browsers support SSL and many web sites use the protocol to obtain confidential user information, such as credit card numbers. By convention, URLs that require an SSL connection start with "https:" instead of "http:."

Secure/Multipurpose Internet Mail Extensions (S/MIME) – A set of specifications for securing electronic mail. Secure/ Multipurpose Internet Mail Extensions (S/MIME) is based upon the widely used MIME standard and describes a protocol for adding cryptographic security services through MIME encapsulation of digitally signed and encrypted objects. The basic security services offered by S/MIME are authentication, non-repudiation of origin, message integrity, and message privacy. Optional security services include signed receipts, security labels, secure mailing lists, and an extended method of identifying the signer's certificate(s).

security – A condition that results from the establishment and maintenance of protective measures that enable an enterprise to perform its mission or critical functions despite risks posed by threats to its use of information systems. Protective measures may involve a combination of deterrence, avoidance, prevention, detection, recovery, and correction that should form part of the enterprise's risk management approach.

Security As A Service (SaaS) – Security-as-a-service (SaaS) is a service delivery model for security management. Typically, Security as a Service involves applications such as anti-virus software delivered over the Internet but the term can also refer to security management provided in-house by an external organization.

Security Assertion Markup Language (SAML) – A protocol consisting of XML-based request and response message formats for exchanging security information, expressed in the form of assertions about subjects, between on-line business partners.

security association – A relationship established between two or more entities to enable them to protect data they exchange.

security attribute – An abstraction representing the basic properties or characteristics of an entity with respect to safeguarding information; typically associated with internal data structures (e.g., records, buffers, files) within the information system which are used to enable the implementation of access control and flow control policies; reflect special dissemination, handling, or distribution instructions; or support other aspects of the information security policy.

security audit – See audit.

security banner – A banner at the top or bottom of a computer screen that states the overall classification of the system in large, bold type. Also can refer to the opening screen that informs users of the security implications of accessing a computer resource.

Security Concept of Operations (Security CONOP) – A security-focused description of an information system, its operational policies, classes of users, interactions between the system and its users, and the system's contribution to the operational mission.

Security Content Automation Protocol (SCAP) – A method for using specific standardized testing methods to enable automated vulnerability management, measurement, and policy compliance evaluation against a standardized set of security requirements.

security control assessment – The testing and/or evaluation of the management, operational, and technical security controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system or enterprise.

security control baseline – The set of minimum security controls defined for a low-impact, moderate-impact, or high-impact information system.

security control inheritance – A situation in which an information system or application receives protection from security controls (or portions of security controls) that are developed, implemented, and assessed, authorized, and monitored by entities other than those responsible for the system or application; entities either internal or external to the organization where the system or application resides. See Common Control.

security controls – The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.

security engineering – An interdisciplinary approach and means to enable the realization of secure systems. It focuses on defining customer needs, security protection requirements, and required functionality early in the systems development lifecycle, documenting requirements, and then proceeding with design, synthesis, and system validation while considering the complete problem.

Security Fault Analysis (SFA) – An assessment usually performed on information system hardware, to determine the security properties of a device when hardware fault is encountered.

Security Features Users Guide (SFUG) – Guide or manual explaining how the security mechanisms in a specific system work.

security impact analysis – The analysis conducted by an organizational official to determine the extent to which changes to the information system have affected the security state of the system.

security incident – See incident.

security inspection – Examination of an information system to determine compliance with security policy, procedures, and practices. See audit

security perimeter – A physical or logical boundary that is defined for a system, domain, or enclave; within which particular security policy or security architecture is applied.

security policy – A set of criteria for the provision of security services.

security posture – The security status of an enterprise's networks, information, and systems based on IA resources (e.g., people, hardware, software, policies) and capabilities in place to manage the defense of the enterprise and to react as the situation changes.

security relevant change – Any change to a system's configuration, environment, information content, functionality, or users which has the potential to change the risk imposed upon its continued operations.

security relevant event – An occurrence (e.g., an auditable event or flag) considered to have potential security implications to the system or its environment that may require further action (noting, investigating, or reacting).

security requirements – Requirements levied on an information system that are derived from applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, or procedures, or organizational mission/business case needs to ensure the confidentiality, integrity, and availability of the information being processed, stored, or transmitted.

security requirements baseline – Description of the minimum requirements necessary for an information system to maintain an acceptable level of risk.

Security Requirements Traceability Matrix (SRTM) – Matrix that captures all security requirements linked to potential risks and addresses all applicable C&A requirements. It is, therefore, a correlation statement of a system's security features and compliance methods for each security requirement.

security safeguards – Protective measures and controls prescribed to meet the security requirements specified for an information system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices.

Security Test and Evaluation (ST&E) – Examination and analysis of the safeguards required to protect an information system, as they have been applied in an operational environment, to determine the security posture of that system.

sensitivity – A measure of the importance assigned to information by its owner, for the purpose of denoting its need for protection.

service level agreement – Defines the specific responsibilities of the service provider and sets the customer expectations.

signature – A recognizable, distinguishing pattern. See also attack signature or digital signature.

signature certificate – A public key certificate that contains a public key intended for verifying digital signatures rather than encrypting data or performing any other cryptographic functions.

Simple Mail Transfer Protocol (SMTP) – The Internet standard for electronic mail (e-mail) transmission across Internet Protocol (IP) networks.

situational awareness – Within a volume of time and space, the perception of an enterprise's security posture and its threat environment; the comprehension/meaning of both taken together (risk); and the projection of their status into the near future.

Six Sigma – A business management strategy, originally developed by Motorola in 1986. Six Sigma became well known after Jack Welch made it a central focus of his business strategy at General Electric in 1995, and today it is widely used in many sectors of industry and government.

Six Sigma seeks to improve the quality of process outputs by identifying and removing the causes of defects (errors) and minimizing variability in manufacturing and business processes. It uses a set of quality management methods, including statistical methods, and creates a special infrastructure of people within the organization ("Black Belts", "Green Belts", etc.) who are experts in these methods. Each Six Sigma project carried out within an organization follows a defined sequence of steps and has quantified financial targets (cost reduction and/or profit increase).

smart card – A credit card-sized card with embedded integrated circuits that can store, process, and communicate information.

sniffer – See packet sniffer or passive wiretapping.

social engineering – An attempt to trick someone into revealing information (e.g., a password) that can be used for identity theft or attacks against networks or computer systems.

software – Computer programs and associated data that may be dynamically written or modified during execution.

Software as a Service – The use of cloud computing to deliver software and associated data to clients Also referred to as "on-demand software"

software assurance – Level of confidence that software is free from vulnerabilities, either intentionally designed into the software or accidentally inserted at any time during its lifecycle and that the software functions in the intended manner.

software system test and evaluation – Process that plans, develops, and documents the qualitative/quantitative demonstration of the fulfillment of all baseline functional performance, operational, and interface requirements.

solid state drive (SSD) – A data storage device that uses integrated circuit assemblies as memory to store data persistently. SSD technology uses electronic interfaces compatible with traditional block input/output (I/O) magnetic hard disk drives. SSDs do not employ any moving mechanical components, which distinguishes them from traditional magnetic disks such as hard disk drives (HDDs) or floppy disks, which are electromechanical devices containing spinning disks and movable read/write heads. Compared with electromechanical disks, SSDs are typically less susceptible to physical shock, are silent, lower power consumption, reduced heat signature and have lower access time and latency, but are currently more expensive per unit of storage than magnetic storage.

spam – Electronic junk mail or the abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages.

spoofing – 1. Faking the sending address of a transmission to gain illegal entry into a secure system.
2. The deliberate inducement of a user or resource to take incorrect action.
Note: Impersonating, masquerading, piggybacking, and mimicking are forms of spoofing.

spyware – Software that is secretly or surreptitiously installed into an information system to gather information on individuals or organizations without their knowledge; a type of malicious code.

steganography – The art, science, and practice of communicating in a way that hides the existence of the communication.

strong authentication – The requirement to use multiple factors for authentication and advanced technology, such as dynamic passwords or digital certificates, to verify an entity's identity. See multi-factor authentication

SUDO – An operating system command that allows a general user to gain privileged access to an information system or application.

Supervisory Control and Data Acquisition (SCADA) – computer systems that monitor and control industrial, infrastructure, or facility-based processes, as described below:

- Industrial processes include those of manufacturing, production, power generation, fabrication, and refining, and may run in continuous, batch, repetitive, or discrete tmodes.
- Infrastructure processes may be public or private, and include water treatment and distribution, wastewater collection and treatment, oil and gas pipelines, electrical power transmission and distribution, wind farms, civil defense siren systems, and large communication systems.
- Facility processes occur both in public facilities and private ones, including buildings, airports, ships, and space stations. They monitor and control HVAC, access, and energy consumption.

(See also Industrial Control Systems.)

supply chain – A system of organizations, people, activities, information, and resources, possibly international in scope, that provides products or services to consumers.

supply chain attack – Attacks that allow the adversary to utilize implants or other vulnerabilities inserted prior to installation in order to infiltrate data, or manipulate information technology hardware, software, operating systems, peripherals (information technology products) or services at any point during the life cycle.

system – Any organized assembly of resources and procedures united and regulated by interaction or interdependence to accomplish a set of specific functions. See also information system.

System Administrator (SA) – Individual responsible for the installation and maintenance of an information system, providing effective information system utilization, adequate security parameters, and sound implementation of established Information Assurance policy and procedures.

System Development Life Cycle (SDLC) – The scope of activities associated with a system, encompassing the system's initiation, development and acquisition, implementation, operation and maintenance, and ultimately its disposal that instigates another system initiation.

System High Mode – Information systems security mode of operation wherein each user, with direct or indirect access to the information system, its peripherals, remote terminals, or remote hosts, has all of the following: 1) valid security clearance for all information within an information system; 2) formal access approval and signed nondisclosure agreements for all the information stored and/or processed (including all compartments, sub compartments and/or special access programs); and 3) valid need-to- know for some of the information contained within the information system.

system integrity – Attribute of an information system when it performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.

system interconnection – The direct connection of two or more information systems for the purpose of sharing data and other information resources.

System Security Plan (SSP) – The formal document prepared by the information system owner (or common security controls owner for inherited controls) that provides an overview of the security requirements for the system and describes the security controls in place or planned for meeting those requirements. The plan can also contain as supporting appendices or as references, other key security-related documents such as a risk assessment, privacy impact assessment, system interconnection agreements, contingency plan, security configurations, configuration management plan, and incident response plan.

system-specific security control – A security control for an information system that has not been designated as a common control or the portion of a hybrid security control that is to be implemented within an information system.

super user – An individual granted a greater level of security access to an information system or application for the purposes of maintenance or support. (see privileged user)

survivability – In engineering, survivability is the quantified ability of a system, subsystem, equipment, process, or procedure to continue to function during and after a natural or man-made disturbance; e.g. nuclear electromagnetic pulse from the detonation of a nuclear weapon, tsunami, or Distributed Denial of Service attack (Ddos).

For a given application, survivability must be qualified by specifying the range of conditions over which the entity will survive, the minimum acceptable level or post-disturbance functionality, and the maximum acceptable outage duration.

T

tampering – An intentional event resulting in modification of a system, its intended behavior, or data.

Target of Evaluation (TOE) – In accordance with Common Criteria, an information system, part of a system or product, and all associated documentation, that is the subject of a security evaluation.

Technical Reference Model (TRM) – A component-driven, technical framework that categorizes the standards and technologies to support and enable the delivery of service components and capabilities.

technical security controls – Security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system.

technical vulnerability information – Detailed description of a weakness to include the implementable steps (such as code) necessary to exploit that weakness.

telecommunications – Preparation, transmission, communication, or related processing of information (writing, images, sounds, or other data) by electrical, electromagnetic, electromechanical, electro-optical, or electronic means.

threat – 1) Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.;
2) An act with a negative consequence.

threat analysis – See threat assessment.

threat assessment – Process of formally evaluating the degree of threat to an information system or enterprise and describing the nature of the threat.

threat monitoring – Analysis, assessment, and review of audit trails and other information collected for the purpose of searching out system events that may constitute violations of system security.

threat source – The intent and method targeted at the intentional exploitation of vulnerability or a situation and method that may accidentally exploit vulnerability.

Theory of Constraints – Adopts the common idiom "A chain is no stronger than its weakest link" as a new management paradigm. This means that processes, organizations, etc., are vulnerable because the weakest person or part can always damage or break them or at least adversely affect the outcome.

The analytic approach with TOC comes from the contention that any manageable system is limited in achieving more of its goals by a very small number of constraints, and that there is always at least one constraint. Hence the TOC process seeks to identify the constraint and restructure the rest of the organization around it.

time bomb – Resident computer program that triggers an unauthorized act at a predefined time.

time-dependent password – Password that is valid only at a certain time of day or during a specified interval of time.

token – Something that the claimant possesses and controls (such as a key or password) that is used to authenticate a claim. See also cryptographic token.

Total Quality Management – A business management philosophy used by management for continuously improving the quality of output from manufacturing and business processes. (See also, 6 Sigma, Lean Six Sigma & Theory of Constraints.)

Traffic Analysis (TA) – Gaining knowledge of information by inference from observable characteristics of a data flow, even if the information is not directly available (e.g., when the data is encrypted). These characteristics include the identities and locations of the source(s) and destination(s) of the flow, and the flow's presence, amount, frequency, and duration of occurrence.

traffic padding – Generation of mock communications or data units to disguise the amount of real data units being sent.

Traffic-Flow Security (TFS) – Techniques by hackers, crackers or untrusted insiders to counter Traffic Analysis. (See also Anti-Forensics.)

tranquility – Property whereby the security level of an object cannot change while the object is being processed by an information system.

transmission – The state that exists when information is being electronically sent from one location to one or more other locations.

transmission security – Measures (security controls) applied to transmissions in order to prevent interception, disruption of reception, communications deception, and/or derivation of intelligence by analysis of transmission characteristics such as signal parameters or message externals.

trap door – 1. A means of reading cryptographically protected information by the use of private knowledge of weaknesses in the cryptographic algorithm used to protect the data. (See also back door.)
2. In cryptography, one-to-one function that is easy to compute in one direction, yet believed to be difficult to invert without special information.

Trojan Horse – A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the program.

trust list – The collection of trusted certificates used by relying parties to authenticate other certificates.

trusted agent – Entity authorized to act as a representative of an Agency in confirming subscriber identification during the registration process. Trusted agents do not have automated interfaces with Certification Authorities.

trusted certificate – A certificate that is trusted by the relying party on the basis of secure and authenticated delivery. The public keys included in trusted certificates are used to start certification paths. Also known as a "trust anchor."

trusted channel – A channel where the endpoints are known and data integrity is protected in transit. Depending on the communications protocol used, data privacy may be protected in transit. Examples include SSL, IPSEC, and secure physical connection.

trusted computer system – A system that employs sufficient hardware and software assurance measures to allow its use for processing simultaneously a range of sensitive or classified information.

Trusted Computing Base (TCB) – Totality of protection mechanisms within a computer system, including hardware, firmware, and software, the combination responsible for enforcing a security policy.

trustworthiness – The attribute of a person or enterprise that provides confidence to others of the qualifications, capabilities, and reliability of that entity to perform specific tasks and fulfill assigned responsibilities.

tunneling – Technology enabling one network to send its data via another network's connections. Tunneling works by encapsulating a network protocol within packets carried by the second network.

Two-Person Control (TPC) – System of storage and handling designed to prohibit individual access by requiring the presence of at least two authorized individuals, each capable of detecting incorrect or unauthorized security procedures with respect to the task being performed.

Two-Person Integrity (TPI) – System of storage and handling designed to prohibit individual access by requiring the presence of at least two authorized individuals, each capable of detecting incorrect or unauthorized security procedures with respect to the task being performed.

U

unauthorized access – Any access that violates the stated security policy.

unauthorized disclosure – An event involving the exposure of information to entities not authorized access to the information.

untrusted process – Process that has not been evaluated or examined for correctness and adherence to the security policy. It may include incorrect or malicious code that attempts to circumvent the security mechanisms.

user – Individual, or (system) process acting on behalf of an individual, authorized to access an information system.

user ID – Unique symbol or character string used by an information system or application to identify a specific user. Used in conjunction with a password or other authentication mechanism.

V

validation – Confirmation (through the provision of strong, sound, objective evidence) that requirements for a specific intended use or application have been fulfilled (e.g., a trustworthy credential has been presented, or data or information has been formatted in accordance with a defined set of rules, or a specific process has demonstrated that an entity under consideration meets, in all respects, its defined attributes or requirements).

verification – Confirmation, through the provision of objective evidence, that specified requirements have been fulfilled (e.g., an entity's requirements have been correctly defined, or an entity’s attributes have been correctly presented; or a procedure or function performs as intended and leads to the expected outcome.

Virtual Private Network (VPN) – Protected information system link utilizing tunneling, security controls (see Information Assurance), and endpoint address translation giving the impression of a dedicated line.

virus – A computer program that can copy itself and infect a computer without permission or knowledge of the user. A virus might corrupt or delete data on a computer, use e-mail programs to spread itself to other computers, or even erase everything on a hard disk.

vulnerability – Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source.

Vulnerability assessment – Systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.

Vulnerability Assessment Review Team (VART) – Group of individuals assigned to review vulnerabilities, assess risks, make recommendations for mitigation and assist in patch management.

W

warm site – Backup site which typically contains the data links and pre-configured equipment necessary to rapidly start operations, but does not contain live data. Thus commencing operations at a warm site will (at a minimum) require the restoration of current data.

Web bug – Malicious code, invisible to a user, placed on web sites in such a way that it allows third parties to track use of web servers and collect information about the user, including IP address, host name, browser type and version, operating system name and version, and web browser cookie.

Wi-Fi Protected Access-2 (WPA-2) – The approved Wi-Fi Alliance interoperable implementation of the IEEE 802.11i security standard. For Federal government use, the implementation must use FIPS approved encryption, such as AES.

Wiki – Web applications or similar tools that allow identifiable users to add content (as in an Internet forum) and allow anyone to edit that content collectively.

Wireless Access Point (WAP) – A device that acts as a conduit to connect wireless communication devices together to allow them to communicate and create a wireless network.

Wireless Application Protocol (WAP) – A standard that defines the way in which Internet communications and other advanced services are provided on wireless mobile devices.

Wireless Equivalent Privacy (WEP) – A security algorithm for wireless networks. Introduced as part of the original wireless standard, its intention was to provide data confidentiality comparable to that of a traditional wired network. The algorithm uses key sizes of 10 or 26 hexadecimal digits, is widely in use and is often the first security choice presented to users by router configuration tools.

Although its name implies that it is as secure as a wired connection, WEP has been demonstrated to have numerous flaws and has been deprecated in favor of newer standards such as WPA2. In 2003 the Wi-Fi Alliance announced that WEP had been superseded by Wi-Fi Protected Access (WPA). In 2004, with the ratification of the full 802.11i standard (i.e. WPA2), the IEEE declared that both WEP-40 and WEP-104 “have been deprecated as they fail to meet their security goals”.

Wireless technology – Technology that permits the transfer of information between separated points without physical connection.
Note: Currently wireless technologies use infrared, acoustic, radio frequency, and optical.

Work factor – Estimate of the effort or time needed by a potential perpetrator, with specified expertise and resources, to overcome a protective measure.

Worm – A self-replicating, self-propagating, self-contained program that uses networking mechanisms to spread itself. See malicious code.

X, Y

X.509 Public Key Certificate – The public key for a user (or device) and a name for the user (or device), together with some other information, rendered unforgettable by the digital signature of the certification authority that issued the certificate, encoded in the format defined in the ISO/ITU-T X.509 standard. Also known as X.509 Certificate.

Z

zero fill – To fill unused storage locations in an information system with the representation of the character denoting "0."

3. STATE OF HAWAI‘I EXECUTIVE BRANCH DEPARTMENTS, DIVISIONS, BRANCHES, OFFICES, BOARDS, COMMISSIONS & COUNCILS

Abbreviation	Definition	Department
AG	Department of Attorney General	
B&F	Department of Budget & Finance	
CIOC	Chief Information Officers Council	Governor
DAGS	Department of Accounting and General Services	
DBEDT	Department of Business Economic Development & Tourism	
DHHL	Department of Hawaiian Home Lands	
DHRD	Department of Human Resources	
DLIR	Department of Labor & Industrial Relations	
DLNR	Department of Land and Natural Resources	
DOA	Department of Agriculture	
DOE	Department of Education	
DOH	Department of Health	
DOT	Department of Transportation	
DOTAX	Department of Taxation	
ELC	Executive Leadership Council	Governor
HCJDS	Hawai‘i Criminal Justice Data Center	AG
HDOD	Hawai‘i Department of Defense	
HPA	Hawai‘i Paroling Authority	PSD
ICSD	Information & Communications Services Division	DAGS
IPSC	Information Privacy & Security Council	DAGS
JJIS	Juvenile Justice Information Services	AG
OIMT	Office of Information Management and Technology	DAGS
PSD	Public Safety Department	
SCD	State Civil Defense	HDOD
SOH	State of Hawai‘i	
SSB	System Services Branch	ICSD
SPO	State Procurement Office	DAGS
TSSB	Telecommunication Shared Services Branch	ICSD
UH	University of Hawai‘i	

4. CIO COUNCIL ADVISORY WORKING GROUPS

Governance & Policy	Technology	Shared Services
Enterprise Architecture (EA)	Networks	Enterprise Resource Planning (ERP)
Policy	Computing and Storage	Global Information Systems (GIS)
People & Organization	Information Assurance & Privacy	Records Management
Innovation	Operations	Email & Collaboration
IT Procurement	Development	

5. COMMONLY USED TECHNICAL ABBREVIATIONS AND ACRONYMS

Acronym	Definition
(ISC)2®	International Information Systems Security Certification Consortium, Inc.
3G	3rd Generation
4G	4th Generation
6∑	6 SIGMA
APT	Advanced Persistent Threat
BPR	Business Process Reengineering
C&A	Configuration & Accreditation
CCB	Change Control Board
CCNA	Cisco Certified Network Associate
CCNE	Cisco Certified Network Engineer
CCSP	Cisco Certified Security Professional
CEH	Certified Ethical Hacker
CIA	Confidentiality Integrity Availability
CIO	Chief Information Officer
CIOC	Chief Information Officer Council
CIP	Capital Infrastructure Planning
CISO	Chief Information Security Officer
CISSP	Certified Information Security Services Professional
COE	Center of Excellence
CSTCB	Cyber Security Technology & Controls Branch
CS	Cyber Security
CSIRT	Computer Security Incident Response Team
CTA	Chief Technical Architect
DAM	Database Access Management
DAR	Data at Rest
DC	Data Center
DCIO	Deputy Chief Information Officer
DIACAP	Defense Information Assurance Certification and Accreditation Program

Acronym	Definition
DIM	Data in Motion
DLP	Data Loss Prevention
DISO	Department Information Security Officer
EA	Enterprise Architecture
ELC	Enterprise Leadership Council
ERP	Enterprise Resource Management
FEDRAMP	Federal Risk and Authorization Management Program
FISMA	Federal Information System Management Act
FTE	Full Time Equivalent
FTP	File Transfer Protocol
GLB	Gramm-Leach-Bliley Act
HIPAA	Health Insurance Portability and Accountability Act
HRM	Human Resource Management
HWIN	Hawai‘i Wireless Interoperability Network
IA	Information Assurance
IaaS	Infrastructure as a Service
IACSD	Information Assurance & Cyber Security Division
IAMSG	Identity & Access Management/Security Governance
ICAM	Identity
ICS	Industrial Control System
IRM	Information Resource Management
IS	Information System / Information Security
IT	Information Technology
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LMR	Land Mobile Radio
LTE	Long Term Evolution
MAN	Metropolitan Area Network
MOA	Memo of Agreement
MOU	Memorandum of Understanding
NGN	Next Generation Network
NIST	National Institute for Standards and Technology
NOC	Network Operations Center
OIMT	Office of Information Management & Technology

Acronym	Definition
PaaS	Platform as a Service
PCI-DSS	Payment Card Industry – Data Security Standard
PII	Personally Identifiable Information
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PM	Program Management
POA&M	Plan of Action & Milestones
RFC	Request for Change
RPZ	Regional Planning Zone
RTM	Requirements Traceability Matrix
SaaS	Software as a Service
SCADA	Supervisory Control and Data Acquisition
SecSaaS	Security as a Service
SCIP	Statewide Communications Interoperability Plan
SIGB	Statewide Interoperability Governing Body
SOC	Security Operations Center
SOCB	Security Operations Branch
SOX	Sarbanes Oxley Act
SSD	Solid State Drive
SSO	Single Sign On
TA	Traffic Analysis
TCB	Trusted Computing Base
TFS	Traffic-Flow Security
TOC	Theory of Constraints
TPI	Two-Person Integrity
TQM	Total Quality Management
VART	Vulnerability Assessment and Review Team
VPN	Virtual Private Network
WAN	Wide Area Network
WAP	Wireless Access Point / Wireless Application Protocol
WEP	Wireless Equivalent Privacy
WPA	Wi-Fi Protected Access
WPA-2	Wi-Fi Protected Access II
VPN	Virtual Private Network

NOTES

NOTES

NOTES

NOTES

REFERENCES

The following documents were used in whole or in part as background material in development of this policy:

1. Public Law 107-347 [H.R. 2458], The E-Government Act of 2002, Title III, the Federal Information Security Management Act of 2002, December 2002.

2. CNSSI No. 4016, National Information Assurance Training Standard for Risk Analysts, November 2005.

3. Public Law 104-106, Clinger-Cohen Act of 1996, January 1996.

4. Committee on National Security Systems Instruction (CNSSI) No. 4009, National Information Assurance Glossary.

5. Public Law 108-458, Intelligence Reform and Terrorism Act of 2004, December 2004.

6. Executive Order 13231, Critical Infrastructure Protection in the Information Age, October 2001.

7. Executive Order 13388, Further Strengthening the Sharing of Terrorism Information to Protect Americans, October 2005.

8. Office of Management and Budget Transmittal Memorandum No. 4, Circular A-130, Management of Federal Information Resources, November 2000.

9. Federal Information Processing Standard Publication 200, Minimum Security Requirements for Federal Information and Information Systems, March 2006.

10. Federal Information Processing Standard Publication 199, Standards for Security Categorization of Federal Information and Information Systems, February 2004

11. CNSS Policy No. 6, National Policy on Certification and Accreditation of National Security Systems, October 2005.

12. CNSS Directive No. 502, National Directive on Security of National Security Systems, December 2004.

13. DoD Instruction 8500.2, Information Assurance Implementation, February 2003.

14. CNSSI No. 4014, Information Systems Security Officers National Information Assurance Training Standard, March 2004