



BUSINESS AND IT/IRM TRANSFORMATION PLAN

ENTERPRISE ARCHITECTURE

TABLE OF CONTENTS

- EXECUTIVE SUMMARY13**
- 1.0 INTRODUCTION17**
 - 1.1 Purpose.....17
 - 1.2 Scope17
 - 1.3 Document Overview17
 - 1.4 Associated Documents.....18
- 2.0 BUSINESS AND IT/IRM GOALS AND STRATEGIES AND THE ROLE OF EA.....20**
 - 2.1 Goals of Enterprise Transformation.....20
 - 2.2 Strategies for Enterprise Transformation.....21
 - 2.3 The Role of Enterprise Architecture21
- 3.0 STATE OF HAWAII EA.....23**
 - 3.1 Context for the EA within the State of Hawai‘i’s Government Transformation.....23
 - 3.2 Current State EA Summary23
 - 3.4 Future State EA Summary24
 - 3.5 Transition and Sequencing Plan Summary25
- 4.0 ENTERPRISE BUSINESS ARCHITECTURE (EBA)27**
 - 4.1 EBA Current State27
 - 4.2 EBA Future State28
 - 4.2.1 Business Reference Model (BRM)29
 - 4.2.2 Service Reference Model (SRM)32
 - 4.2.3 Performance Reference Management (PRM)32
 - 4.3 EBA Transition and Sequencing (T&S) Planning Summary.....34
 - 4.3.1 Reengineer Administration Operational Functions35
 - 4.3.2 Replace the Existing Financial and Business Management Solution.....35
 - 4.3.3 Upgrade the IT Infrastructure35
 - 4.3.4 Information Stewards/Leads, Participants, and Stakeholders.....35
 - 4.3.5 Remove Barriers to Information Sharing.....35
 - 4.3.6 Simplify and Secure Information Gathering from Citizens.....35
 - 4.3.7 Ensure Required Services are Delivered.....35
 - 4.3.8 Promote Process Reengineering within the State35
- 5.0 ENTERPRISE INFORMATION ARCHITECTURE (EIA)37**
 - 5.1 EIA Current State.....37
 - 5.2 EIA Future State.....38
 - 5.2.1 Information Management and Usage38
 - 5.2.1.1 Semantic Web.....39

5.2.1.2 Knowledge Management.....	40
5.2.2 EIA Elements	41
5.2.2.1 Common Information Framework.....	41
Enterprise Resource	41
Integration Enabler	42
Information Architecture Levels for Sharing.....	42
Stewardship/Leadership Responsibility and Governance Structure	42
Information Description	42
Information Confidentiality.....	42
Information Integrity	42
Information Availability	43
5.2.2 Conceptual Information Architecture.....	43
5.2.3 Requirements for Information Delivery and Sharing.....	45
Operational Information Management Requirements.....	45
Information Sharing and Delivery Requirements.....	46
Analysis, Visualization, and Reporting Requirements.....	46
5.3 EIA Transition and Sequencing Planning Summary.....	46
5.3.1 Establish the Enterprise Data and Services Administration.....	46
5.3.1.1 Governance Standards and Practices	46
5.3.1.2 Common Data and Services Architecture.....	46
5.3.1.3 Data and Database Administration Standards and Practices.....	47
5.3.2 Establish Enterprise Common Data and Services for the ERP Implementation.....	47
5.3.3 Establish Enterprise Common Data and Services for the Affordable Care Act.....	47
5.3.4 Establish Enterprise Common Data and Services for the Support Services.....	47
5.3.5 Establish Enterprise Common Data and Services for the Core Mission LOBs.....	47
6.0 ENTERPRISE SOLUTION ARCHITECTURE (ESA).....	49
6.1 ESA Current State	49
6.2 ESA Future State.....	50
6.2.1 Vision for the Future State ESA.....	51
6.2.2 Guiding Principles for the Common Solutions Framework	52
6.2.2.1 Enterprise Integration.....	52
6.2.2.2 Use of Industry Standard Application Software within a Services-Oriented Architecture	52
6.2.2.3 Stewardship/Leadership and Governance.....	53
6.2.2.3 Open Source Software and Compliance with Open Standards.....	53
6.2.2.4 Service Orientation, Software Reuse, and Solutions Integration.....	53
6.2.2.5 Standard Enterprise Solution Patterns.....	53
6.2.2.6 The Role of the ESA	54

6.2.3 Conceptual Solutions Architecture	54
6.2.3.1 LOB Services	55
Enterprise Services.....	55
Enterprise Mission Support Services	55
Customer Management Services	56
Business Management Services.....	56
Knowledge Management Services	57
ERP Services	58
Service Management Services.....	60
Enterprise Common Services	61
Data Management Services	61
Analytical Services.....	61
Software Development and Integration Services.....	63
Security Management Services.....	63
Collaboration Services	64
Communication Services	65
Search Services.....	65
Systems Management Services	66
6.3ESA Transition and Sequencing Planning Summary.....	66
6.3.1 Stabilize	66
6.3.1.1 Address Current “Flagship” Opportunities.....	66
6.3.1.2 Legacy Application Solution Upgrades.....	67
6.3.2 Rationalize and Integrate	67
6.3.2.1 Implement ERP System	67
6.3.2.2 Implement Other Enterprise Solutions	68
Enterprise Email System	68
Enterprise Collaboration Solution	68
Enterprise Identity Management Solution	68
Enterprise Dashboard Solution	68
Open Government Solutions	68
Knowledge Management Solution.....	68
Customer Service Solution (Request and Incident Reporting).....	68
Enterprise System Management Solution	68
6.3.2.3 Establish Standard Enterprise Solution Patterns.....	68
Enterprise Web Application Solution Pattern	69
Enterprise Mobile Application Solution Pattern.....	69
Enterprise Data Analytics Application Solution Pattern.....	69
Enterprise Application Integration Web Service Solution Pattern.....	69
Community Application Software “Stores”, Repositories, and Directories.....	69
6.3.2.4 Implement Enterprise Application Integration Services.....	70

Support Services – Security – Identity and Access Management.....	71
Digital Asset Services – Document/Records Management.....	71
Business Analytics Services – Geospatial	71
Business Analytics Services – Dashboard Reporting	71
Back Office Services – ERP	71
Process Automation Services – Workflow.....	71
Process Automation Services – Case Management	71
Customer Services – Event/ Incident/Request Reporting	71
7.0 ENTERPRISE TECHNOLOGY ARCHITECTURE (ETA).....	73
7.1 ETA Current State	73
7.2 ETA Future State	76
7.2.1 Elements of the ETA Future State Vision.....	77
7.2.1.1 Infrastructure: Hawai`i Cloud Computing Centers (HC3).....	77
7.2.1.2 One Network for Hawai`i (OneNet)	78
7.2.1.3 Adaptive Computing Environment (ACE).....	78
7.2.1.4 Information Assurance and Privacy	78
7.2.1.5 Enterprise Operations	78
7.2.1.6 Collaboration and Messaging	78
7.2.1.7 IT Services Management (ITSM) Framework	79
Current State SWOT for ITSM	79
Future State Vision for ITSM	79
Service Management	79
ITSM	80
ITSM Best Practices	81
ETA Transition and Sequencing Planning Summary for ITSM	82
7.2.3 Technology Domain Architecture.....	87
7.2.3.1 Infrastructure Domain	89
Current State SWOT for the Infrastructure Domain	89
Future State Vision for the Infrastructure Domain.....	89
Hosting, Cloud, Data Center Sub-Domain.....	91
Hawai`i Cloud Computing Centers (HC3).....	92
Disaster Recovery Sub-Domain.....	97
Backup - Restore.....	97
Backup – Restore System Behavior	97
Servers and Storage Sub-Domain.....	98
Directory Services Sub-Domain	99
Enterprise Systems Management Sub-Domain.....	100
ETA Transition and Sequencing Planning Summary for Infrastructure Domain	101
Develop and Construct or Build Out a Primary and Backup Data Center Environment.....	101
Define Primary Data Center and DR Strategy Based on Three Alternatives.....	102
Consolidate Data Centers	102

Develop Secondary Data Center (State Owned Facility).....	106
Create Three Island Data Centers (State Owned Facilities).....	109
Migrate Applications from the Current Data Centers to the Primary Data Center	111
Develop a State-Wide Active Directory Services Environment	112
7.2.3.2 Network Domain	113
Current State SWOT for the Network Domain.....	113
Future State Vision for the Network Domain	113
Wired Sub-Domain	116
Wireless Sub-Domain	117
Radio Sub-Domain	117
ETA Transition and Sequencing Planning Summary for the Network Domain.....	118
Design and Implement OneNet.....	118
Provide Video Support	119
Create IP Addressing – Removal of Network Address Translation from Departments	119
Create IP Addressing – Transition from IPv4 to IPv6 Initiative.....	119
Define and Implement Comprehensive Network Security	120
Staffing Network Security Organization	120
Implement Network Life Cycle Methodology	121
7.2.3.3 End User Computing Domain.....	122
Current State SWOT for the End User Computing Domain	122
Future State Vision for the End User Computing Domain	122
Desktop, Laptop, and Mobile Sub-Domain.....	124
User Productivity Software Sub-Domain.....	124
User Presentation Sub-Domain	125
Peripherals Sub-Domain	126
ETA Transition and Sequencing Plan Summary for the End User Computing Domain	126
Create Virtual Desktop Infrastructure	126
Conduct a Pilot Test of VDI.....	127
Define and Implement Next Steps VDI Implementation.....	127
7.2.3.4 Unified Communications Domain	128
Current State SWOT for the Unified Communications Domain.....	129
Future State Vision for the Unified Communications Domain.....	132
Email and Collaboration Sub-Domain.....	133
Voice Sub-Domain	133
Video Sub-Domain	133
Broadcast Messaging Sub-Domain.....	133
Messaging and Social Media Sub-Domain	134
Citizen Communication and Engagement.....	134

ETA Transition and Sequencing Planning Summary for the Unified Communication Domain.....	135
Evaluate Leading Technology Platforms	135
Pilot VoIP	135
Implement VoIP State-wide	135
7.2.3.5 Information Management Domain	137
Current State SWOT for the Information Management Domain	137
Future State Vision for the Information Management Domain	137
Digital Content Management Sub-Domain.....	138
Document Management Sub-Domain.....	139
Data Management Sub-Domain	139
Analytics Sub-Domain	140
Geographic Information System (GIS) Sub-Domain.....	140
ETA Transition and Sequencing Planning Summary for the Information Management Domain.....	140
7.2.3.6 Application Environment Domain	141
Current State SWOT for the Application Environment Domain	141
Future State Vision for the Application Environment Domain.....	141
Application Development and Integration Sub-Domain.....	145
Client Server Applications Sub-Domain.....	145
Web Applications Sub-Domain	146
Mobile Applications Sub-Domain	146
Embedded Systems Sub-Domain.....	146
ETA Transition and Sequencing Planning Summary for the Application Environment Domain	147
Software Engineering Improvement	147
Formalize an Enterprise SDLC Methodology.....	147
Adopt Enterprise SDLC Methodology.....	147
Implement Software Engineering Project Management Improvement.....	147
Implement Software Engineering Continuous Improvement Program.....	147
Implement Software Engineering Mentoring and Consulting Program.....	147
Develop Solution Patterns.....	148
Implement Software Engineering Continuous Improvement Program Operations.....	148
Enterprise Data and Services Standardization and Sharing	148
Implement Software Development Community Ecosystem.....	148
Implement EA Common Information and Solutions Architecture / Framework Administration	148
Create a Common Portal Implementation.....	149
Implement Enterprise Services	149
Migrate Legacy Systems	150
Create Project Registry and Reporting	150
7.2.3.7 Information Assurance and Privacy Domain.....	151
Current State SWOT for the Information Assurance and Privacy Domain.....	151
Future State Vision for the Information Assurance and Privacy Domain.....	152

Security Devices Sub-Domain.....	159
Privacy Sub-Domain	160
ETA Transition and Sequencing Planning Summary for the Information Assurance and Privacy (IA&P) Domain.....	160
Implement Network Data Loss Prevention (NDLP).....	161
Create and Implement IT Security Policy.....	161
Implement Data at Rest (DAR) Encryption	161
Initiate Server Configuration Stability Monitoring.....	161
Initiate Automated Security Configuration Compliance Monitoring and Reporting.....	161
Implement Privacy Program Staffing and Sensitive Information Protection Improvements	161
Implement Enterprise Security Operations Center(s)	161
Implement Computer Incident Response Centers (CIRCs)	162
Implement Enterprise Penetration Testing Capability	162
Common Standards for Protecting Privacy and Other Sensitive Data	162
Implement a Secure Applications Testing Program	162
Implement an Enterprise Identity Management Solution.....	162
Implement Network-Based Network Access Control (NAC)	162
Implement a Secure Wireless Access Solution.....	162
Implement Network End-to-End Encryption Solution.....	163

8.0 ENTERPRISE LEVEL TRANSITION AND SEQUENCING PLAN 166

8.1 Approach Transition and Sequencing Planning.....	166
8.2 Enterprise Level Transition and Sequencing Analysis.....	166
8.2.1 Strategic Portfolio Views.....	167
8.2.1.1 Investment Status by LOB.....	167
8.2.1.2 Enterprise Support Systems and Enterprise Services.....	167
8.2.1.3 ESA and ETA Investments.....	167
8.2.1.4 EA Compliance	167
8.2.1.5 Strategic Value	167
8.3 Specific Projects and Activities.....	167

9.0 CONCLUSION 169

LIST OF FIGURES

Figure 1: Priority Transition and Sequencing Activities.....	15
Figure 2: Evolution of the EA for the State	18
Figure 3: Business and IT/IRM Transformatin Vision for the State of Hawai`i.....	20
Figure 4: Business and IT/IRM Transformation Strategy for the State of Hawai`i	21
Figure 5: State of Hawai`i EA Practice	21
Figure 6: EA Practice Context for the State of Hawai`i.....	23
Figure 7: Gartner's Key Forces that are Shaping IT.....	24
Figure 8: Priority Transition and Sequencing Activities.....	25
Figure 9: State of Hawai`i Future State Enterprise Architecture.....	25

Figure 10: Current State EBA.....28

Figure 11: BRM, SRM, and PRM Components of the EBA.....28

Figure 12: Value Chain for the State of Hawai'i Featured Through the LOB.....29

Figure 13: Detailed BRM and Business Functions within the LOBs30

Figure 14: LOB Leads, Participants, and Stakeholders.....31

Figure 15: SRM Relationship to LOB Business Functions with the Added Dimensions of Enterprise Services.....32

Figure 16: PRM Line of Sight from Input to Business Outcome32

Figure 17: EBA Future State Vision.....33

Figure 18: Business Transformation Strategies Required to Achieve the Future State EBA.....34

Figure 19: Information Management Continuum37

Figure 20: Purpose and Role of the Future State EIA38

Figure 21: The Future State Vision for Information Management and Usage in the State of Hawai'i.....39

Figure 22: Example Protocols for the Semantic Web from W3C40

Figure 23: Focus Areas of the Enterprise Information Architecture.....41

Figure 24: LOBs Providing Support Externally Subject Area Diagram.....43

Figure 25: Representative View Support Area LOB Subject Area Diagram44

Figure 26: Future State Vision for ESA.....51

Figure 27: Current State ETA.....73

Figure 28: ETA Future State Vision for Hawai'i77

Figure 29: Future State Vision for the ITSM Model80

Figure 30: Roadmap for Achieving Future State ITSM87

Figure 31: Technology Architectural Domains and Sub-Domains for the State of Hawai'i88

Figure 32: Data Center Future State View90

Figure 33: Cloud Computing Paradigm93

Figure 34: Proposed Cloud Computing Framework for the State of Hawai'i94

Figure 35: Notional View of Cloud Computing Framework96

Figure 36: Notional View of a Multi-Site Data Center Disaster Recovery Environment97

Figure 37: Notional Representation of Data Center Storage (Gartner Developed).....98

Figure 38: Roadmap to Achieve the Future State for the Infrastructure Domain 112

Figure 39: Conceptual Model of the Network Domain Infrastructure..... 114

Figure 40: OneNet Future State Vision 114

Figure 41: Shared Service Center Vision for the ETA..... 115

Figure 42: Roadmap for Achieving the Future State Network Domain 121

Figure 43: Virtual Desktop Migration 122

Figure 44: Secure Managed Services with Virtual Desktop 123

Figure 45: Roadmap for Achieving the Future State of the End User Computing 128

Figure 46: Notional View of the Future State of Communications 130

Figure 47: Collaboration-as-a-Service – An Essential Future State Element of ETA 131

Figure 48: Roadmap to Future State for the End User Domain 137

Figure 49: Elements of Future State Software Development Environment..... 141

Figure 50: Transition & Sequencing Plan to achieve Future State Software Development Environment 150

Figure 51: Future State Notional View of the Hybrid Cloud Security Architecture 152

Figure 52: Roadmap for Achieving Future State Vision for the Information Assurance and Privacy Domain (1 of 2).....	163
Figure 53: Roadmap for Achieving Future State Vision for the Information Assurance and Privacy Domain (2 of 3).....	164
Figure 54: T&S Process	166
Figure 55: Investment Components.....	167

LIST OF TABLES

Table 1: Current and Future State Summaries by Architectural Layer	14
Table 2: Current State Information Sharing Assessment Results From Two Information Sharing Perspectives.....	37
Table 3: Solution or Applications Assessment Results	49
Table 4: Common Set of Specification Areas for Each Solution Pattern.....	54
Table 5: Customer Management Services Domain Description	55
Table 6: Business Management Services Domain Description	56
Table 7: Knowledge Management Services Domain Description	57
Table 8: ERP Services Domain Description.....	58
Table 9: Service Management Services Domain Description	60
Table 10: Data Management Services Domain Description	61
Table 11: Analytical Services Domain Description.....	61
Table 12: Software Development and Integration Services Domain Description	63
Table 13: Security Management Services Domain Description.....	63
Table 14: Collaboration Services Domain Description	64
Table 15: Communication Services Domain Description	65
Table 16: Search Services Domain Description.....	65
Table 17: Systems Management Services Domain Description	66
Table 18: Opportunities for Flagship Projects to Lay Enterprise Foundations	67
Table 19: Solution Pattern Operating Levels Indicating Evolution of Adoption within the Enterprise.....	69
Table 20: Services-Oriented Operating Levels indicating Evolution of Adoption within the Enterprise.....	70
Table 21: Technical Architecture Domain/Sub-Domain and Current State of Technology Details	74
Table 22: Future State ITSM Best Practices	81
Table 23: ITSM Implementation Actions.....	82
Table 24: Key Criteria and Requirements for the State of Hawai'i Data Center.....	91
Table 25: Future State Characteristics for the Hosting, Cloud, and Data Centers.....	92
Table 26: Hosting, Cloud, and Data Center Sub-Domain Description.....	96
Table 27: Disaster Recovery Sub-Domain Description.....	98
Table 28: Servers and Storage Sub-Domain Description	99
Table 29: Directory Services Sub-Domain Description	99
Table 30: Enterprise Systems Management Sub-Domain Description.....	100
Table 31: Server Closets, Server Rooms, and Data Centers by Department.....	102
Table 32: Estimated Costs to Complete a Data Center Consolidation	103
Table 33: Projects and Initiatives Associated with Data Center Consolidation	103
Table 34: Estimated Costs to Develop Secondary Data Center	106
Table 35: Projects and Initiatives Associated with Secondary Data Center	107
Table 36: Estimated Costs for Development of the Third Data Center	109

Table 37: Projects and Initiatives Associated with Development of the Third Data Center..... 109

Table 38: Estimated Costs to Perform Application Migration..... 111

Table 39: Projects and Initiatives Associated with Application Migration 111

Table 40: Wired Sub-Domain Description 116

Table 41: Wireless Sub-Domain Description 117

Table 42: Radio Sub-Domain Description 118

Table 43: Desktop, Laptop, and Mobile Sub-Domain Description..... 124

Table 44: User Productivity Software Sub-Domain Description..... 124

Table 45: User Presentation Sub-Domain Description 125

Table 46: Peripherals Sub-Domain Description 126

Table 47: Email and Collaboration Sub-Domain Description 132

Table 48: Voice Sub-Domain Description 132

Table 49: Video Sub-Domain Description 133

Table 50: Broadcast Messaging Sub-Domain Description 133

Table 51: Messaging and Social Media Sub-Domain Description 134

Table 52: Citizen Communication and Engagement Sub-Domain Description..... 134

Table 53: Typical LAN Upgrade Costs..... 135

Table 54: Digital Content Management Sub-Domain Description 138

Table 55: Document Management Sub-Domain Description 139

Table 56: Data Management Sub-Domain Description 139

Table 57: Analytics Sub-Domain Description 140

Table 58: GIS Sub-Domain Description 140

Table 59: Application Development and Integration Sub-Domain Description 145

Table 60: Client Server Applications Sub-Domain Description 145

Table 61: Web Applications Sub-Domain Description..... 146

Table 62: Mobile Applications Sub-Domain Description..... 146

Table 63: SWOT for Information Assurance and Privacy Domain 151

Table 64: Security Principles for the Future State 154

Table 65: Security Devices Sub-Domain Description 159

Table 66: Privacy Sub-Domain Description..... 160



EXECUTIVE SUMMARY

EXECUTIVE SUMMARY

This State of Hawai'i's Enterprise Architecture (EA) document is an appendix to the Business Transformation and Information Technology (IT)/Information Resource Management (IRM) Strategic Plan.

The purpose of the EA is to describe the To Be or future state EA that will guide information technology (IT) architectural directions and decisions within the State from this point forward. The EA defines the current state but focuses on the future state vision for each EA element or layer (business architecture, information architecture, solutions architecture, and technology architecture).

In addition, the EA includes a strategic roadmap (Transition and Sequencing [T&S] Plan) of projects and initiatives that will close the gaps between the current state and future state vision. The T&S plan elements are described for each layer of the EA and for the State's lines of business (LOB) and provides details relative to the:



1. ongoing and planned investments and projects that will address the transition between the As Is and To Be states; and,
2. strategic order or sequence of the defined investments or projects to achieve or move the State of Hawai'i closer to the future state vision over the next ten years.

The EA for the State of Hawai'i is a comprehensive description of the enterprise or all IT components of the State (each Department or more specifically each LOB) and the relationships of these components with one another (e.g., services delivered internally and services delivered to residents) as well as the relationships with external entities (e.g., the city and county

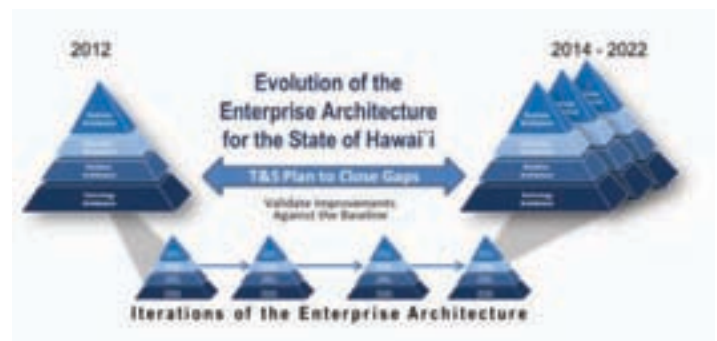


governments, other offices and entities, business partners, and the Federal government). This description includes the goals for the enterprise, business processes, roles, organizational elements or business alignment, business information, solutions or software applications and computer systems, and the IT infrastructure that supports the environment.

Each of the EA layers is defined by taxonomies, diagrams, documents, and models to describe the components and their logical organization of business functions, business capabilities, business processes, people organization, information resources, business systems, software applications, computing capabilities, and the information exchange and communications infrastructure within the enterprise. These are presented in an ever increasing level of detail in an effort to improve the effectiveness and efficiency of the State through:

- an improved organizational structure for service delivery,
- the integration/centralization or distribution of business processes,
- the quality, availability, and timeliness of business information,
- ensuring that IT investments are aligned and justified.

The EA is a living document and will be reviewed at least annually and updated in order to incorporate new technology advancements, as appropriate, and account for the changing needs of the State and especially the changing needs of the LOBs. The population of an EA tool, while underway, will require significant attention to ensure all information associated with the current environment is captured. The T&S Plan in particular will require continual update to account for new initiatives and projects.



¹ Line of Business (LOB) is an approach for defining the activities performed and services provided within the enterprise. The LOBs are subdivided into Enterprise Mission Support Services that are citizen-facing services and Enterprise Common Support Service Areas that are provided internally to support the mission service delivery areas. 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/leadership responsibilities for business service/process performance, information quality and availability, and information system functionality, usability, and integration.

The foundation for EA is the State’s strategy for business transformation. This transformation is defined as part of the New Day Plan and identifies three key elements:

- immediate job growth as Hawai`i’s economy is shifted to a sustainable foundation,
- invest in the education, skills, and well-being of Hawai`i’s people, and
- transform State government into an efficient and effective enterprise.



Stated another way the strategy for transformation includes ensuring that State government is cost-effectively and efficiently managing all resources (e.g., investments, revenues, employees, IT) and delivering services and programs to all stakeholders (e.g., people of Hawai`i, citizens, residents,

businesses, cities, counties, State employees, State government, business partners) in a manner they want/need; and operating in an aligned, streamlined, and integrated manner so that stakeholders’ service expectations and information needs are met in terms of quality, timeliness, reliability, and transparency.

The current state environment for the State of Hawai`i was characterized in the Final Report published in 2011 and the key elements are identified by architectural layer in Table 1. In the future, each of the items identified for the current state architectural layers must undergo a transformation in order for the State of Hawai`i to more effectively and efficiently deliver services to people of Hawai`i, the citizens, and other stakeholders. The transformation will occur by addressing every action and activity (e.g., business processes, IT investment decisions, information use and utility, taking advantage of new less expensive hardware, software, and data management solutions) from an enterprise perspective. A summary of the future state vision by architectural layer is also summarized in Table 1.

Table 1: Current and Future State Summaries by Architectural Layer


Current State by Architectural Layer	Future State by Architectural Layer
<ul style="list-style-type: none"> • Enterprise Business Architecture (EBA) - organized in a siloed, bottom-up approach with only pockets of Departments actually having or practicing EBA and primarily evolved due to the manner in which funding is provided at the program level and by default for IT. 	<ul style="list-style-type: none"> • Enterprise Business Architecture (EBA) - composed of a series of integrated value streams across the State’s Departments that can be further developed by LOB and by reference models. By using LOB and reference models to define the enterprise moves or transitions the State away from the siloed approach of functional processes and disconnected IT projects to an integrated environment
<ul style="list-style-type: none"> • Enterprise Information Architecture (EIA) – characterized by a general lack of information sharing across Departments and organizations within the State even though some exceptions exist. 	<ul style="list-style-type: none"> • Enterprise Information Architecture (EIA) – characterized by information and data that are recognized/acknowledged by everyone as a statewide asset and are managed and shared effectively among all State organizations
<ul style="list-style-type: none"> • Enterprise Solution Architecture (ESA) - characterized by: few, true statewide solutions; large numbers of Department-specific applications have proliferated within the State; and, need to “right-size” the State’s applications portfolio. 	<ul style="list-style-type: none"> • Enterprise Solution Architecture (ESA) – features a dynamic mobile integration architecture that responds rapidly to change and delivers quality information from trusted sources to all stakeholders.
<ul style="list-style-type: none"> • Enterprise Technology Architecture (ETA) - decentralized because the technical infrastructure supports a very fragmented ESA and EIA. 	<ul style="list-style-type: none"> • Enterprise Technology Architecture (ETA) – enables rapid deployment of new services to LOBs, employees, and residents and fully supports the EBA, EIA, and ESA.

As the current state was analyzed and the future state was defined, a number of high priority transition projects or initiatives were identified across the four architectural layers. Figure 1 identifies each of the priority items and its associated architecture layer(s).

The business services provided within each LOB scope are also defined within the EA in terms of the future state vision for a comprehensive IT solutions architecture to deliver all required business services and functions and the investment initiatives required to achieve the targeted future state for each of the LOB segments is also included provided.

Of particular note, this version of the EA for the State of Hawai'i has addressed business analysis and planning at two levels: 1) the state-wide enterprise which established the LOBs, and 2) the individual LOB business segment architectures and two priority segments Health IT and the ERP. The primary accomplishment of this planning function and all associated meetings with LOB leads has been the building of cultural momentum for enterprise solutions and consolidated investment planning. Additional opportunities will exist in the years ahead for specific LOB Business Segments to be analyzed in more detail to expand and provide additional architectural detail to other priority areas. The LOBs, Health IT, and the ERP business segments are included in Appendix A - Line of Business Segment Architecture Transformation.

The projects and initiatives required



Priority Future State Areas	Architectural Layer
★ OneNet - Enterprise Services Network	ETA
★ Adaptive Computing Environment	ETA
★ Shared Services Center	ETA
★ Information Assurance, Security/Privacy	EIA, ESA, ETA
★ Email/Collaboration	ESA, ETA
★ Open Gov	EIA
★ Mobile Technologies	ESA, ETA
★ Tax Modernization	ESA
★ ERP	ESA
★ Health IT	ESA

Figure 1: Priority Transition and Sequencing Activities

to move the State from the current to the future state environment for each EA layer and by LOB are described at a high level as part of the T&S planning summaries by architectural layer and in Appendix A. Each project and initiative is then further described as a business case and with budgetary detail (i.e., description of specific activities and tasks associated with the initiative or activity; hours to perform the task by fiscal year; labor costs; equipment and hardware costs; estimated lease costs, and any other associated costs) as part of an

Appendix B - Project Charters.

This document is intended for IT practitioners to use when planning technology directions (i.e., development, modernization, enhancement (D/M/E); operations and maintenance (O&M) of existing technology/steady state (SS); or retirement) within the LOB

and Departments. The document also supports the evaluation of technology reviews/requests/approvals by the Chief Information Officer (CIO), Office of Information Management and Technology (OIMT), Department leadership and IT management, Executive Leadership Council (ELC), and CIO Council (CIOC) and IT Steering Committee.



1.0 INTRODUCTION

1.0 INTRODUCTION

1.1 PURPOSE

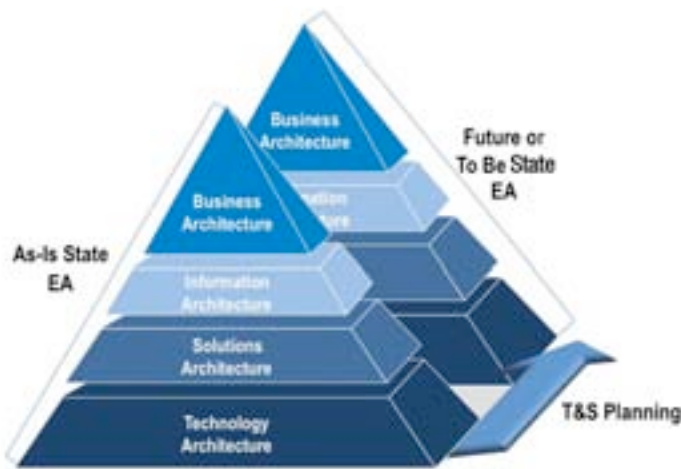
The purpose of the State of Hawai'i's Enterprise Architecture (EA) document is to describe the To Be or future state EA that will be guide information technology (IT) architectural decisions within the State from this point, and provide a strategic roadmap (Transition and Sequencing [T&S] Plan) to close the gaps between the As Is or current state and the To Be vision. This document is an appendix to the *Business Transformation and Information Technology (IT)/Information Resource Management (IRM) Strategic Plan*.



1.2 SCOPE

The EA for the State of Hawai'i includes a description of the current or As Is state as well as the future or To Be state for each EA element or layer (business architecture, information architecture, solutions architecture, and technology architecture). In addition, a transition and sequencing (T&S) plan has been developed and is included for each layer of the EA and the State's lines of business (LOB). The T&S Plan provides details relative to the:

1. ongoing and planned investments and projects that will address the transition between the As Is and To Be states; and,
2. strategic order or sequence of the defined investments or projects to achieve or move the State of Hawai'i closer to the future state vision over the next ten years.



1.3 DOCUMENT OVERVIEW

The EA for the State of Hawai'i is a comprehensive description of the enterprise or all IT components of the State (each Department or more specifically each LOB) and the relationships of these components with one another (e.g., services delivered internally and services delivered to residents) as well as the relationships with external entities (e.g., the city and county governments, other offices and entities, business partners, and the Federal government). This description includes the goals for the enterprise, business processes, roles, organizational elements or business alignment, business information, solutions or software applications and computer systems, and the IT infrastructure that supports the environment.

Each of these components is defined in terms of the As Is and To Be state. Taxonomies, diagrams, documents, and models are included to describe the components and their logical organization of business functions, business capabilities, business processes, people organization, information resources, business systems, software applications, computing capabilities, and the information exchange and communications infrastructure within the enterprise. These are presented in an ever increasing level of detail in an effort to improve the effectiveness and efficiency of the State through:

- an improved organizational structure for service delivery,
- the integration/centralization or distribution of business processes,
- the quality, availability, and timeliness of business information, and
- ensuring that IT investments are aligned and justified.

This document also describes the gap closure activities or transition projects, through a T&S Plan, that are required to move the current or As Is state of the EA (and its four layers) to the To Be or future state EA. Further, these gap closure activities are sequenced in terms of timing and dependencies.

The creation of the EA has been facilitated by engaging stakeholders (i.e., Departmental CIOs, IT managers, business entities within Hawai'i, citizens, residents, business partners, other governmental entities) in the development and review of each component. This engagement has validated the As Is state and ensured the To Be vision is aligned with and responsive to the needs of the enterprise or State going forward.

The EA is a living document that will be maintained and updated at least annually and more frequently (depicted in Figure 2), as required. The intended audience for this document is any individual involved in decision making about IT within the State including the Chief Information Officer (CIO), Office of Information Management and Technology (OIMT), Department leadership and IT management, Executive Leadership Council (ELC), and CIO Council (CIOC) and IT Steering Committee.

This document along with the EA Methodology is appendices to the Business Transformation and Information Technology (IT) Information Resource Management (IRM) Strategic Plan.

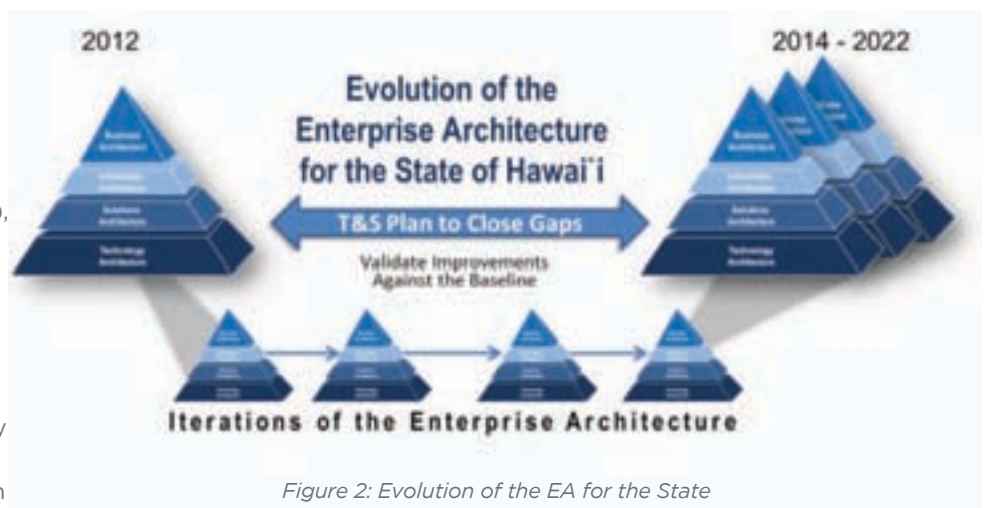


Figure 2: Evolution of the EA for the State

² Line of Business (LOB) is an approach for defining the activities performed and services provided within the enterprise. The LOBs are subdivided into Enterprise Mission Support Services that are citizen-facing services and Enterprise Common Support Service Areas that are provided internally to support the mission service delivery areas. 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/leadership responsibilities for business service/process performance, information quality and availability, and information system functionality, usability, and integration.

1.4 ASSOCIATED DOCUMENTS

The associated documents listed below are those documents referenced by or related to this document. This includes guidance from State entities as well as reference documents from the Federal and other State governments.

- State of Hawai`i, Business Transformation Strategy and IT/IRM Strategic Plan, 2012 (referred to hereafter as the "Strategic Plan")
- State of Hawai`i, Governance Methodology and Organizational Charters, 2012
- State of Hawai`i, Portfolio Management (Pfm) Methodology, 2012
- State of Hawai`i, Enterprise Architecture (EA) Methodology, 2012
- OIMT, Project Management Methodology, 2012
- Baseline of Information Management and Technology and Comprehensive View of State Services (known hereafter as the "Final Report") prepared by SAIC
- Federal Segment Architecture Methodology (FSAM)
- Federal Enterprise Architecture (FEA), Business Reference Model (BRM)
- State of Hawai`i, Business Process Reengineering (BPR) Methodology, 2012
- OIMT, Project Management Methodology, 2012
- State of Hawai`i, Administrative Directive Number 11-02, 2011
- DOH Business Services and Data Systems Service Oriented Architecture (SOA) Diagrams and the Public Health Domain Matrix for IT Systems and Initiatives
- World Wide Web Consortium, <http://www.w3.org/2001/sw/>



2.0

**BUSINESS AND IT/IRM GOALS
AND STRATEGIES AND THE ROLE OF EA**

2.0 BUSINESS AND IT/IRM GOALS AND STRATEGIES AND THE ROLE OF EA

In Fiscal Year (FY) 2012, 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 CIO, the appointment of a Business Transformation Executive, and the establishment of OIMT. These executives and this organization were given

the mandate to lead the overall transformation. In addition, the CIO was tasked by the Legislature to create the State's Strategic Plan. To support the implementation of the Strategic Plan, the need for an EA and its implementation as a practice was identified in order to give structure and direction to the IT transformation efforts.

2.1 GOALS OF ENTERPRISE TRANSFORMATION



The foundation for EA is the State's strategy for business transformation. This transformation is defined as part of the New Day Plan and identifies three key elements:

- immediate job growth as Hawai'i's economy is shifted to a sustainable foundation,
- invest in the education, skills, and wellbeing of Hawai'i's people, and
- transform State government into an efficient and effective enterprise

Stated another way the strategy for transformation includes:

- ensuring that State government is cost effectively and efficiently managing all resources (e.g., investments, revenues, employees, IT) and delivering services and programs to all stakeholders (e.g., people of Hawai'i, citizens, residents, businesses, cities, counties, State employees, State government, business partners) in a manner they want/need; and
- operating in an aligned, streamlined, and integrated manner so that stakeholders' service expectations and information needs are met in terms of quality, timeliness, reliability, and transparency.

To achieve business transformation a set of goals or business outcomes have been defined along with supporting information resource management (IRM) and IT goals. Each of these is discussed in detail in the Strategic Plan and is summarized in Figure 3.

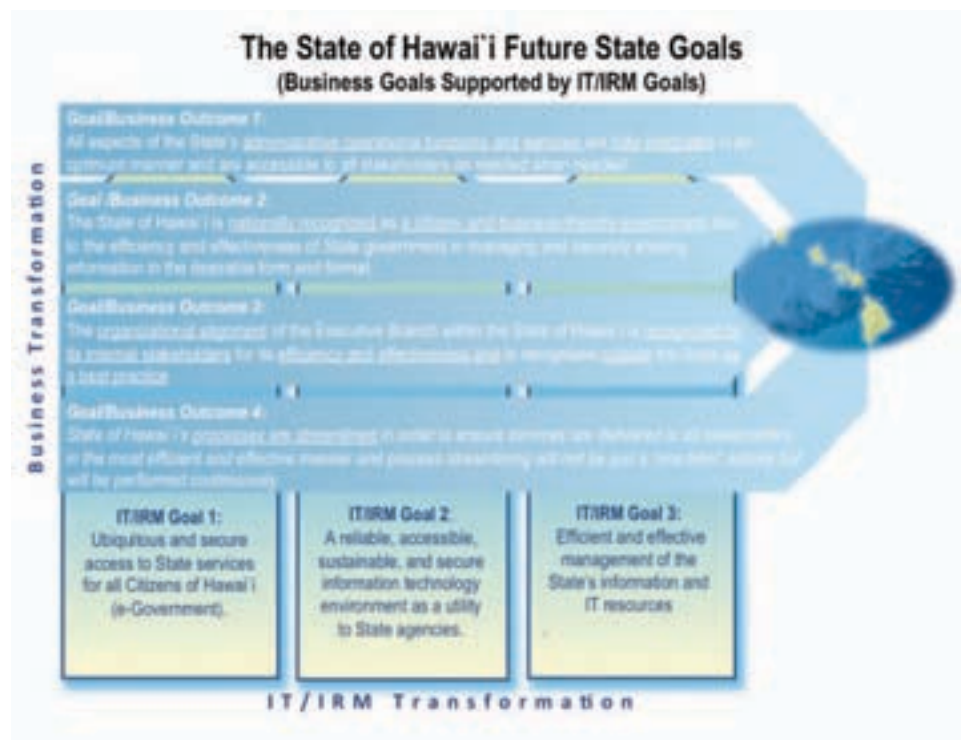


Figure 3: Business and IT/IRM Transformation Vision for the State of Hawai'i

2.2 STRATEGIES FOR ENTERPRISE TRANSFORMATION

To achieve the enterprise transformation goals, a number of strategies have been defined as part of the Strategic Plan. These strategies are aligned to each business transformation and IRM/IT goal. Figure 4 highlights these strategies for achieving the defined transformation goals.

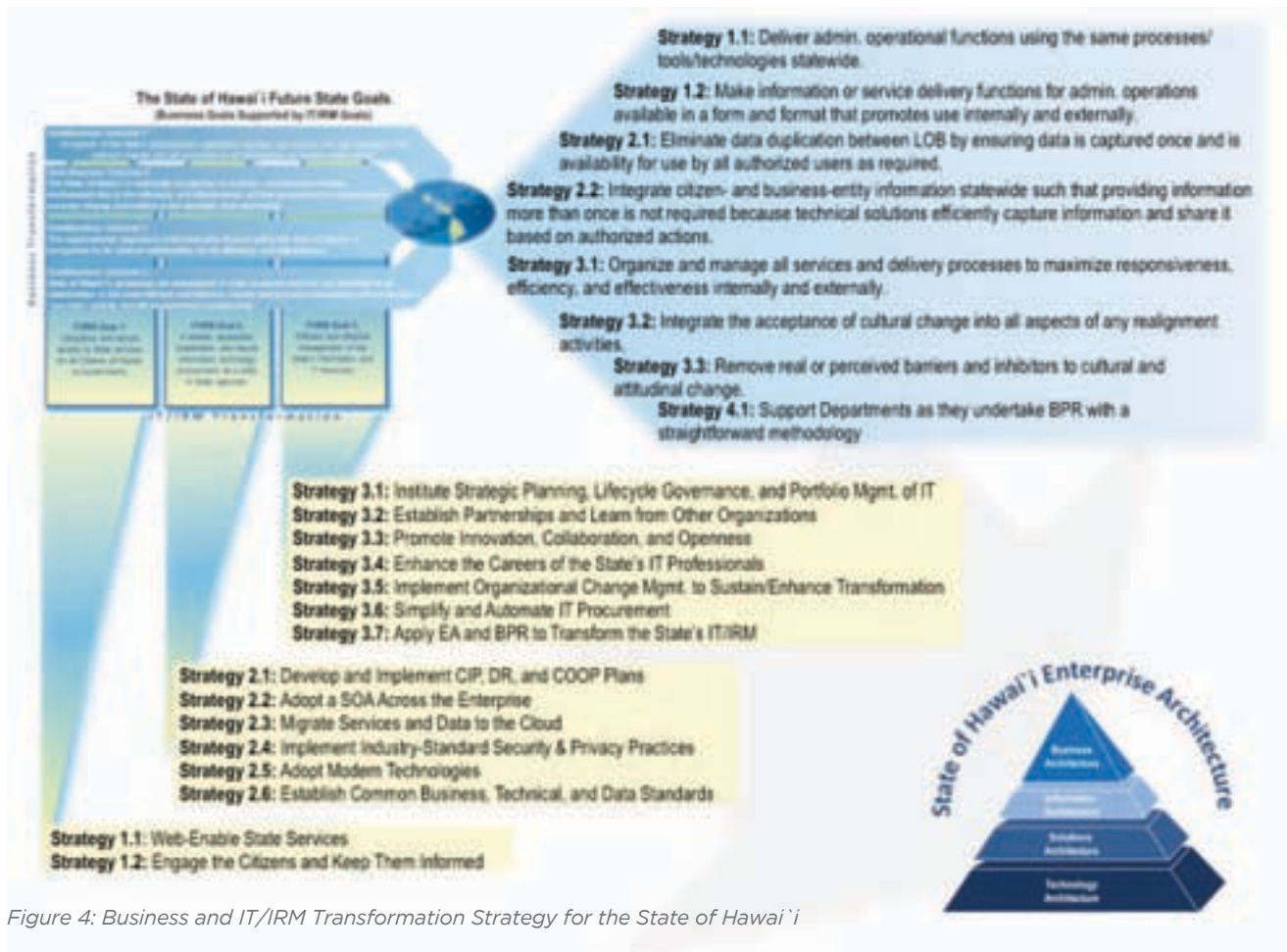


Figure 4: Business and IT/IRM Transformation Strategy for the State of Hawai'i

2.3 THE ROLE OF ENTERPRISE ARCHITECTURE

With the foundation of EA established by the business transformation and IRM/IT goals and strategies, the role of EA is to describe the As Is and to define the To Be architecture for the enterprise from

four perspectives or architectural layers: business, information, solution, and technical. Figure 5 illustrates the elements of the EA practice.

The EA also serves as the recipe for aligning resources to improve business performance and helps the State and each Department better execute their

core missions. In addition the EA defines a plan for transitioning from the current state to the desired future state. The State of Hawai'i, Enterprise Architecture Methodology describes the role and elements of EA in greater detail. To summarize, Figure 5 illustrates the EA practice as it is defined for the State of Hawai'i.



Figure 5: State of Hawai'i EA Practice



3.0 STATE OF HAWAII EA

3.0 STATE OF HAWAII EA

3.1 CONTEXT FOR THE EA WITHIN THE STATE OF HAWAII'S GOVERNMENT TRANSFORMATION

The EA helps organize, prioritize, achieve the future state for the IT environment, and then supports the management of the IT environment 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 (annotated by number in Figure 6) 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. The EA and projects, defined within the T&S Plan that are approved, funded, and initiated within the proposed sequence and timeframes. These include Business Process Reengineering (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 6 provides an overview of this integration and other functions, practice, or program areas.

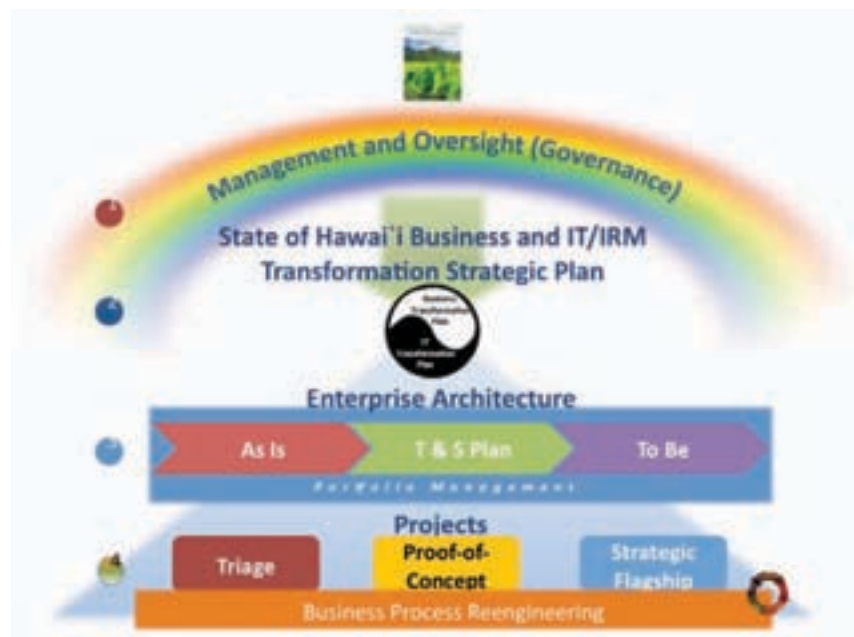


Figure 6: EA Practice Context for the State of Hawaii

Finally, once specific projects are initiated, the EA future state guidance in the information, solutions, and technical architecture layers is used as a crosswalk to the Systems Development Life Cycle (SDLC) within the context of an EA governance and change management process.

3.2 CURRENT STATE EA SUMMARY

The current state or As Is environment for the State of Hawaii is characterized in the Final Report published in 2011 and is further described in the remainder this document. As a summary of the current state, the following provides a high-level summary of the As Is for each architectural layer:

- Enterprise Business Architecture (EBA) - organized in a siloed, bottom-up approach with only pockets of Departments actually having or practicing EBA and primarily evolved due to the manner in which funding is provided at the program level and by default for IT.
- Enterprise Information Architecture (EIA) - characterized by a general lack of information sharing across Departments and organizations within the State even though some exceptions exist.
- Enterprise Solution Architecture (ESA) - characterized by: few, true statewide solutions; large numbers of Department-specific applications have proliferated within the State; and, need to “right-size” the State’s applications portfolio.
- Enterprise Technology Architecture (ETA) - decentralized because the technical infrastructure supports a very fragmented ESA and EIA.

A cornerstone of any EA program is an EA and Portfolio Management (PfM) integrated tool suite and an EA Repository. These tools will contain details regarding each of the current application software solutions and planned investments. The EA Repository will be the common information store for all digital data and content behind the EA program.

The baseline of the “As Is” or current state was initially populated in an Enterprise Alignment Database (EAD). The EAD currently contains detailed information regarding the State’s over 200 business services, over 700 application software systems, server inventory of the three data centers and over 20 server rooms, and approximately 6400 different technology product types used within the State. Currently, a new EA and PfM tool suite is being acquired and implemented for the State, and all baseline data will be moved into a new EA repository database. This tool suite and integrated repository will provide a foundation for all future planning and system and technology investment decisions. The information made available via the tool suite will support making informed decisions regarding how to manage and move IT forward in the State through the:

- analysis of options relative to IT transformation activities;
- development of the strategic plan;

3.4 FUTURE STATE EA SUMMARY

In the future, each of the items identified for the current state must undergo a transformation in order for the State of Hawai`i to more effectively and efficiently deliver services to its constituents. The transformation will be carried out by addressing every action and activity (e.g., business processes, IT investment decisions, information use and utility, taking advantage of new less expensive hardware, software, and data management solutions) from an enterprise perspective. As a summary of the future state, the following provides insight into the To Be vision for each architectural layer:

- Enterprise Business Architecture (EBA) - composed of a series of integrated value streams across the State’s Departments that can be further developed by LOB and by reference models. By using LOB and reference models to define the enterprise moves or transitions the State away from the siloed approach of functional processes and disconnected IT projects to an integrated environment.

- Enterprise Information Architecture (EIA) – characterized by information and data that are recognized and acknowledged by everyone as a statewide asset and are managed and shared effectively among all State organizations.
- Enterprise Solution Architecture (ESA) – features a dynamic mobile integration architecture that responds rapidly to change and delivers quality information from trusted sources to all stakeholders.
- Enterprise Technology Architecture (ETA) – enables rapid deployment of new services to LOBs, employees, and residents and fully supports the EBA, EIA, and ESA.

The future state vision described by the previous list is supported by Gartner’s most recent list of the four forces that are shaping the future of IT (Figure 7) and within their four top predictions:

- By 2015, mobile application development (AD) projects targeting smartphones and tablets will outnumber native PC projects by a ratio of 4-to-1.



- definition of a governance approach;
- creation of training plans for staff;
- resourcing of projects; and,
- identifying and prioritizing IT investments.

- By 2015, 35% of enterprise IT expenditures for most organizations will be managed outside the IT department’s budget.
- Through 2015, more than 85% of Fortune 500 organizations will fail to effectively exploit big data for competitive advantage.



Figure 7: Gartner’s Key Forces that are Shaping IT

3.5 TRANSITION AND SEQUENCING PLAN SUMMARY

As the current state was analyzed and the future state was defined, a number of high priority transition projects or initiatives were identified across the four architectural layers. Figure 8 identifies each of the priority items and its associated architecture layer (s).

Priority Future State Areas	Architectural Layer
☆ OneNet - Enterprise Services Network	ETA
☆ Adaptive Computing Environment	ETA
☆ Shared Services Center	ETA
☆ Information Assurance, Security/Privacy	EIA, ESA, ETA
☆ Email/Collaboration	ESA, ETA
☆ Open Gov	EIA
☆ Mobile Technologies	ESA, ETA
☆ Tax Modernization	ESA
☆ ERP	ESA
☆ Health IT	ESA

Figure 8: Priority Transition and Sequencing Activities

Figure 9 illustrates the future state EA and the priority items associated with each EA layer.



Figure 9: State of Hawai'i Future State Enterprise Architecture.

The following sections describe the EA for the State of Hawai'i within the four architectural layers. For each layer the current state is described and the target future state is defined. Additional supporting detail regarding the architectures is maintained in the State's EA repository. These priority items are discussed throughout the EA and are highlighted by the assigned icons identified in Figure 8.



4.0 ENTERPRISE BUSINESS ARCHITECTURE (EBA)

4.0 ENTERPRISE BUSINESS ARCHITECTURE (EBA)

The Enterprise Business Architecture (EBA) is essentially a model of the components within the State that enable the execution of its mission. Key concepts modeled within the EBA or the characteristics of the EBA's structure include:

- Business processes (i.e., value streams or value chains) that create business outcomes.
- Business outcomes that are organized and managed as Lines of Business (LOB) that involve both services to end customers (i.e. residents) and services provided internally as enabling or supporting the service delivery to residents.
- Business functions and sub-functions that further define the LOBs.
- Organizations, governance formality, and the interaction of the organizations responsible for executing business processes and creation of business outcomes.
- Business outcomes and value chains which are measurable through delivered value or quality or throughput.



The following sections describe the As Is or current state, the To Be or future state, and the activities or projects required to close the gaps for the EBA.

4.1 EBA CURRENT STATE

The current state of the EBA for the State of Hawai'i is organized in a siloed, bottom-up fashion with only a few Departments actually having or practicing EBA. This current state has evolved primarily due to the manner in which funding is provided for programs. The Departments with larger overall funding also have a larger percentage of funding to dedicate to IT and IT maturity. Larger organizations, usually referred to as the "haves", such as the Department of Education and Department of Health, are in this category. IT funding is often tied to an external program from a federal or special project, Departments with large exposure to federal funding are more likely to have some type of EBA.

While the Departmental EBAs might not be considered "formal", they do reflect many of the characteristics of a working EBA. Given the disjointed nature of federal funding to a State as well as special projects often the resulting EBA and related IT spending does not take the holistic view that a mature EBA would provide.

Another factor associated with the current state of the EBA, is the fact that the State has not (until July 2011) had a dedicated CIO or a chartered and tiered governance process. While the larger Departments such as Education and Health have a Departmental CIO and some remnants governance, the interactions and opportunities to work in a single strategic direction across the State have been limited. This lack of a State CIO and governance has led to a lack of a single vision for the State's IT organizations to move towards.

To offset the siloed and high variability in IT maturity the resulting business architecture from an organizational view has historically been managed by each Department through their Administrative Services Office (ASO). The ASOs in turn have worked to minimize or overcome the lack of an enterprise approach relative to:

- How business is conducted and services are delivered effectively and efficiently within the State (i.e., EBA),

- How information is required and shared across the State (i.e., EIA), and

- How IT solutions and their supporting infrastructure technology is planned, funded, created, integrated, deployed, maintained, and retired to maximize business outcomes (i.e., ESA and ETA).

The lack of a statewide EBA has resulted in systems and processes that are not compatible and this often leads to manual entry, data errors, delays in service, duplicative systems and infrastructure, and aging technology that translates to escalated overall IT costs for the State. While many Departments feel they may be optimizing their IT spending it has been shown that this lack of an enterprise view provided by the EBA leads to greater overall IT spending for the State. Figure 10 illustrates the disjointed, inefficient, cost heavy, and fragmented service delivery environment across the State.

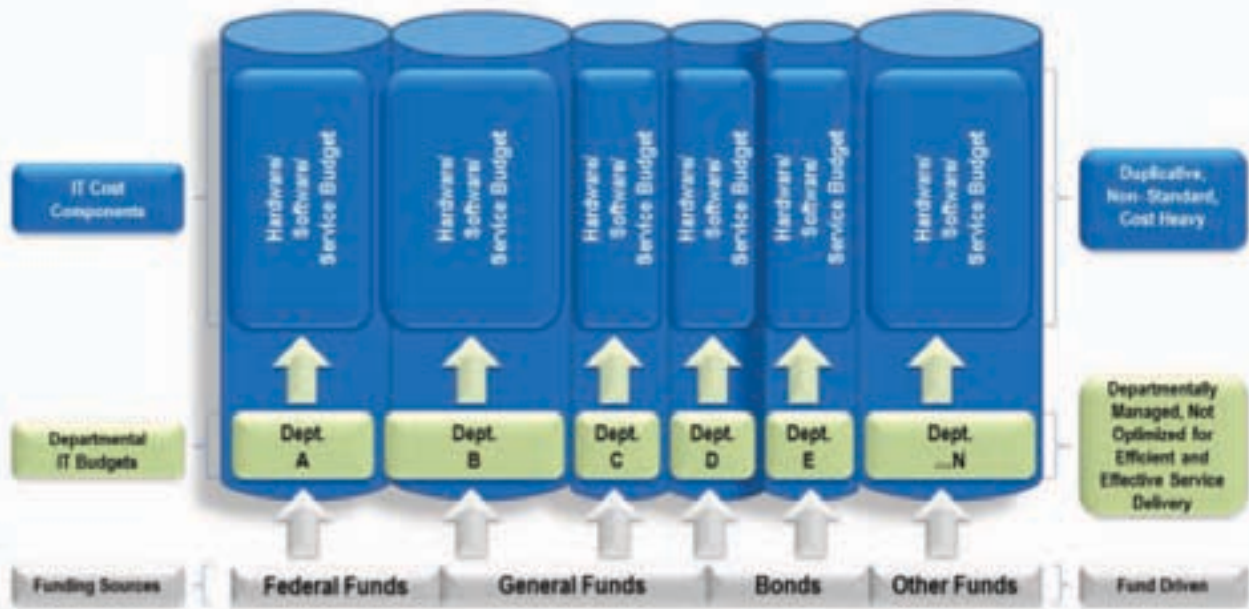


Figure 10: Current State EBA

4.2 EBA FUTURE STATE

The defined future state of the EBA is composed of a series of integrated value streams across the State's Departments that can be further developed by LOB and State of Hawai'i tailored reference models. By using LOB and tailored reference models to define the enterprise, the State will be positioned to move in an organized manner away from the siloed approach of repetitive processes, duplicated information, and non-integrated IT solutions and infrastructure or technology.

The EBA future state, depicted in Figure 11, provides a view of:

- LOBs that provide support services externally to residents and other stakeholders and the LOBs that provide required support to the mission delivery LOBs; defined within the Business Reference Model (BRM);
- cross-cutting or enterprise solutions that are required for the State to more effectively provide services and conduct business defined within the Service Reference Model (SRM); and

- quantitative indicators, defined within the Performance Reference Model (PRM), to help determine what success means in the future state and whether the State is achieving success or not.

The following sections discuss the BRM, SRM, and PRM in more detail.

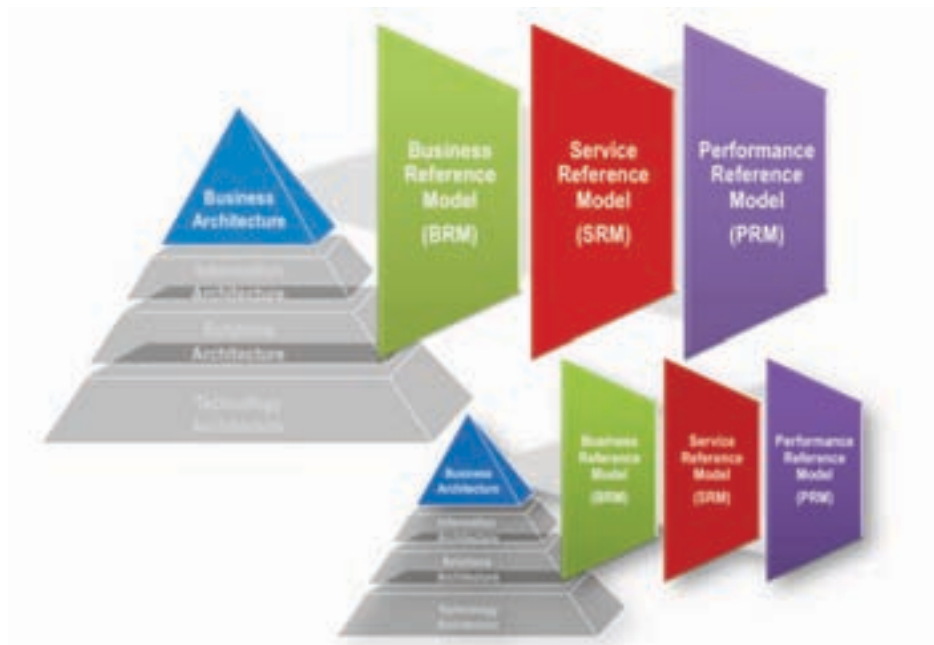


Figure 11: BRM, SRM, and PRM Components of the EBA

4.2.1 BUSINESS REFERENCE MODEL (BRM)

The BRM is the first step in:

1. identifying the opportunities for horizontal integration of IT based on mission support to residents and common services that support mission delivery,
2. improving the management of technology investments for the entire State using an enterprise portfolio perspective for selection of IT spending, and
3. providing a critical building block in defining the complete EA.

The BRM provides an organized, hierarchical construct for describing the day-to-day business of the State of Hawai`i's Executive Branch. While many tools exist for describing organizational constructs - organization charts, location maps, etc. - the BRM represents the business or services performed by Departments from a functional perspective. The various functional perspectives are outlined as individual LOBs with further detail given as sub-functions or services of each individual LOB.

The BRM represents the link between the LOB and the final recipient of the LOBs' services. This is the beginning point for the value chain development for the State and is a representation of how the business of the State is performed functionally.

Figure 13 represents a summary and detailed level a representation of the BRM and business functions within each LOB. While many of the LOBs identified in Figure 13 correlate directly to a Department within the State, the LOB is not intended to represent a single Department. In most cases, a LOB will have business functions that are shared across multiple Departments. For example, the LOB for public health includes many of the business functions provided by the Department of Health (DOH) for the State, many of these functions for public health are shared with other Departments such as the Department of Education (DOE) which is responsible for the health of students while attending school. This is an example of how a single Department within the State is identified and designated as the lead for the LOB for public health while other Departments within the State are identified as being a LOB participant while still others are designated as stakeholders in the policy and other activities the LOB provides. The public

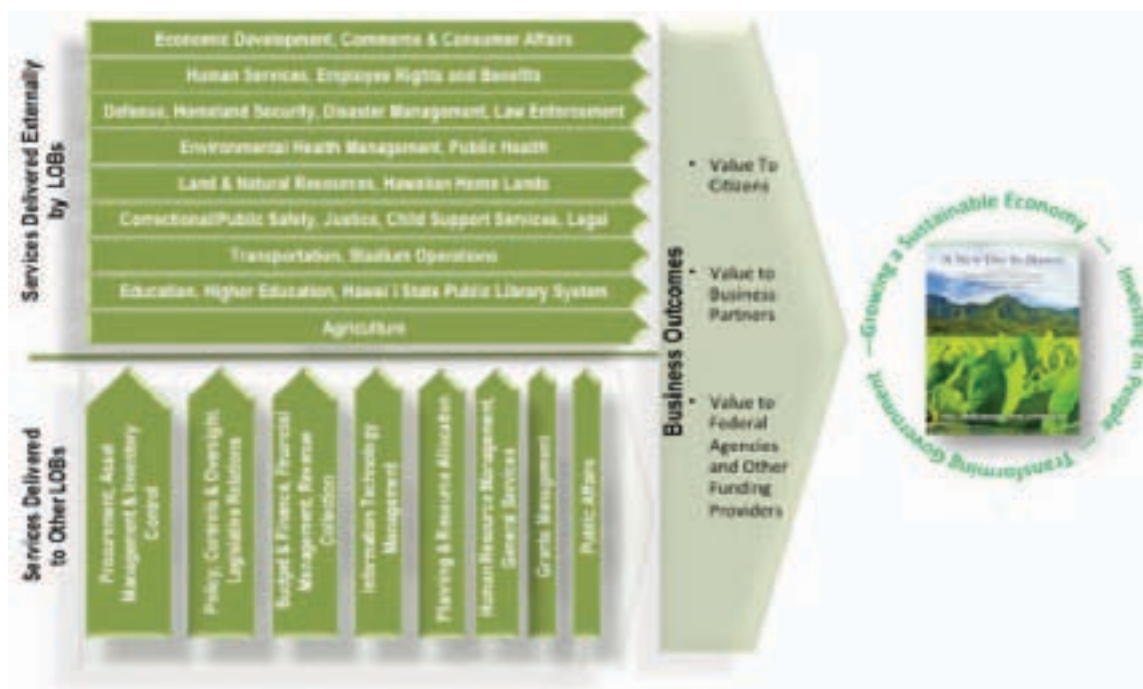


Figure 12: Value Chain for the State of Hawai`i Featured Through the LOB

The State's EBA and its accompanying newly defined BRM is the first layer of the State's EA and it is where analysis starts for other layers of the EA in terms of information, service components, solutions, and technology. Figure 12 depicts the BRM from a summary perspective and defines the high level business outcomes or value chain for the State as a whole. Additional definitions and details regarding each of the functions and sub-functions and functional interfaces or dependencies within these business services will ultimately be documented in the EA repository.

health example also illustrates how the BRM's enterprise view supports the business of government and supports the integration of IT. Without the BRM view, the value chain that delivers public health services to the residents of Hawai`i would be narrower and lose the perspective of the LOB participants and stakeholders.



Figure 13: Detailed BRM and Business Functions within the LOBs

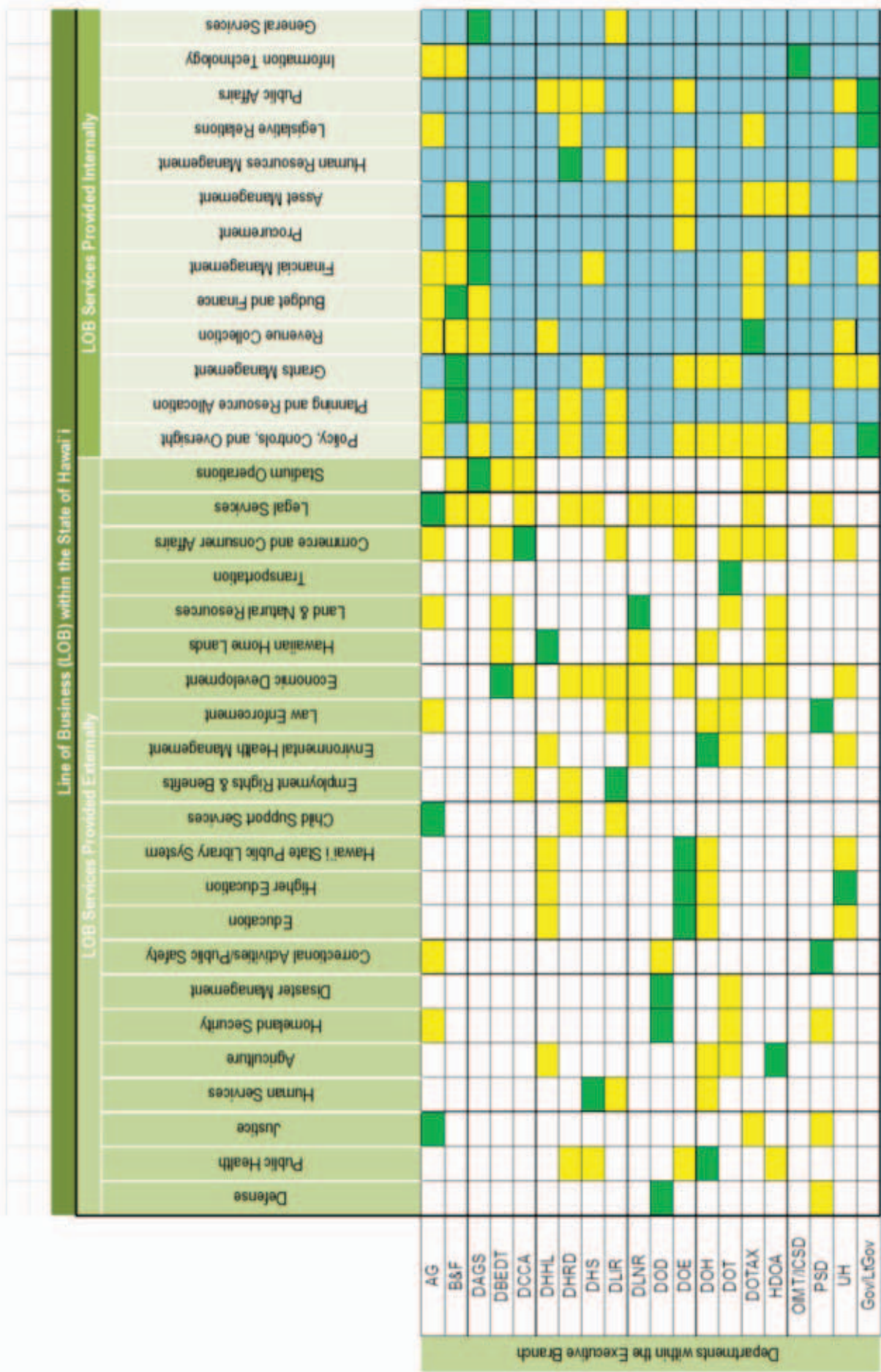


Figure 14: LOB Leads, Participants, and Stakeholders

Figure 14 depicts LOB lead with an identified Department, the relationships of other Departments with the LOB, and also the stakeholders for a LOB. The boxes marked as bright green depict Department that has been designated as the LOB lead with yellow shading indicating the Department(s) interest or information needs in the LOB (LOB participant). Blue indicates stakeholders for the LOB by Department.

4.2.2 SERVICE REFERENCE MODEL (SRM)

The next element of the future state EBA represents the enterprise services (those required across the State) and will be a key component to any direction for and investment in IT for the State and its Departments or LOBs. Enterprise services represent a business-driven approach for classifying the required business functions that are common across multiple LOBs (e.g., those functions described in EBA current state as being performed by the ASOs in each Department).

These enterprise services are described in the Service Reference Model (SRM) and represent horizontal service components that span across multiple LOBs. Figure 15 depicts how the SRM and specifically the enterprise services relate horizontally to the LOBs.

The SRM is organized across horizontal service areas (independent of the business functions) and provides a leverage-able foundation for reuse of information, applications, or solution components, and technologies.

The BRM and SRM components are rolled forward into the ESA and further detailed. All BRM functional components are translated into LOB services within the ESA, and the horizontal

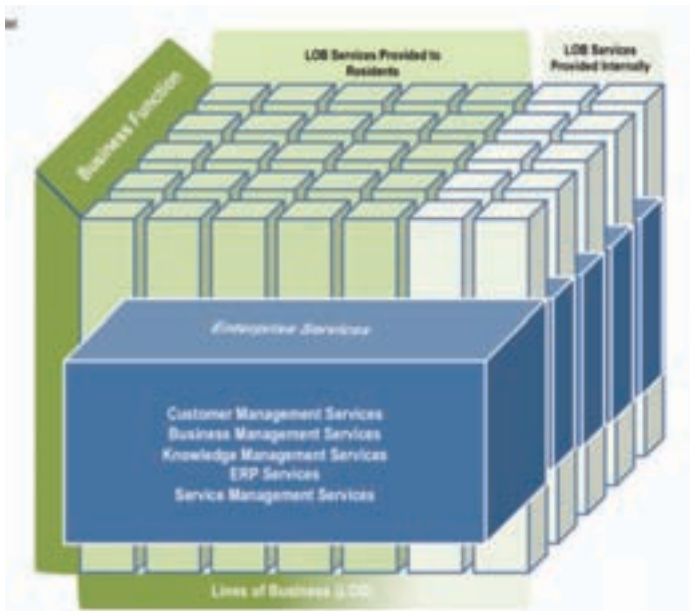


Figure 15: SRM Relationship to LOB Business Functions with the Added Dimensions of Enterprise Services

or cross-cutting SRM services are translated into shared or common enterprise services; following an “everything is a service” paradigm which is explained further below.

The SRM is a critical piece of the State’s EA due to the common services and activities associated with the SRM. These common activities and processes are where IT for the State will focus development efforts for common information, common data, common technology, and common infrastructure. It is in the SRM that IT investment has the highest Return on Investment and provides the greatest impact to automation of State services and processes. The SRM is where investment of IT starts for the State’s CIO.

4.2.3 PERFORMANCE REFERENCE MANAGEMENT (PRM)

The PRM is designed to clearly identify and illustrate the cause-and-effect relationship or “line of sight” between inputs, outputs, and outcomes. PRM is built upon “line of sight” relationships and is critical for the executive leadership, IT management, project managers, and other key stakeholders to understand how, and to what extent key inputs enable progress toward desired business outcomes regarding mission achievement and delivery of services to residents. The PRM captures and reports, based on the “line of sight”, how value is created for each LOB as inputs impact outcomes. Guiding the entire PRM are the

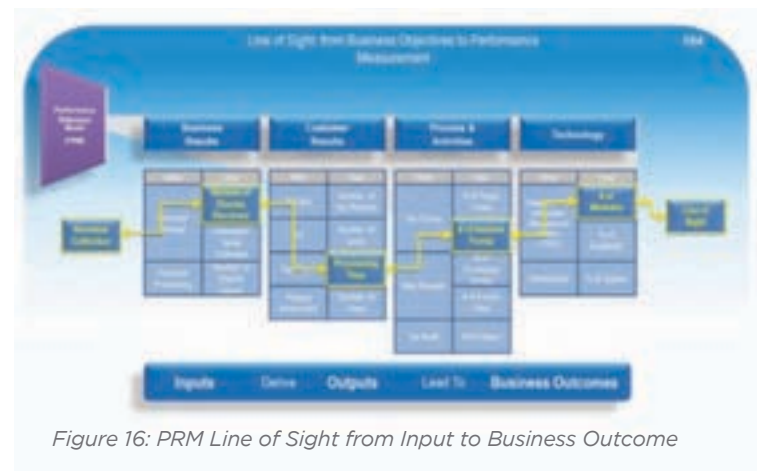


Figure 16: PRM Line of Sight from Input to Business Outcome

“strategic outcomes” identified in the New Day Plan, Strategic Plan, and the Departments’ Measures of Effectiveness (MoE) and both are illustrated in Figure 16.

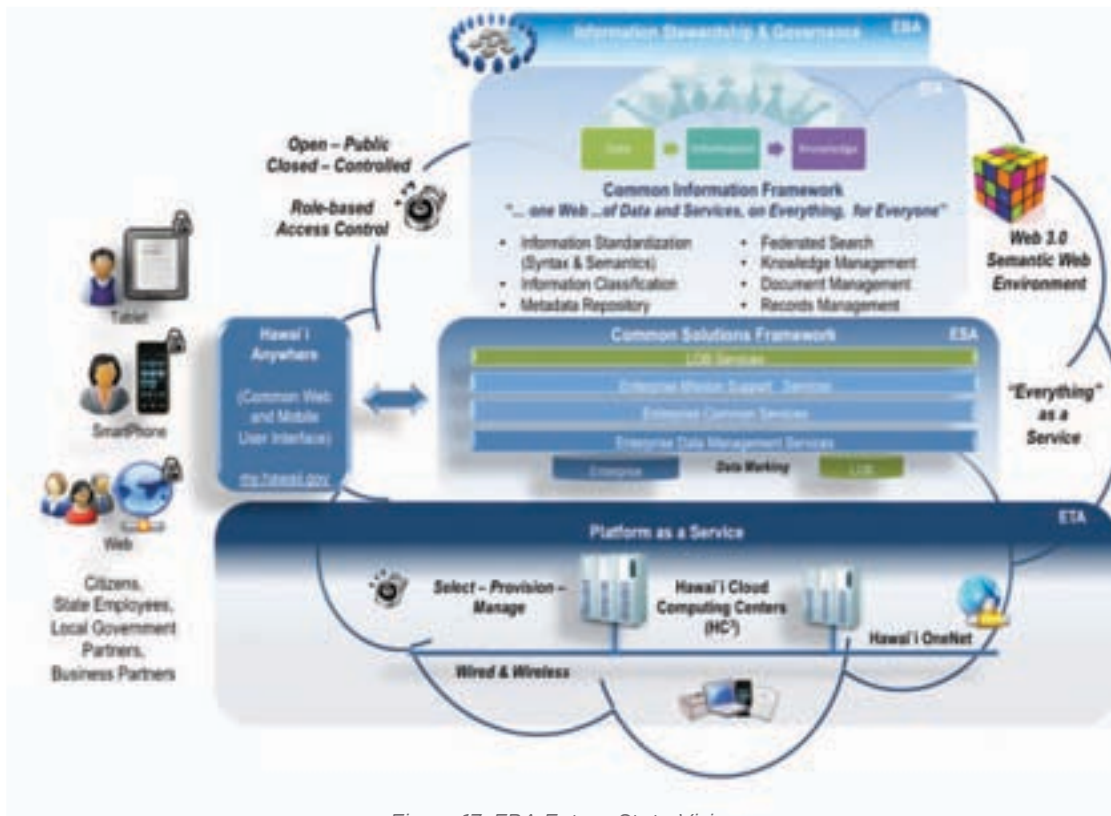


Figure 17: EBA Future State Vision

The following areas define the PRM focus for the State of Hawai`i :

- Mission and Business Results Measurements - captures the outputs Departments' outcomes the State seeks to achieve. These measures commonly include New Day Plan directives, Strategic Plan strategies, and Departmental and Program MoE.
- Functional Effectiveness - captures how well a Department, LOB, program, or specific process is serving its identified user base/constituents. These measures commonly revolve around constituent benefit, service quality, service accessibility, etc.
- Process and Activity Indicators - consists of outputs directly from the process supported by an IT investment. These measures commonly revolve around productivity, financial management etc.
- Technology - captures performance directly related to the technology investment. These measures commonly involve cost, quality assurance, information and data availability, and reliability.
- Human Capital Management - related to the ability of a Department to have the right people with the right skills in the right positions. This measurement area will be developed in accordance with bargaining unit rules to determine true effectiveness.

These measures will be captured and communicated as part of an electronic dashboard to track and the outcomes will be monitored. These outcomes provide the indicators as to how well IT is supporting and enhancing the ability of LOB's to accomplish their mission.

For times when the performance of an LOB increases the changes made should be leveraged across other LOB's to achieve similar results. In cases where a performance indicator decreases the change should be reversed.

The PRM is critical in defining performance in a timely manner that allows for rapid and accurate decision making by the various IT governance committees.

The composite view of the future state EBA is provided in Figure 17.

4.3

EBA TRANSITION AND SEQUENCING (T&S) PLANNING SUMMARY

The T&S Plan for the EBA is focused on areas that are not inherently technical in nature, but instead on areas such as organization of IT staff, process steps, development of meaningful measures and looking in to the future of IT trends. T&S Plan elements associated with the EBA start with alignment to the goals and standards established for business transformation and IT is depicted in Figure 18.

The advantage to the EBA T&S activities is that many of these areas will be worked in parallel with emphasis not on the urgent and immediate actions but on strategic and long-term activities. The T&S goals associated with the EBA and also derived from the Strategic Plan have implications for the EIA, ESA, and ETA. The EBA transitioning and sequencing initiatives include the following:

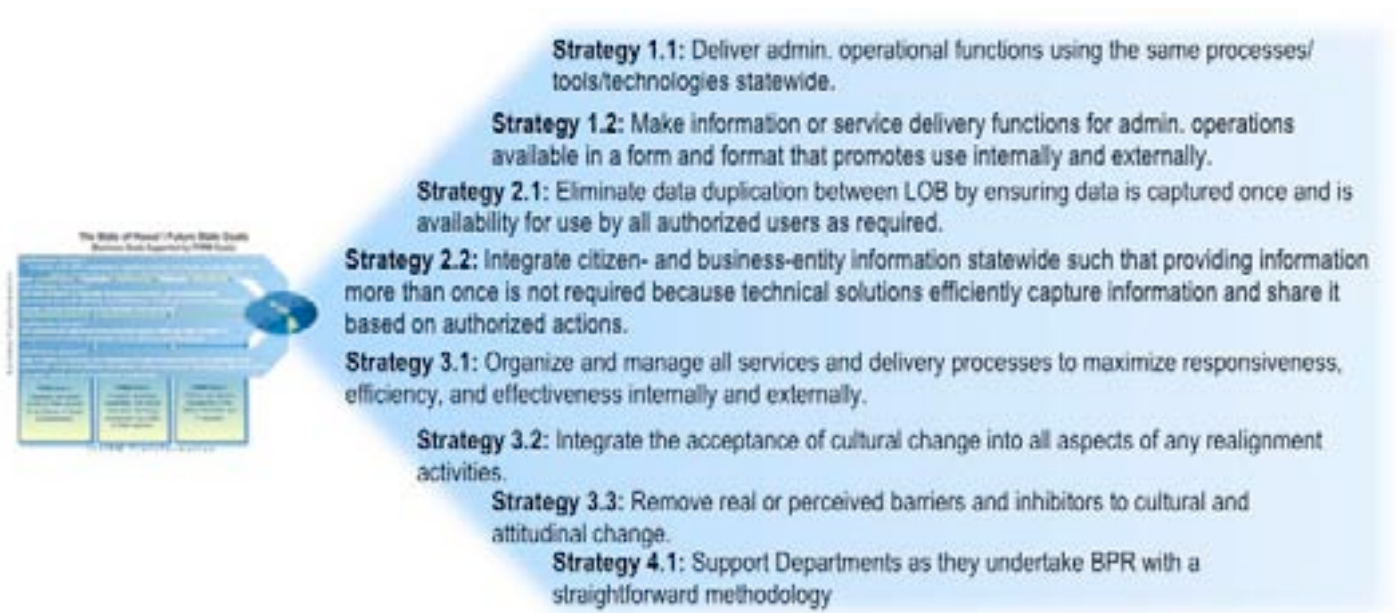


Figure 18: Business Transformation Strategies Required to Achieve the Future State EBA

4.3.1 REENGINEER ADMINISTRATION OPERATIONAL FUNCTIONS

As noted in the current state, the ASOs work to minimize or overcome the lack of an enterprise approach relative to reengineering existing processes and implementing associated systems is required beginning with those having the highest immediate return on investment (ROI) enterprise-wide:

- Time and attendance reporting and tracking
- Department of Labor and Industrial Relations unemployment distribution via checks
- Enterprise-wide document management and tracking and records management
- Enterprise-wide legislative bill tracking

4.3.2 REPLACE THE EXISTING FINANCIAL AND BUSINESS MANAGEMENT SOLUTION

The Final Report as well as the analysis of the LOBs and Departmental reporting needs clearly identified the overwhelming need to plan, procure, and implement a new financial and business management solution that accommodates:

- revenue collection/accounts receivable [Department of Taxation (DOTAX) and other organizations with revolving funds]; accounting, procurement and acquisition;
- inventory management; accounts payable including payroll and time and attendance reporting, [Department of Accounting and General Services (DAGS) and Department of Human Resources Development (DHRD)];
- budgetary planning and financial management [Department of Budget and Finance (B&F)]

4.3.3 UPGRADE THE IT INFRASTRUCTURE

The need to plan and upgrade the State of Hawai'i IT infrastructure and the facilities that house this infrastructure to support information needs was identified repeatedly as an overarching business need. This upgrade includes not only the retirement of existing hardware but also the creation of a disaster recovery environment.

4.3.4 INFORMATION STEWARDS LEADS, PARTICIPANTS, AND STAKEHOLDERS

As an extension of the BRM and the identified LOBs identify and assign information stewards/leads, participants, and identify all stakeholders for each identified LOB for all data sets within the State.

4.3.5 REMOVE BARRIERS TO INFORMATION SHARING

Identify and reengineer existing processes that inhibit information sharing within the State with priority on newly identified needs including:

- Patient Protection and Affordable Care Act (PPACA) implementation
- Geographic Information System (GIS information utility)
- Longitudinal information
- Death Records information
- Business License information
- Unpaid Business Tax information

4.3.6 SIMPLIFY AND SECURE INFORMATION GATHERING FROM CITIZENS

Identify the complete set of information required from citizens and business entities within the State, gathering once and enforce re-use by across the State. Address and resolve information management, privacy, and protection issues associated with the management and use of the identified information set

4.3.7 ENSURE REQUIRED SERVICES ARE DELIVERED

Within each Department define all services defined by statute/act or administrative directive and crosswalk these requirements to actual services being performed. Based on service identification results, evaluate the effectiveness of the current organizational structure for the Executive Branch of State.

4.3.8 PROMOTE PROCESS REENGINEERING WITHIN THE STATE

While numerous processes will be improved via the implementation of new systems, many of the activities performed within the State are independent from IT solutions. For these independent processes (e.g., tax collections, tax return receipt and processing, job requisition processing) perform reengineering prioritized based on projected ROI within each Departments.

The investment initiatives to accomplish these T&S goals are defined and further specified within the following sections of the EA that describe EIA, ESA, and ETA.



5.0 ENTERPRISE INFORMATION ARCHITECTURE (EIA)

5.0 ENTERPRISE INFORMATION ARCHITECTURE (EIA)

The overarching Enterprise Information Architecture (EIA) for the State of Hawai'i is described in this section. The EIA is discussed in terms of the current or As Is state of information management, the future state or To Be vision for information management, and in terms of the implications for actionable focus areas to be expanded in the gap closure or T&S Plan.



The State's Strategic Plan has as its primary vision the realization of a State government that is operating as a fully integrated enterprise. This was echoed in the future state vision for the EBA as well. This vision of full integration includes:

1. the streamlined and efficient operation of all business processes,
2. secure and reliable access to information anytime, anywhere, and to anyone who is authorized to see it, and
3. the effective delivery of information to all citizens, state employees, and other stakeholders using a state-of-the-art, highly optimized, and standardized technology infrastructure.

Consequently, the information management objectives for the State cited in this architecture were developed to facilitate the realization of that vision.

The continuum in Figure 19 depicts the progression in the discipline of information management. This progression takes an enterprise through management of data, to the management of information, to the end goal of managing knowledge. Each element in the progression must be mastered before taking



Figure 19: Information Management Continuum

the next step. With this in mind, the EIA has been defined to support the State of Hawai'i in this progression in order to achieve the future state vision.

5.1 EIA CURRENT STATE

The current state of information management was characterized as part of the Final Report and the lack of information sharing across Departments and organizations within the State was noted. The assessment surveyed critical information needs and information flows used in conducting the Department's business and the corresponding critical information sources and databases. In assessing information management and data sharing across Departments (or across divisions or programs within Departments), there were several noted instances where systems were dedicated to making critical data available for analysis and decision making on a broader scale. Examples included the Financial Accounting Management Information System (FAMIS) data mart and the Department of Health's (DOH) data warehouse. However, across the State these noted instances or examples were the exceptions not the rule, and the overarching findings related to information management indicated that within the State a data sharing culture was not present. These findings are summarized in Table 2 and are presented from two different information sharing perspectives:

- Perspective 1: Effective use of information at the individual or user level for analysis and decision making.
- Perspective 2: Application or system integration used to support the streamlining and integration of business process.

Table 2: Current State Information Sharing Assessment Results From Two Information Sharing Perspectives

Information Sharing Perspective	Assessment/Question of Need	Findings
1.1 Individual analysis and decision making perspective	Do people have access to the information they need to effectively do their jobs and make key decisions, and more specifically, do the key user communities of State workers, workgroups or project teams, management, and the public have the requisite access?	<ul style="list-style-type: none"> • Across the enterprise, the facilitation of end user access to data through a data mart warehouse approach including ad-hoc query and reporting tools was not common. • IT systems in legacy mainframe environments were not well positioned to facilitate end user analysis and reporting to minimize the need for manual intervention by already overtaxed employees. • State workers were found to rely heavily on the content and presentation of pre programmed reports. The continual maintenance of these reports is expensive and the entire approach is often inadequate to address rapidly changing needs and requirements. • Solutions provided explicitly for "making information available to a broad user community" were sparse, indicating that the engineering of solutions to support this level of sharing is not an area of emphasis within the State's Business or IT culture.

Information Sharing Perspective	Assessment/Question of Need	Findings
2.1 Application or system integration perspective	Do applications that support mission execution have access to information that they need that might exist outside their own internally maintained set of data?	<ul style="list-style-type: none"> The State's current management of data and data sharing is characterized by numerous silos of data and information, and a large number of complex and interdependent data feeds. Where no actual data feeds exist, interfaces are often accomplished via the printing of information from one system and manual re-entry of that same data into another system, resulting in the effective use of resources, introduction of errors, and unnecessary time lags. Examples include the fixed asset inventory, personnel benefits, and time and attendance processes. There are essentially no shared databases within or across Departments. The GIS database is one notable exception. The poor level of data sharing and information management is likely the result of the natural tendency of Departments to adapt and address their own data needs without the benefit of any statewide, enterprise-level policies, approaches, and solutions that encourage, facilitate, and enable application data integration and sharing.

5.2 EIA FUTURE STATE

State of Hawai'i Information Management
Future State Vision by 2022:

Information management is optimized and information capital effectively captures, uses, and transfers knowledge.

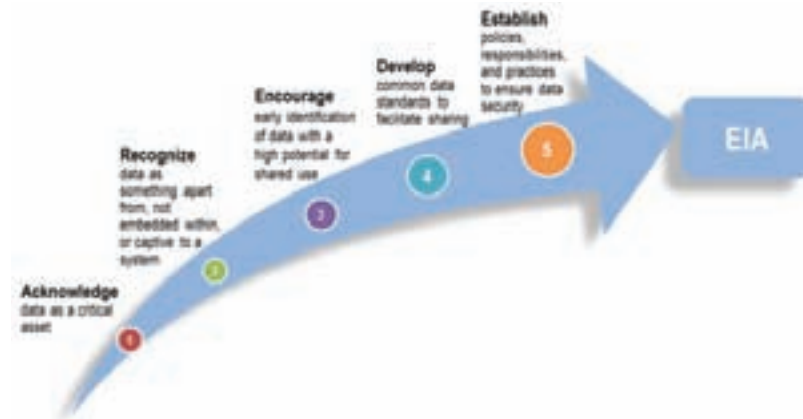


Figure 20: Purpose and Role of the Future State EIA

The future state design for the State's information management practices is one where information and data are recognized/acknowledged by everyone as a statewide asset and are managed and shared effectively among all State organizations. As with any critical statewide asset, appropriate management processes and methodologies will be established to enable and facilitate sharing and reuse. The purpose and role (as depicted in Figure 20) of the future state EIA is to:

- acknowledge or bring visibility to the concept that information and data as a critical state asset.
- recognize the fact that a data or information asset is something apart from and not embedded within or captive to information systems that might use it.
- encourage or promote the identification of critical information and data that has a high potential for shared use;

- develop a common information/data structure to facilitate sharing across systems and organizations.
- establish policies, responsibilities, and practices that ensure the on-going security of data and information from the three requisite security perspectives of confidentiality, integrity, and availability.

...of Data and Services, on Everything, for Everyone”.

A major component of a Web 3.0 environment is the establishment of a semantic web. In such an environment the web not only provides a linkage to and presentation of documents and files to people but it also serves as a vehicle to link and present data in a computer interpretable format for direct consumption by software systems. Both individuals and programmatic constructs such as web services or computer applications can easily integrate or “ mash up” any kind of data. This semantic web of data provides an environment in which data is not embedded within systems, but rather exists independently from them. In addition, differences in vocabularies and formats are essentially overcome and result in real and significant opportunities for data reuse.

5.2.1 INFORMATION MANAGEMENT AND USAGE



The future state vision for information management and usage within the State of Hawai'i includes the realization of a Web 3.0 environment as

characterized by the World Wide Web Consortium, “Evolution toward one Web

The realization of this vision requires a common information framework within the State that:

- Represents a disciplined environment that prevents the creation of redundant information, ensures the integrity of an “item of information” at the time and point of origin, and channels any subsequent use or update of the item of information to its single authoritative storage location.
- Promotes blending of structured data (e.g. data content in relational databases), with semi-structured data (e.g. data and messaging content in an email); and unstructured data (e.g. textual and graphical content in a document or web page) in a manner that make search and traversal across these information structures are transparent as possible

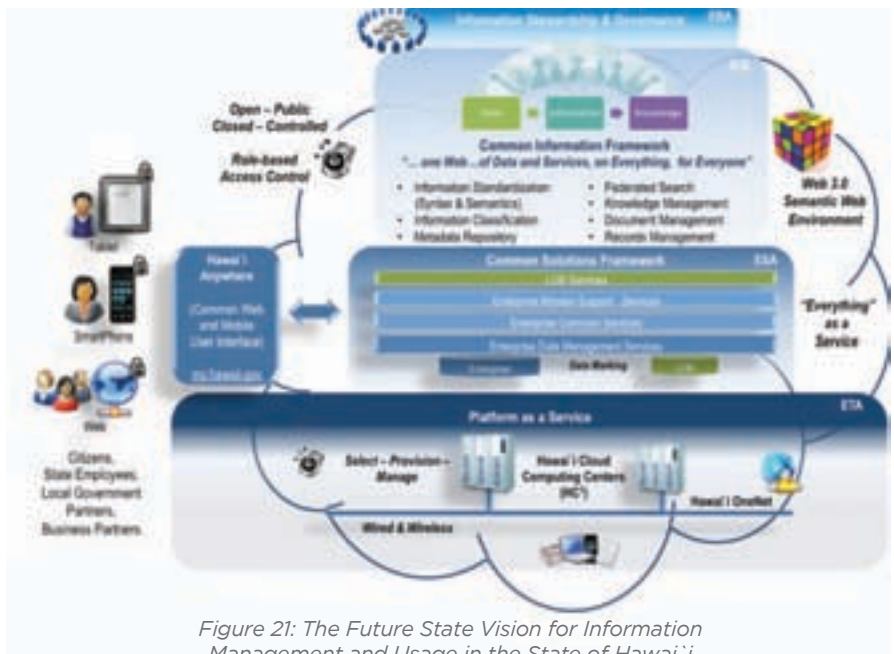


Figure 21: The Future State Vision for Information Management and Usage in the State of Hawai'i

- Promotes a mature management discipline that ensures all data: is well-designed and structured consistent with the “real world objects” of the State government. These objects would include all those from the operational and subject domain data for State business services, and would include all critical dimensions such as time and geospatial data to fully support historical analysis of operations at a point in time or location, or that support any associated trending analysis; is appropriately stored, secured, and protected; and, has no unnecessary boundary that hides or impedes access for any authorized person or business process.
- Allows people and processes, whenever practical, to search and relate data and information across multiple LOB without having to design and program that capability in advance or in other words, boundaries across applications and organizations will, to the extent practical, be non-existent.
- Includes a common or universal information standardization and mapping capability built on real world objects in the State government. Standardization of this mapping capability will facilitate web enabled traversal among information sources much like we navigate among document links in the environment of today.
- Supports the inclusion of all appropriate State data and information into a mature knowledge management system or discipline where knowledge is given

a preeminent value as a critical State resource and by extension provides for a corresponding emphasis on supporting the information and data assets that underlie that knowledge. A mature knowledge management discipline will support the capture of all operational and subject domain knowledge and facilitate its effective use for educating, problem analysis, and decision making for all State management and staff.

- The operation of all the above with the assurance that all necessary policies ensure that the confidentiality and integrity of the information is achieved at all time.

The future state vision for information management and usage in the State of Hawai'i is summarized in Figure 21.

Two key features of the future state vision – the Semantic Web and knowledge management. These are described in more detail below.

5.2.1.1 SEMANTIC WEB

Standards, protocols, languages, and methods that support the ten-year vision for the State’s EIA was established using numerous standards and protocols originally created by organizations such as the World Wide Web Consortium (W3C). These standards and protocols enable an effective transformation of the Web from a vehicle for the linking of human interpretable document content to a vehicle that additionally provides

for the linking of computer interpretable data. Key elements of the Semantic Web framework and the related evolution are described below and have considerable implications for the State of Hawai'i . Several of these are discussed below.

XML (eXtensible Markup Language) is a foundational element or a scheme for providing a format for tagging metadata or describing the attributes of a “real world object”, such as the author of a Web page. Prior to emergence and adoption of XML, data was almost exclusively stored in database or file formats, where only one or a limited set of applications understood the structure and format of the data to make effective use of it.. XML provides a more or less universal self-describing data syntax that is both human readable (to an extent) and machine interpretable. Presenting data in an XML format does in fact support and improve upon the exchange and sharing of data – but that exchange and sharing is still largely only accomplished within a limited community of applications in a single problem domain that share and understand the semantics of the data described with the XML syntax.

The emerging protocols and technologies associated with the Semantic Web provide the next evolutionary step as a standard approach for describing “resources” (the real world objects referred to above) from a semantic perspective, enabling an ability to link across resources from multiple domains and establishing and leveraging semantic relationships. The foundational protocol

is the Resource Description Framework (RDF); the RDF and other related standards and protocols can be seen in Figure 22 below. These standards and protocols enable the meaning (semantics) of the data to be embedded with the data in a computer interpretable manner that supports a semantic linkage among the data – creating the aforementioned web of data as to opposed to the simpler web of documents. From the W3C “Semantic Web Activity” Web site (<http://www.w3.org/2001/sw/>): “The Semantic Web is about two things. It is about common formats for integration and combination of data drawn from diverse sources, where on the original Web mainly concentrated on the interchange of documents. It is also about language for recording how the data relates to real world objects. That allows a person, or a machine, to start off in one database, and then move through an unending set of databases which are connected not by wires but by being about the same thing.”

Semantic web’s Protocol and RDF Query Language (SPARQL) as a query language for accessing data/databases in order to retrieve and manipulate data stored in RDF format. It is considered as one of the key technologies of semantic web.

Making effective use of these new standards and protocols to achieve the benefits of data with embedded semantics will require the State to make a significant investment and to place a real emphasis on the support of a st requisite polices, practices and technologies. Figure 22 provides additional examples of the numerous protocols for the Semantic Web from W3C.

5.2.1.2 KNOWLEDGE MANAGEMENT

Knowledge is the last element in the information continuum and knowledge management is the discipline that outlines the lifecycle process of identifying, capturing, organizing, and leveraging knowledge assets to improve overall performance and efficiency. Further as noted above in the discussion of the information sharing perspectives, knowledge management discipline is when individual experience, expertise, and insight is captured, standardized, and then transferred or shared with others. This discipline effectively supports the expansion of organizational insight and knowledge and will facilitate the achievement the future state vision for the State.

To achieve this vision, the State’s knowledge management capabilities will have overcome the data and information overload phenomenon and will facilitate targeted access to the



relevant tailored information needed within a specific problem domain. Going forward, business processes will systematically incorporate new insight and knowledge into operational processes, policies, and actions. Given that the people involved in a community of practice around a business service are constantly learning, the intent of knowledge management is that their experience and expertise is institutionalized. The community’s experience is organized into operational histories that facilitate the analysis of trends over time and the relevant impact of any significant event.

Initial implementations of both the EA and the LOB Segment Architectures are planned for development during the second half of FY2012. Moving forward these architectures will be maintained and used as the “north star” guidance for achieving the desired integration of all information assets, systems, and technologies. Individual information system projects will obtain integration and standardization requirements from these architectures and will design and implement the target systems in compliance with the architectures.

.....

State of Hawai‘i Knowledge Management Future State Vision by 2022:

The State of Hawai‘i will be widely recognized and characterized as a knowledge-based organization where mature data and information management process that supports a cultural awareness regarding the preeminence of knowledge as an enterprise resource to be harnessed and reused at an advanced level of problem solving. It is expected that the State will be widely recognized and characterized as a knowledge-based organization.

.....

RIF	Rule Interchange Format: expressing business rules for computer interpretation.
OWL	Web Ontology Language: further strengthening of descriptive meaning of data.
SPARQL	Simple Protocol and RDF Query Language: queries across RDF data on the web.
RDF-S	Resource Description Framework – Schema: expand RDF to a full schema.
RDF	Resource Description Framework: Description of resources and cross links.
XML	eXtensible Markup Language: base all above description protocols on XML.
URI	Uniform Resource Identifier: use a web link to get to data (not just a document).

Figure 22: Example Protocols for the Semantic Web from W3C

5.2.2 EIA ELEMENTS

To support the utilization of the EIA within the State, three primary focus areas are defined:

1. The Common Information Framework—establishes the common goals, end objectives, strategies, policies, and guiding principles for definition and management of enterprise information.
2. The Conceptual Information Architecture—establishes a classification system through a subject area hierarchy of the State’s information assets to facilitate stewardship leadership boundaries and associated responsibilities; and, supports the identification of authoritative and duplicative information resources.
3. The Requirements for Information Delivery and Sharing establishes requirements for the Enterprise Solution and Technology Architectures to achieve the future state vision for the EIA.

Figure 23 illustrates the three focus areas and their purpose.

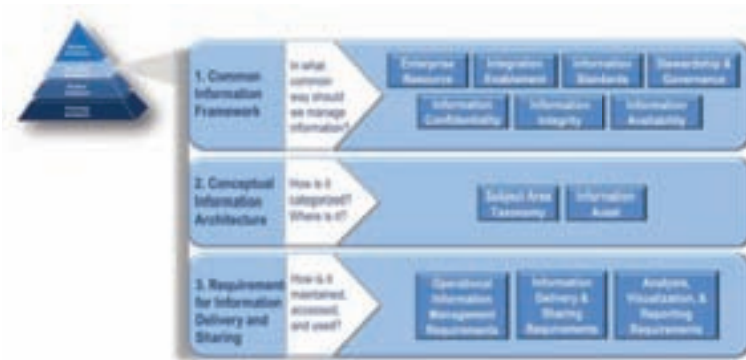


Figure 23: Focus Areas of the Enterprise Information Architecture

The following sections provide additional insight into these three focus areas:

5.2.2.1 COMMON INFORMATION FRAMEWORK

The guiding principles for the State’s Common Information Framework, while outlined above, are expanded upon below. This framework provides the foundation for achieving the future state vision.



ENTERPRISE RESOURCE

The first order of importance is the recognition of data, information, and knowledge for the State of Hawai‘i as a critical, valuable resource or asset that must be managed consistent with any other valued resource.

As a result, the State of Hawai‘i manages this important resource or asset in a manner that will:

- control the quality of information at the point of origin,
- facilitate the sharing of information across the enterprise,
- minimize redundant information,
- provide the timeliness of information for the intended purpose, and,
- ensure the confidentiality, integrity, and availability of the data in compliance with State and Federal regulations and laws.

In this context, information is defined to include structured data (data maintained within computer databases), semi-structured data (email), and unstructured information (documents, images, web content, etc.).

To achieve the future state relative to information as an enterprise resource, government operations within the State must be conducted within an open and transparent environment, enhancing the public trust and empowering citizens, State employees, and other stakeholders through access to information. There will be a thorough and strong classification approach to ensure that data and information that should be protected from dissemination by law or regulation will be “marked” and managed appropriately. (Note: The majority of State’s information is already public in nature and the future state environment provides greater availability and transparency by facilitating open access to all public information.)

Challenge Faced by the State Relative to Treating Information as an Enterprise Resource

To discuss the treatment of information as an enterprise resource is direct and straightforward; however, moving from discussion to action will require a cultural change throughout the State and within the Departments in terms of how information is viewed, treated, and managed going forward. There are two significant challenges to effecting this cultural change.

First, because data and information are inherently less tangible than hard IT assets (e.g., systems and infrastructure components that have very evident cost drivers) executives/managers often equate “data” and “data management” to “bits and bytes” that are addressed in the context of storage and server infrastructure. Information and data management must be viewed as separate from hard assets and stand on its own as a discipline to address the classification and management of data at level above that of storage management.

Second, in some instances the value of information and data has been recognized and elevated, but the culture has allowed significant autonomy at the Department or program level but not at the enterprise level. The Departmental or program manager is often allowed to be entrenched as the “owner” of information and therefore controls data availability. In reality, it is often a struggle to achieve appropriate data availability within a Department, much less across Departments.

KNOWLEDGE MANAGEMENT

A streamlined and efficient operation of all business processes is enabled through effective access and use of information. It is the intent of the State of Hawai`i to achieve optimal business performance through integrated business functions and using enterprise information provided by common information repositories. These repositories will not be unnecessarily constrained by organizational (i.e., Department, Agency, Branch, Attached Office, or Program) boundaries. Key tenets regarding integration enablement include:

- The State of Hawai`i will manage the design and implementation of integrated information repositories (e.g. operational and analytical databases based on its EA Methodology that works in tandem with the Systems Development Life Cycle (SDLC Methodology and promotes compliance with the EIA.
- To facilitate information enablement, emphasis will be placed on managing information architectures at both an enterprise level and LOB level. The CIO and OIMT will have primary responsibility for managing at the enterprise level and the Department Directors or other individuals designated as the LOB Lead will have primary responsibility for managing at the LOB level. The architectural components that exist at the LOB level will be referred to by the moniker of LOB Segment Architecture.
- Integration will be achieved through analysis of integration requirements at both levels and architecting information solutions and technologies to satisfy those requirements.

INFORMATION ARCHITECTURE LEVELS FOR SHARING

As noted above, management of the scope of common or shared information across the State is done at two levels: the enterprise level and the LOB level. Corresponding management practices for associated governance across the stakeholder community will be applied at these same two levels.

STEWARDSHIP/LEADERSHIP RESPONSIBILITY AND GOVERNANCE STRUCTURE

For the benefit of all internal and external stakeholders, management and oversight of common information assets, systems, and supporting technologies will be based on a stewardship/leadership approach. Stewardship/leadership responsibilities for management and oversight will be established at two levels of integration – the enterprise level and the LOB level. The overarching responsibilities and requirements are:

- All information and data assets will be managed as valued assets to the State. Information and data assets will have appropriate stewardship responsibility assigned either at the enterprise or LOB level. Information stewardship leadership responsibilities are essentially the same at each level and vary only according to the body of stakeholders represented by the lead.
- Primary responsibility for establishing the EIA resides with the CIO and OIMT. The CIO is supported by the OIMT EA Program. Governance of the EIA will be the responsibility of the OIMT EA Program. This organization will establish information architecture policy and standards that apply for the State. The CIOC has been established to provide initial direction and approval of the EIA. Whenever necessary, the CIO Working Group (a subcommittee of technical experts from a representative segment of the CIOC or other subject matter experts) will be formed to further clarify issues and propose standards.

The role of “information steward/lead” will be established within each of the LOBs. These individuals will have primary responsibility for an information subject area and its associated business processes and applications. The leads will be responsible for assuring the quality of information is enforced and enterprise standards are followed. Their primary role of the steward/lead will be to understand the data, business rules, and toolsets in order to properly define the data and monitor its quality, accuracy, consistency, security, privacy, and to facilitate information sharing.

INFORMATION DESCRIPTION

Information used within the State will have a uniform description to support information sharing. The development of the standard information description will enable Departmental stakeholders to agree on the structure (syntax) and meaning (semantics) of the information. The standard information descriptions are documented as artifacts of the EIA. Information description artifacts include metadata (data about data) and information/data models using industry standards such as entity-relationship (ER) models.

INFORMATION CONFIDENTIALITY

All information lifecycle management activities and specifically information access and delivery will be done in a secure and reliable manner. In addition, all federal and state laws and regulations regarding information confidentiality and privacy will be complied with at all times. Industry best practices regarding information assurance, security, and privacy serve as standard practices within the State, and are performed as part of on-going operations, and routinely evaluated and assessed to ensure operations are being conducted in compliance with the practices.

Items or portions of information that fall under confidentiality and privacy requirements will be appropriately classified and “marked”, and information access and delivery systems to ensure that appropriate access permissions have been granted and that appropriate computing boundaries for sensitive information are maintained and sensitive items of information would not cross these boundaries.

Responsibility for information assurance, security, and privacy will rest with the CIO and the OIMT security officer.

INFORMATION INTEGRITY

LOB leads have primary responsibility for ensuring the confidentiality, integrity, and availability of information. Business rules that define and establish the integrity of information will be adhered to in information creation and update operations. Items of information (or information objects) are managed to ensure a single point of origin and an authoritative source. Redundant information sources – the same intended

information from multiple sources – must be avoided and eliminated when identified. Copies of information are controlled and information location is tracked and controlled to ensure traceability to the authoritative source and point of origin.

INFORMATION AVAILABILITY

Access to the right information anytime and anywhere to anyone who has an appropriate need for it should be enabled and assured. Information access is supported through the effective utilization of state-of-the-art technological interfaces such as the Web and mobile devices for citizens, State employees, and all other stakeholders through an optimized and standardized technology infrastructure.

5.2.2.2 CONCEPTUAL INFORMATION ARCHITECTURE



The Conceptual Information Architecture is an enterprise level information model that categorizes government information into a hierarchy of subject areas in greater levels of detail. The top two levels of the taxonomy mirror the top two levels in the Conceptual Business Architecture (LOB and Business Services), promoting a common stewardship/leadership structure between

the business functions and information perspectives. Further levels of decomposition identify key business information entities or objects for which information must be defined and maintained. A common information model streamlines information exchange processes within State government and between State government and external stakeholders (e.g., citizens, business entities, Federal government). In addition, the information taxonomy will support the sorting of existing data assets according to their authoritative sources and will facilitate the recognition and elimination of redundant information sources.

The next two diagrams identify the top level subject areas for the core mission LOBs and the support service LOBs. These diagrams set the stage for assignment of stewardship or lead responsibilities and then moving through subsequent segment architecture and data/service standardization projects to continue the development and maturation of the EIA over time.

Figure 24 identifies the top level subject areas and notional information dependencies for the core mission LOBs. Further expansion of the Core Mission LOB subject areas is accomplished through the segment architecture projects. Information sharing in these areas will mostly be within the LOB, with some exceptions indicated by the notional information dependencies crossing the LOB subject areas.

Figure 25 identifies the top two levels of subject areas and notional information dependencies for the Support Service LOBs. All core mission LOBs have information dependencies with the support service LOBs. The level of sharing is predominately at the enterprise level.

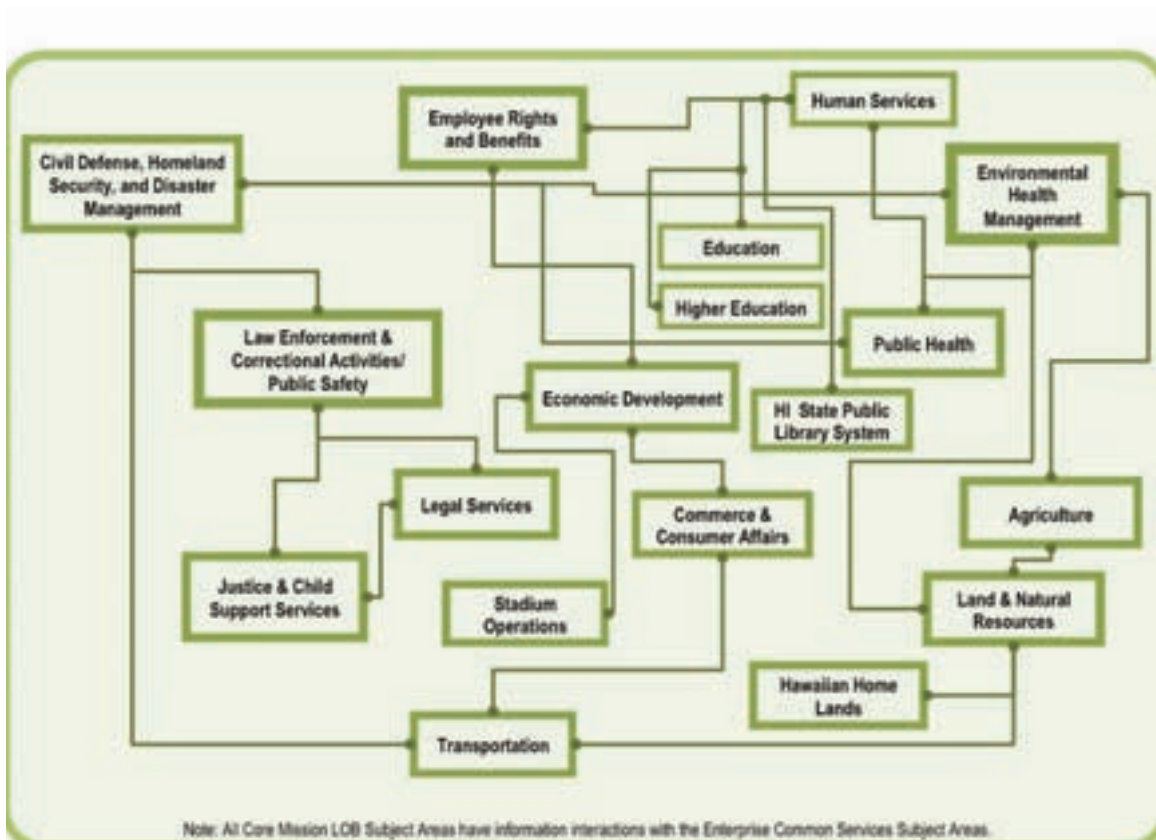


Figure 24: LOBs Providing Support Externally Subject Area Diagram

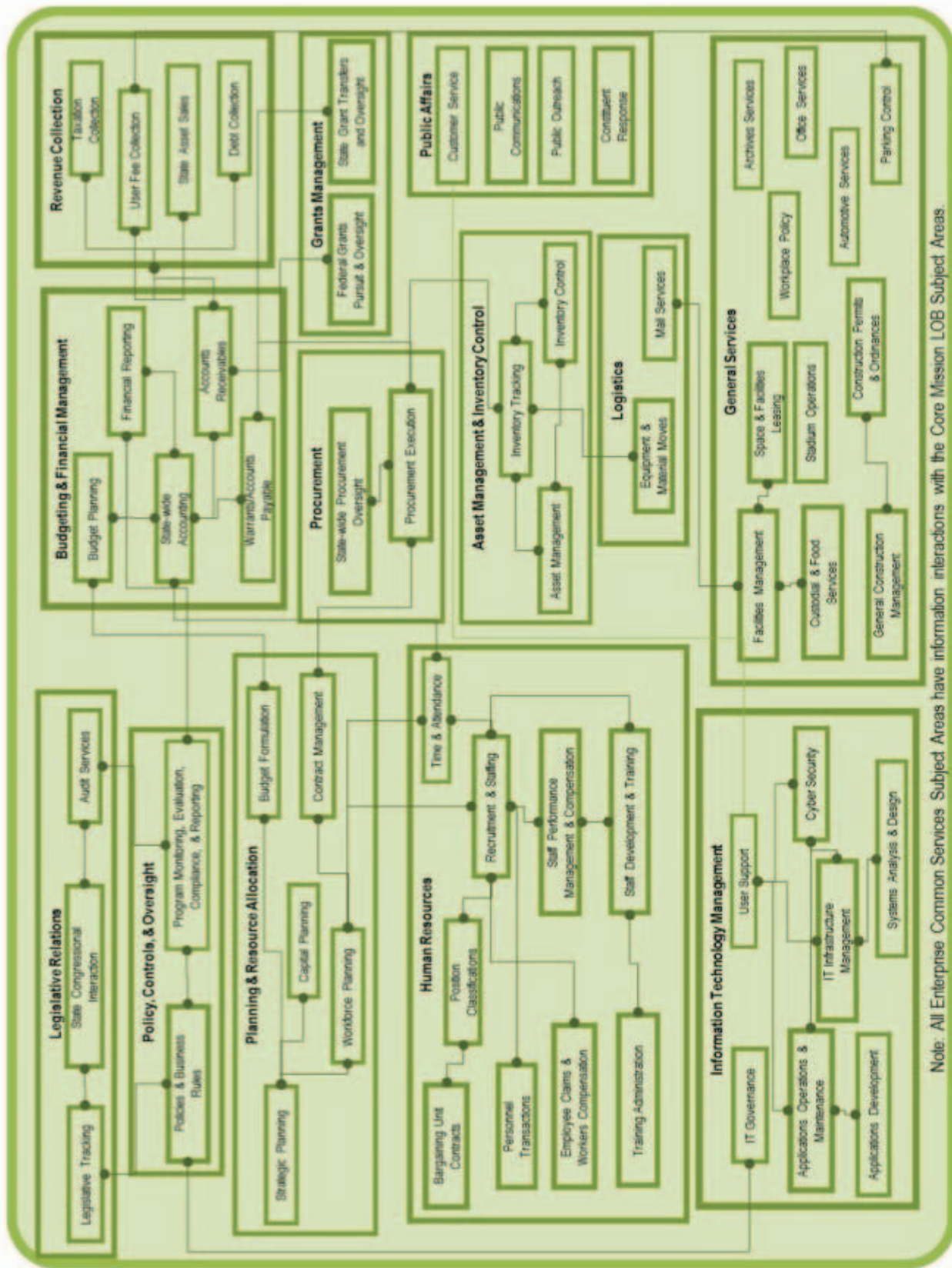


Figure 25: Representative View Support Area LOB Subject Area Diagram

It is the essence of the EIA to fully expand the enterprise information definition over time to establish common information descriptions, common data models, common data element definitions, and common data structures. Common data models may include ER models, National Information Exchange Model (NIEM), and in the future Semantic Web protocols such as Resource Description Framework (RDF). As the common definitions are implemented across the State, integration efforts and information quality will be improved.

The EIA is further detailed, iteratively and incrementally, through segment architecture development, data/service standardization projects, and solution architecture projects. The EA program and LOB information leads work collaboratively within these projects to create information standards (models, data structure, service components, and business rules) that ensure that all Departments and stakeholders' requirements are met. Pragmatic progress must be balanced with the evolution of stakeholder involvement through incremental version releases. The standard information models are stored in the EA repository within OIMT.

5.2.2.3 REQUIREMENTS FOR INFORMATION DELIVERY AND SHARING

The EIA places requirements upon both enterprise solutions and technologies needed to realize the information architecture future state vision. This section outlines those requirements that would flow down to the ESA and ETA respectively.



OPERATIONAL INFORMATION MANAGEMENT REQUIREMENTS

The operational information management requirements relate to the data and information management practices to support business operations, such as data storage, retention, and management.

All State data is maintained within databases using standard Data Base Management Systems.

Management practices for databases housing State data are common and standard to safeguard the confidentiality, integrity, and availability of the data. Database management standards and products are defined in the ETA.

Databases and other legacy data assets must be identified, inventoried, and have their metadata cataloged for inclusion in the EIA. All databases are considered official in nature and managed as such.

A common EA solution will be used for this purpose.

Databases are recognized and managed as separate valued resources apart from the applications that use them. Databases are designed for use by multiple applications and positioned and managed to this end. The data management philosophy is that data about a business object would be created by one application but may then be referenced by multiple applications from the same database – with direct access to the database or through a service. The ESA will enforce these principles.

State databases are categorized according to the two levels of sharing – enterprise and LOB and two primary types of databases will be established and used within the State:

- Operational database—primary support of operations and characterized by optimization for transactional processing through normalization (Third Normal Form (3NF) or greater).
- Analytics database—primary support of analysis and reporting and characterized by de-normalized design. An analysis and reporting database is principally built upon data derived from operational databases.

Standards and practices related to the administration of official databases will be established in the ESA and ETA.

INFORMATION SHARING AND DELIVERY REQUIREMENTS

Information sharing and delivery of shared informed will occur through three primary approaches within the State:



1. official databases,
2. master data sets, and
3. web services.

A catalog of data assets is maintained as part of the EIA within the EA repository as a tool in locating common data. Data assets may be located in an official database or in official master data set established for collaboration and sharing.

Tools are present to allow for XML (or eventually RDF) data sets to be extracted from enterprise and LOB databases to support internal exchange of data across the LOBs. Data for public access is made available through XML data sets (RDF in the future) hosted in a data.Hawaii.gov domain.

A catalog of web services is maintained as part of the ESA within the EA repository as a tool in locating common services.

Standards and practices for data and web service implementation and access are established in the ESA and ETA.

ANALYSIS, VISUALIZATION, AND REPORTING REQUIREMENTS

The ESA will establish a standard solution pattern for application solutions that support analysis, visualization, and reporting. The data analytics solution pattern will in turn establish requirements for the specific technology products needed for data derivation, and extraction, transformation, and loading (ETL); data query; analysis and trending; visualization including geospatial data; and dashboards and end user reporting.

EIA TRANSITION AND SEQUENCING PLANNING SUMMARY

Investment initiatives for achieving the future state of the EIA include the following projects:

5.3.1 ESTABLISH THE ENTERPRISE DATA AND SERVICES ADMINISTRATION

Within the EA Program, a series of activities and accomplishments must be completed to establish these enterprise-wide data and services management standards and practices. These include:

5.3.1.1 GOVERNANCE STANDARDS AND PRACTICES

Establish governance standards and practices which include the role of the information steward/LOB lead and the processes for collaboration, agreement, documentation, and change management of common enterprise or LOB data and services – a process the industry may refer to as master data management.

5.3.1.2 COMMON DATA AND SERVICES ARCHITECTURE

Establish the common data and services architecture within the EA tool and repository, inventories of enterprise and LOB data assets and services; and the approach and practices for defining shared (or master) data standards.

5.3.1.3

DATA AND DATABASE ADMINISTRATION STANDARDS AND PRACTICES

Establish data and database administration standards and practices for creating and maintaining official enterprise and LOB databases.

The investment initiatives to accomplish these three activities are further defined and specified within Section 7 in the ETA.

5.3.2

ESTABLISH ENTERPRISE COMMON DATA AND SERVICES FOR THE ERP IMPLEMENTATION

Within the scope of the support services LOBs to be included in an ERP system, establish standard data and services for key enterprise business objects. These include: Organizations, Programs, Employees, Citizens, Facilities, Assets; General Ledger Accounts; Projects; etc.

The investment initiatives to accomplish this are defined within Appendix A, ERP Implementation.

5.3.3

ESTABLISH ENTERPRISE COMMON DATA AND SERVICES FOR THE AFFORDABLE CARE ACT

Within the scope of new business processes to support the Affordable Care Act, establish data standards and shared services for key common business objects.

The initiatives to accomplish this are defined within Appendix A, Health IT.

5.3.4

ESTABLISH ENTERPRISE COMMON DATA AND SERVICES FOR THE SUPPORT SERVICES

In addition to the data and services standardization initiative for the ERP system implementation, establish data standards and shared services for key common business objects within the remaining support services LOBs to include: Legislation, Policies, Program Performance Reporting, and Grants.

The initiatives to accomplish this are defined within Section 7 and Appendix A.

5.3.5

ESTABLISH ENTERPRISE COMMON DATA AND SERVICES FOR THE CORE MISSION LOBS

As business needs drive priorities and opportunities, establish data standards and shared services for key common business objects within the each of the core mission LOBs.

The initiatives to accomplish this are defined within Appendix A.



6.0

ENTERPRISE SOLUTION ARCHITECTURE (ESA)

6.0

ENTERPRISE SOLUTION ARCHITECTURE (ESA)

The overarching ESA is described in this section and includes a discussion of the current state and future state of the solutions environment. For the current state the focus is on information systems/applications software and for the future state vision the focus is on a comprehensive set of services-oriented solutions to meet State’s business needs. This section also includes a summary of the T&S Plan to achieve the future state vision for the ESA.



The ESA plays a critical role in enabling the State’s vision of realizing an integrated enterprise that consists of streamlined and efficient operations for all business processes. The ESA is also the most tangible and direct support layer of the EA in

relation to the business mission and services. It also is the IT component that staff and the public directly interact with in automation of business process and information delivery. The ESA is considered as the driving force for the structure and complexity of the underpinning technology architecture layer and requires a robust multi-functional technological platform.

6.1 ESA CURRENT STATE

The current state of the ESA was characterized as part of the Final Report. The report noted the weaknesses and legacy condition of the few, true statewide solutions, the large number of applications that have proliferated within the State and the critical need for “right-sizing” the applications portfolio. The findings from the Final Report are summarized in Table 3 by the criteria that indicate the maturity of the application portfolio as a whole and the characterization of any single application within this spectrum.

Table 3: Solution or Applications Assessment Results

Application Portfolio Assessment Criteria	Findings
<p>Stability – the number and extent of failures, down-time, “break-fix” cycles, or general risk</p>	<ul style="list-style-type: none"> • Numerous applications due to staff reductions and funding shortages exist in an aged condition • Many initiatives to upgrade or replace legacy applications and their supporting middleware and hardware infrastructures were postponed
<p>Optimization – measuring redundancy, duplication, and “waste”</p>	<ul style="list-style-type: none"> • Over 700 applications • A significant set of older mainframe applications, based on the “batch processing” model, require numerous smaller applications to support data interface feeds and outputs • A lack of enterprise-wide data governance and integrated databases results in numerous interfaces in order to support data mapping and translation • A lack of effective central systems for many of the shared service areas cause the Departments to develop their own supporting systems to ease their interfaces with the central system • Federal program-driven funding promotes solution architecture decisions that do not support enterprise application consolidation • A lack of budget/funding creates an environment that proliferates single user or small work group applications that are easier and less costly to create

Application Portfolio Assessment Criteria	Findings
<p>Standardization – measuring the underlying technologies (middleware and hardware/software platforms) required</p>	<ul style="list-style-type: none"> • Lack of funds to support upgrades results in a broad set of older technologies continuing to be used in the environment, and this increases incompatibilities (e.g., desktops requiring older, unsupported version of Windows or Internet Explorer) • Numbers of software product incompatibilities make it almost impossible to plan for enterprise-level upgrades, and this mixture of new and old software versions opens the enterprise to increasing levels of vulnerability from malware
<p>Integration – the characteristics and ability for an application to be well integrated with other applications and data within the enterprised</p>	<ul style="list-style-type: none"> • Point-solution approaches/situations have proliferated and work against enterprise or LOB integration • Lack of an enterprise organization to champion integration and/or funding to support enterprise solutions reduces integration
<p>Alignment – to business mission, services, priorities, strategies – the value in achievement of critical, high priority mission objectives</p>	<ul style="list-style-type: none"> • Significant investments within the “have” Departments and minimal investments in the “have not” Departments to develop and maintain applications perpetuate an imbalanced environment • Fundamental capabilities expected in enterprise solutions are lacking (e.g., global address list, shared calendaring, paper-based processes, lack of emerging technology support such as mobile devices and social media) cause frustration
<p>Responsiveness and Agility – to changing business needs – ability to respond with relative ease to change versus being overly complex and awkward to supporting change</p>	<ul style="list-style-type: none"> • Agility is limited because considerable customizations have been made to custom-off-the-shelf (COTS) software • Reliance on one-off applications (e.g., the DCCA Lotus Notes-based Legislation Tracking System) and their proliferation as pseudo-enterprise systems are now preventing the application of vendor upgrades

One of the weakest areas of the solutions or applications portfolio is the apparent lack of control in enterprise integration and consolidation for statewide support services. As noted in Table 3 many Departments have developed redundant capabilities. Creating the “right number” of enterprise support service solutions is the key challenge for the future state.

6.2 ESA FUTURE STATE

The State is facing an environment of continuous and rapid change due to technological surges and the need to transform old paradigms into new agent-based, service-oriented dynamic integration architectures. The demand for real time integration across disparate lines of business, enterprise applications, Web services, mobile interfaces, and networks, is driving industry toward pursuing standards that will enable open systems architectures to realize seamless access to multiple platforms and services. The desired outcome is the total integration of internal and external entities across the total enterprise.

The vision for the future ESA is a dynamic mobile integration architecture that responds rapidly to change and delivers quality information from trusted sources all stakeholders. This promising computing environment enables efficient services selection by LOBs delivering enterprise services while providing for the seamless integration with external stakeholders and in this case the citizens and residents of Hawai`i . The combination of intelligent Web services and mobile agents provides for the personalized demands needed by state employees to perform their missions and for the citizens and residents of Hawai`i to directly access information that is relative to their personal situations.

The future state ESA will be implemented within a common solutions framework that achieves the desired interoperability and integration, as illustrated in Figure x below. The key elements of the future state vision are outlined Figure 26 .

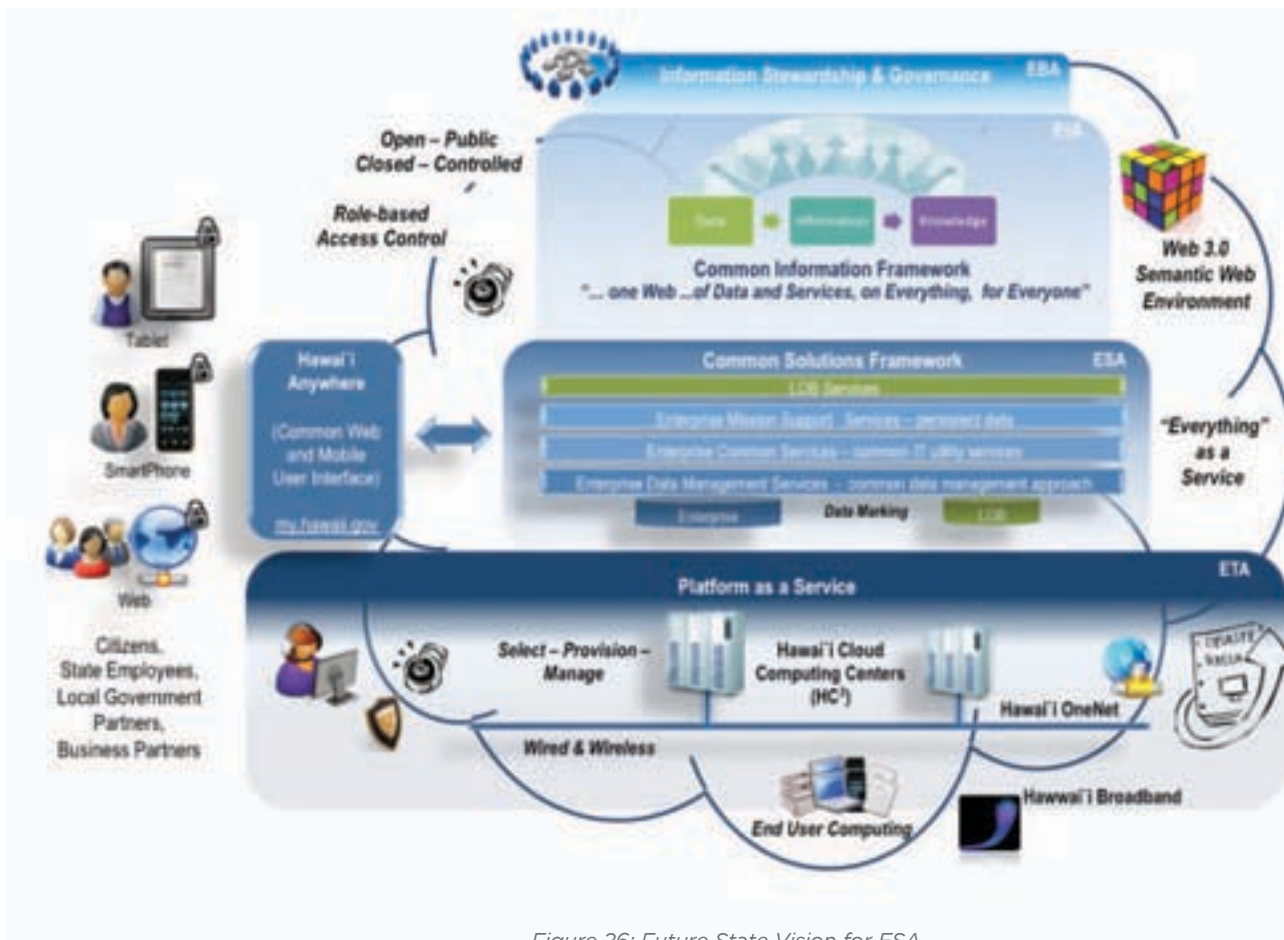


Figure 26: Future State Vision for ESA

6.2.1 VISION FOR THE FUTURE STATE ESA

The enabling of this vision occurs through a common solutions framework within the State that includes the following:

- Each individual's user experience with the State's automated solutions is personalized through a "my Hawaii.gov" portal that knows the person's roles, history of service usage, information interests, and tailors the portal accordingly - constantly changing based on usage. The user interface has shifted to mobile Smartphones and tablets with the portal look and feel consistent across all user devices. Solutions are built once with a user interface standard like HTML5 that works equally well across all mobile platforms.
- The solutions within the State's portfolio have been completely rationalized and transformed. All common support services have been reengineered with new service oriented solutions that effectively meet the needs of the core mission areas - all redundant support applications, like procurement or financial reporting have been eliminated.



- All of the support services have been automated through a common, integrated ERP system - resulting in broad integration across these shared services. The ERP scope includes planning and resource allocation, budgeting, financial tracking and reporting, time and attendance, payroll, accounts payable/warrants, accounts receivable, revenue collection, human resource management, procurement, asset management, facilities management, and other general services.
- "Everything is a service" is the new solutions paradigm enabling full integration across the enterprise. Business process automation has moved to a to a full component assembly approach, like LEGOTM building blocks, implemented through services and linked resources supplying information (Semantic Web).
- Cross-cutting services are organized into two subordinate layers for effective governance:
 - Enterprise Common Services - a "utility" layer for common enterprise IT services to include security services such as identity and access management; digital content services supporting documents and records; process automation supporting end-to-end workflow, robust search capabilities across the enterprise; and integrated collaboration, analytics, and geospatial visualization capabilities.



6.2.2 GUIDING PRINCIPLES FOR THE COMMON SOLUTIONS FRAMEWORK

The guiding principles for the State’s Common Solutions Framework were outlined above and are expanded below. The discussion identifies the common goals, end objectives, strategies, policies, and guiding principles of the State’s Common Solutions Framework to achieve the future state vision.

6.2.2.1 ENTERPRISE INTEGRATION

It is the intent of the State of Hawai`i to achieve optimal business performance through business functions and processes being integrated through the use of common solutions. The solutions will be viewed as enterprise assets and not “owned by” individual Departments or programs.

The State of Hawai`i directs and controls the design and implementation of integrated solutions through its EA Methodology. The emphasis for achieving integration is placed on managing architectures at an enterprise level and at a LOB segment level. Integration will be achieved through analysis of integration requirements at these respective levels and architecting solutions and technologies to implement them.

6.2.2.2 USE OF INDUSTRY STANDARD APPLICATION SOFTWARE WITHIN A SERVICES-ORIENTED ARCHITECTURE

Standard practice for the State of Hawai`i is to pursue the acquisition and implementation of industry standard application software. For State government, industry standards are found in both commercially available and government available off-the-shelf application software (COTS/GOTS). Industry standard application solutions should adhere to standards for services-orientation; so that they will be compatible with and interoperable with all service components within the ESA common solutions framework.

Implementing comprehensive application software packages provides a significant advantage due to industry standard “best practices” and the scope of integration across the business functions they implement. Packages are chosen to address as many functions within the enterprise as is practical. As a result, the number of application packages is minimized. Customizations to the standard industry business processes and rules contained within the package are kept to a minimum.

The State is an active participant in State and Federal communities of practice in order to collaborate on standard solutions. The State leverages and reuses applications from other States and the Federal government.

- Enterprise Mission Support Services – a layer for common business support functions and information persistence to include customer and case master information; business management master information for organizations, programs, plans, and portfolios; service management life cycle support for performance tracking and continuous improvement; ERP services for common budgeting, financial, human resources, and acquisition functions; and knowledge management for retention and reuse of problem domain knowledge.
- The enterprise data layer has been separated from the application software itself through a robust set of official enterprise and LOB databases and Web accessible data resources – the enterprise information and data has been liberated for widespread use within and outside the State government, and all State business solutions can make use of it.
- The people of Hawai`i and citizens are full stakeholders – State information is published through “data.Hawaii.gov” and some of the most important new applications are created by citizens. The solutions portfolio for the core mission areas such as public health or land and natural resources has a true blending of support from joint partnerships with community, private businesses, and Federal and local governments.
- “App stores” or catalogs are maintained across these stakeholder communities for sharing and reuse. The application communities include the ability to leverage and reuse applications from other States and the Federal government. An applications development ecosystem model is used to support the collaboration and reuse of open source and community source software.
- Internal to the State’s portfolio management discipline, solution patterns have been standardized resulting in optimized development approaches, tools, technical skills, and technology infrastructures, which reduces maintenance support costs and facilitates synergies in enterprise-wide knowledge and expertise. In a controlled manner, any recommendations for evaluating new emerging technologies are sanctioned, and an overall enterprise discipline for “new product/technology evaluation and insertion” has matured. The solutions portfolio includes a lifecycle perspective, incorporating refresh plans after a reasonable life expectancy.

6.2.2.3 STEWARDSHIP/LEADERSHIP AND GOVERNANCE

Management and oversight of common information assets, systems, and supporting technologies is based on a stewardship approach that continually assesses the benefit for the people of Hawai'i and citizens and internal and external organizational stakeholders. Stewardship/leadership responsibilities are established at the two levels of integration.

1. The CIO and OIMT will have primary responsibility for managing the EA, and
2. The Department Director/Deputy Director designated as the LOB lead or portfolio executive has primary responsibility for managing the LOB Segment Architecture.

The overall management and oversight of the ESA is conducted in accordance with the established OIMT governance model with two primary bodies – the Executive Leadership Council (ELC) leading business strategy and architecture and the CIO Council (CIOC) leading IT strategy and architecture. The ELC governs decisions regarding customizations to COTS/GOTS software and function as a liaison to the Legislature for appropriate legislative adjustments to facilitate changes to business processes to minimize COTS/GOTS customizations.

6.2.2.3 OPEN SOURCE SOFTWARE AND COMPLIANCE WITH OPEN STANDARDS

The State of Hawai'i should consider the use of software that incorporates or uses open standards when making decisions on software solution procurements. Open source software presents opportunities to implement solutions with minimal acquisition cost and maintenance of licenses. Decisions on use of open source software or software in compliance with open standards should be made in the context of total cost of ownership to include both acquisition and on-going operational costs.

6.2.2.4 SERVICE ORIENTATION, SOFTWARE REUSE, AND SOLUTIONS INTEGRATION

The EA development for the State of Hawai'i inserts itself into a "point in time" where the software development paradigm continues to evolve from object orientation to component-based development and now to service-oriented architecture (SOA). Each of these paradigms and frameworks share some common foundational goals for best practices in software development:

- Objects, components, and services all represent natural building blocks. By moving software development to a building block and assembly paradigm, like LEGOTM building blocks, building of more complex structures is facilitated through reuse of solid, well formed, and tested pieces resulting in higher quality solutions.

- The building blocks are defined and structured to accomplish discrete routine functions that are highly interoperable and facilitate reuse, and this very building block/assembly paradigm results in unique approaches within the software architecture, design, and implementation lifecycle activities.
- Each block is structured as an independent "black box" (i.e. self contained) in accomplishing its function(s) and it presents a well defined and relatively simple "interface" to its users or consumers {loose coupling or loosely joined} in order to maximize reuse.
- Services go beyond object-oriented or component-based development paradigms in achieving these goals of independence, loose coupling, and simplicity of interface. Services are independently published for use and stand on their own (no linking or builds of executables), have no specific development technology or platform constraints, and services have evolved relatively simple and elegant interface specifications through Web service technologies such as XML and Simple Object Access Protocol (SOAP).

To achieve these benefits, the State's common solutions framework incorporates a services orientation approach and framework within its software development life cycle (SDLC) – a set of principles, methods, and tools/technologies for architecting, designing, and developing enterprise solutions using highly interoperable services. To this end, the ESA features a horizontal services layer that implements these common reusable services to achieve extensive integration across the enterprise.

It should be noted that the development of a services orientation or SOA framework for the State of Hawai'i is approached in a pragmatic manner. There is recognition in the value of the design principles of SOA even at a departmental level, and that benefits can be realized with a standardization of Web service oriented technologies, as opposed to implementation of a framework based on proprietary technology choices, an example being an enterprise service bus technology. It is this lightweight approach that the State will be pursuing.

Effective reuse of services as well as open source or community source software requires knowledge within the development community of what services and software are available and how to effectively use them. The OIMT Enterprise Architect has the primary responsibility for maintaining a catalog of services and for steering the architecture of individual solutions towards use of the enterprise services and software.

6.2.2.5 STANDARD ENTERPRISE SOLUTION PATTERNS

One of the primary objectives and standardization strategies of the ESA is the establishment and maintenance of standard enterprise solution patterns. Standard solution patterns include guidance and specifications on implementation methods, platforms, tools/technologies, service/component reuse, available training, and available consulting support. Standard approaches and technologies for application software development are required to optimize human resource skills within the increasing complexity of the multi-tier development paradigm for Web and mobile applications (apps).

The cultural history of the State government has funded programs to create individual point solutions that are implemented on a dedicated technical infrastructure. Going forward programs “buy into” the standard solution patterns that are part of the ESA with necessary representation, participation, and collaboration from the CIOC. In the long run, the overall cost effectiveness of managing standard technologies and the ability for the enterprise to more effectively leverage technology for enhancing impact in business service delivery are optimized.

Also, standard solution patterns support and are facilitated by the State moving to a cloud computing environment where standard application platforms can be rapidly provisioned through a service catalog request.

Solution patterns are initially developed by a working group convened and empowered by the CIO and the CIOC to develop the details of the framework. The working group includes technical architects from a number of State Departments that have significant experience with software development and system integration.

The Enterprise Solution Patterns framework is used to give focus to the development and maintenance of solution patterns that have broad application across the State’s business lines. A list of potential solution patterns includes the following:

- Web Application
- Mobile Application
- Web Service
- Analytics Application

Any given application or system might not fit cleanly into exactly one of these patterns. The patterns are not meant to concisely categorize an application, but rather to provide guidance to the design, development, and deployment of applications that have significant elements from any and all patterns. The fundamental idea is to provide guidance on how to effectively implement solutions that fit one or more of the standard patterns.

Each solution pattern specification provides guidance for the common set of topics provided in Table 4.

Table 4: Common Set of Specification Areas for Each Solution Pattern

Guidance Area	Description
Implementation Methods and Best Practices	• Guidance provided on extensions to the standard SDLC methodology specific for the pattern.
Implementation Platforms	• Guidance provided (consistent with the State’s ETA) on platforms that are recommended for implementation.
Tools/Technologies	• Guidance provided that outlines appropriate and recommended tools and technologies applicable to the pattern.
Available Training and Consulting Support	• Guidance provided on useful and available training relevant to implementation of the pattern. Where appropriate, sources of potential consulting or 3rd party assistance will be identified.

6.2.2.6 THE ROLE OF THE ESA

Initial implementations of both the EA and the LOB Segment Architectures were developed during the second half of FY2012. Moving forward these architectures will be maintained and used as the goal or “north star” guidance for achieving the desired integration of all information assets, systems, and technologies. Individual technical solution projects obtain integration and standardization requirements from these architectures and design and implement the target systems in compliance with the architectures.

6.2.3 CONCEPTUAL SOLUTIONS ARCHITECTURE

The conceptual solutions architecture depicts the future state enterprise solutions architecture as a common model of the comprehensive set of services required to fulfill all business requirements for the State.

The conceptual solutions architecture is characterized as follows:

- Formative – The conceptual solutions architecture establishes the overarching structure of the ESA to organize vertical LOB solutions and horizontal services and to clarify stewardship leadership boundaries. It is an initial high level version implemented with the expectation that it will continue to be refined and expanded. The diagram organizes the solutions and services within three horizontal bands: 1) Enterprise Mission Systems or LOB solutions, 2) the Enterprise Support Systems, and 3) the Enterprise Services.
- Notional Approach – This set of solutions are notionally based on the defined business functions within the LOBs. A primary goal of the ESA is to move the State towards a rationalized set of solutions recognizing that the current state has over 700 applications or systems. There are approximately 200 business services associated with the LOBs within in the EBA layer and one business solution per business function supported by Enterprise Services provides a more reasonable portfolio size. Additionally, the implementation of COTS/GOTS packages (e.g.,

ERP system within the Enterprise Support Systems band of the future state model) further supports the consolidation.

- The set of Enterprise Services is also notionally based on the SRM identified in the EBA and defines a set of shared services for further evaluation and refinement.

6.2.3.1 LOB SERVICES

Some Departments are further along in the development of a future state ESA architecture for their associated LOBs and in those cases the conceptual solutions architecture must be perpetually updated with that information. Additional refinement to the ESA also occurs as a result of the segment architecture development, and this information is discussed in Appendix A.

6.2.3.2 ENTERPRISE SERVICES

One of the most important elements of the ESA is establishing the approach and framework for integrating the State’s applications or solutions going forward. As discussed above, this integration is primarily achieved through the Enterprise Common Services band within the ESA. It supports the services oriented framework that provides – independent of business function – a leverage-able foundation to support the reuse of applications, application capabilities, components, and business services.

Key concepts and considerations for future action regarding the Enterprise Services are outlined here.

- The organization and content for the services structure is originally based on the Federal SRM. This provides the State a vetted starting point, while making some adjustments that streamline the set to those services oriented to common shared use. The initial set of services derived from the SRM need to be continually assessed, refined, and prioritized for use in the State.

Table 5: Customer Management Services Domain Description

Service Types	Service Components
Customer Relationship Management	<ul style="list-style-type: none"> • Customer / Account Management – retains identifying information about the customers of the organization and their interest in specific services • Customer Analytics – the analysis of an organization’s customers as well as the scoring of third party information as it relates to an organization’s customers. • Contact and Profile Management – provides a comprehensive view of all customer interactions, including calls, email, correspondence and meetings; also provides for the maintenance of a customer’s account, business and personal information. • Partner Relationship Management – provides a framework to promote the effective collaboration between an organization and its business partners, particularly members of the distribution chain (e.g., channel and alliance partners, resellers, agents, brokers, and dealers) and other third parties that support operations and service delivery to an organization’s customers; includes performance evaluation of partners. • Customer Feedback – collect, analyze and handle comments and feedback from an organization’s customers.

- The enterprise services are organized within 2 levels; the rationale for this is to facilitate the appropriate stakeholder governance participation for requirements and change management.
- The Enterprise Mission Support Services are business functional services that are common in support of LOB mission activities and feature the management and persistence of key shared data. Examples include customer (citizen, resident, state employee, business partner) data retention, or common functions within the enterprise resource planning realm such as financial tracking, asset inventory tracking, or procurement execution.
- The Enterprise Common Services are common IT utility services such as collaboration, digital content management, or geospatial visualization.

- The level of the conceptual solutions architecture establishes an organizational structure, scope and boundaries, and business objectives for these services. Oversight of this architecture should move into a next phase to detail requirements and to determine opportunities to prototype/pilot, and to determine an overall implementation approach.

Descriptions of each of the service domains are discussed below organized within the two layers of Enterprise Mission Support Services and Enterprise Common Services.

ENTERPRISE MISSION SUPPORT SERVICES

Customer Management Services

The Customer Services Domain consists of the capabilities and persistent information that are directly related to the end customer, the interaction between the business and the customer, and the customer-driven activities or functions. Table 5 provides a description of these areas.

Service Types	Service Components
Customer Preferences	<ul style="list-style-type: none"> • Personalization – defines the set of capabilities to change a user interface and how data is displayed. • Subscriptions – defines the set of capabilities that allow a customer to join a forum, listserv, or mailing list. • Alerts and Notifications – defines the set of capabilities that allow a customer to be contacted in relation to a subscription or service of interest.
Customer Assistance	<ul style="list-style-type: none"> • Self-Service – defines the set of capabilities that allow an organization’s customers to sign up for a particular service at their own initiative. • Reservations / Registration – defines the set of capabilities that allow electronic enrollment and confirmations for services. • Multi-Lingual Support – defines the set of capabilities that allow access to data and information in multiple languages. • Assistance Request - defines the set of capabilities that support the solicitation of support from a customer. • Scheduling - defines the set of capabilities that support the plan for performing work or service to meet the needs of an organization’s customers.
Customer Case Management	<ul style="list-style-type: none"> • Customer Case Management – defines the set of capabilities for identifying and tracking the history of claims or investigations for a customer and presumption of a particular case or investigation within its workflow

The Business Management Services Domain consists of the capabilities that support the management and execution of business functions and organizational activities that maintain continuity across the business and value-chain participants.

Table 6: Business Management Services Domain Description

Service Types	Service Components
Organizational Management	<ul style="list-style-type: none"> • Organizational Management – defines the set of capabilities that support management of all levels of organization within the enterprise, including the organization hierarchy structure; all inherent levels such as departments, agencies, divisions, branches, etc.; and the identification of executives, managers, and staff members within the various sub-groups of the organization.
Program/Project Management	<ul style="list-style-type: none"> • Program/Project Management – defines the set of capabilities that support management of programs and projects, as well as more ad hoc workgroups of multiple users working on related tasks; and the associated executives, managers, and staff members.
Process Management	<ul style="list-style-type: none"> • Change Management – defines the set of capabilities that control the process for updates or modifications to the existing business processes of an organization. • Configuration Management – defines the set of capabilities that control the environments, as well as documents of an organization. • Requirements Management – defines the set of capabilities that gather, analyze, and fulfill the needs and prerequisites of an organization’s efforts. • Governance / Policy Management – defines the set of capabilities intended to influence and determine decisions, actions, business rules and other matters within an organization.

Table 6: Business Management Services Domain Description

Service Types	Service Components
Process Management	<ul style="list-style-type: none"> • Quality Management - defines the set of capabilities intended to help determine the level of assurance that a product or service will satisfy certain requirements. • Business Rule Management – defines the set of capabilities for the management of the enterprise processes that support an organization and its policies. • Risk Management – defines the set of capabilities that support the identification and probabilities or chances of hazards as they relate to a task, decision or long-term goal; includes risk assessment and risk mitigation
Investment Management	<ul style="list-style-type: none"> • Strategic Planning and Management – defines the set of capabilities that support the determination of long-term goals and the identification of the best approach for achieving those goals. • Portfolio Management – defines the set of capabilities that support the administration of a group of investments held by an organization. • Performance Management – defines the set of capabilities for measuring the effectiveness of an organization’s financial assets and capital.
Resource Planning and Allocation	<ul style="list-style-type: none"> • Resource Planning and Allocation – defines the set or capabilities that support the determination of strategic direction, the identification and establishment of programs and processes, and the allocation of resources (capital and labor) among those programs and processes.

KNOWLEDGE MANAGEMENT SERVICES

The Business Management Services Domain consists of the capabilities that support the management and execution of business functions and organizational activities that maintain continuity across the business and value-chain participants.

Table 7: Knowledge Management Services Domain Description

Service Types	Service Components
Knowledge Management	<ul style="list-style-type: none"> • Categorization – defines the set of capabilities that allow classification of data and information into specific layers or types to support an organization. • Knowledge Engineering – defines the set of capabilities that support the translation of knowledge from an expert into the knowledge base of an expert system. • Knowledge Capture – defines the set of capabilities that facilitate collection of data and information. • Knowledge Distribution and Delivery - defines the set of capabilities that support the transfer of knowledge to the end customer.
Information Management	<ul style="list-style-type: none"> • Information Retrieval – defines the set of capabilities that allow access to data and information for use by an organization and its stakeholders. • Information Mapping / Taxonomy – defines the set of capabilities that support the creation and maintenance of relationships between data entities, naming standards and categorization. • Information Sharing – defines the set of capabilities that support the use of documents and data in a multi-user environment for use by an organization and its stakeholders.

The ERP Services Domain consists of the capabilities that support the management of enterprise planning transactional-based functions.

Table 8: ERP Services Domain Description

Service Types	Service Components
Financial Management	<ul style="list-style-type: none"> • Billing and Accounting – defines the set of capabilities that support the charging, collection and reporting of an organization’s accounts. • Credit / Charge – defines the set of capabilities that support the use of credit cards or electronic funds transfers for payment and collection of products or services. • Expense Management – defines the set of capabilities that support the management and reimbursement of costs paid by employees or an organization. • Payroll – defines the set of capabilities that involve the administration and determination of employee’s compensation. • Payment/ Settlement – defines the set of capabilities that support the process of accounts payable. [Component and definition discovered in CRM dated 5/05] • Debt Collection – defines the set of capabilities that support the process of accounts receivable. • Revenue Management – defines the set of capabilities that support the allocation and re-investment of earned net credit or capital within an organization. • Internal Controls – defines the set of capabilities that support the methods and procedures used by the organization to safeguard its assets, produce accurate accounting data and reports, contribute to efficient operations, and encourage staff to adhere to management policies and mission requirements. [Added in FY06 submission; definition from CRM dated 5/05] • Auditing – defines the set of capabilities that support the examination and verification of records for accuracy. • Activity – Based Management – defines the set of capabilities that support a defined, specific set of finance-related tasks for a given objective. • Currency Translation - defines the set of capabilities that support the calculations and differences among multiple mediums of exchange.
Human Resources	<ul style="list-style-type: none"> • Recruiting – defines the set of capabilities that support the identification and hiring of employees for an organization. • Resume Management – defines the set of capabilities that support the maintenance and administration of one’s professional or work experience and qualifications. • Career Development and Retention – defines the set of capabilities that support the monitoring of performance as well as the professional growth, advancement, and retention of an organization’s employees. • Time Reporting – defines the set of capabilities that support the submission, approval and adjustment of an employee’s hours. • Awards Management – defines the set of capabilities that support the recognition of achievement among employees of an organization. • Benefit Management – defines the set of capabilities that support the enrollment and participation in an organization’s compensation and benefits programs. • Retirement Management - defines the set of capabilities that support the payment of benefits to retirees.

Table 8: ERP Services Domain Description

Service Types	Service Components
Human Resources	<ul style="list-style-type: none"> • Personnel Administration – defines the set of capabilities that support the matching between an organization’s employees and potential opportunities as well as the modification, addition and general upkeep of an organization’s employee-specific information. • Education / Training – defines the set of capabilities that support the active building of employee competencies to include the range of training from professional development to general awareness training. • Health and Safety – defines the set of capabilities that support the security and physical well-being of an organization’s employees. • Travel Management – defines the set of capabilities that support the transit and mobility of an organization’s employees for business purposes.
Human Capital Management	<ul style="list-style-type: none"> • Skills Management – defines the set of capabilities that support the proficiency of employees in the delivery of an organization’s products or services. • Workforce Directory / Locator – defines the set of capabilities that support the listing of employees and their whereabouts. • Contingent Workforce Management – defines the set of capabilities that support the continuity of operations for an organization’s business through the identification of alternative organization personnel. • Workforce Acquisition / Optimization – defines the set of capabilities that support the hiring and re-structuring of employees and their roles within an organization.
Assets/Materials Management	<ul style="list-style-type: none"> • Property / Asset Management – defines the set of capabilities that support the identification, planning and allocation of an organization’s physical capital and resources. • Asset Cataloging / Identification – defines the set of capabilities that support the listing and specification of available assets. • Asset Transfer, Allocation, and Maintenance – defines the set of capabilities that support the movement, assignment, and replacement of assets. • Facilities Management – defines the set of capabilities that support the construction, management, and maintenance of facilities for an organization. • Computers / Automation Management – defines the set of capabilities that support the identification, upgrade, allocation and replacement of physical devices, including servers and desktops, used to facilitate production and process-driven activities.

Table 8: ERP Services Domain Description

Service Types	Service Components
Supply Chain Management	<ul style="list-style-type: none"> • Procurement - defines the set of capabilities that support the ordering and purchasing of products and services. • Sourcing Management – defines the set of capabilities that support the supply of goods or services as well as the tracking and analysis of costs for these goods. • Inventory Management – defines the set of capabilities that provide for the balancing of customer service levels with inventory investment. • Catalog Management – defines the set of capabilities that support the listing of available products or services that an organization offers. • Ordering / Purchasing – defines the set of capabilities that allow the placement of request for a product. • Invoice / Requisition Tracking and Approval – defines the set of capabilities that support the identification of where a shipment or delivery is within the business cycle. • Storefront / Shopping Cart - defines the set of capabilities that support the online equivalent of the supermarket cart, where orders and merchandise are placed. • Warehouse Management – defines the set of capabilities that provide for the storage and movement of materials within a warehouse, including these processes: material receipt, order picking, packaging, labeling, and shipping. • Returns Management – defines the set of capabilities for collecting, analyzing, and resolving product returns or service cancellations. • Logistics and Transportation – defines the set of capabilities that provide for efficient freight and traffic management.

SERVICE MANAGEMENT SERVICES

The Service Management Services Domain consists of the capabilities that support the development, management, execution, performance tracking, and continuous improvement of business services.

Table 9: Service Management Services Domain Description

Service Types	Service Components
Service Portfolio Management	<ul style="list-style-type: none"> • Service Portfolio Management – defines the set of capabilities that facilitate the creation and maintenance of products and services, including the design of service levels. • Service Demand Management – defines the set of capabilities that facilitate the promotion of a product or service, and the management of customer needs and service demand, and the management of customer service agreements.
Service Analytics	<ul style="list-style-type: none"> • Service Analytics - defines the set of capabilities that allow for the extraction, aggregation, and presentation of information to facilitate decision analysis and business evaluation, specifically analysis of service performance, customer satisfaction, and continuous improvement.

ENTERPRISE COMMON SERVICES

Data Management Services

The Data Management Services Domain consists of the capabilities that provide for the usage, processing and general administration of structured data and databases.

Table 10: Data Management Services Domain Description

Service Types	Service Components
Data Management	<ul style="list-style-type: none"> • Data Exchange – defines the set of capabilities that support the interchange of information between multiple systems or applications; includes verification that transmitted data was received unaltered. • Data Mart – defines the set of capabilities that support a subset of a data warehouse for a single department or function within an organization. • Data Warehouse – defines the set of capabilities that support the archiving and storage of large volumes of data. • Meta Data Management – defines the set of capabilities that support the maintenance and administration of data that describes data. • Data Cleansing – defines the set of capabilities that support the removal of incorrect or unnecessary characters and data from a data source. • Extraction and Transformation – defines the set of capabilities that support the manipulation and change of data. • Loading and Archiving – defines the set of capabilities that support the population of a data source with external data. • Data Recovery – defines the set of capabilities that support the restoration and stabilization of data sets to a consistent, desired state. • Data Classification – defines the set of capabilities that allow the classification of data.

ANALYTICAL SERVICES

The Analytical Services Domain consists of the capabilities that support the extraction, aggregation, and presentation of information to facilitate decision analysis and business evaluation.

Table 11: Analytical Services Domain Description

Service Types	Service Components
Analysis and Statistics	<ul style="list-style-type: none"> • Mathematical – defines the set of capabilities that support the formulation and mathematical analysis of probabilistic models for random phenomena and the development and investigation of methods and principles for statistical inference. • Structural / Thermal – defines the set of capabilities that support the use of data flow and data modeling diagrams for applying systematic analysis of data. • Radiological – defines the set of capabilities that support the use of radiation and x-ray technologies for analysis and scientific examination. • Forensics – defines the set of capabilities that support the analysis of physical elements using science and technology for investigative and legal purposes.

Table 11: Analytical Services Domain Description

Service Types	Service Components
Visualization	<ul style="list-style-type: none"> • Graphing / Charting – defines the set of capabilities that support the presentation of information in the form of diagrams or tables. • Imagery – defines the set of capabilities that support the creation of film or electronic images from pictures or paper forms. • Multimedia – defines the set of capabilities that support the representation of information in more than one form to include text, audio, graphics, animated graphics and full motion video. • Mapping / Geospatial / Elevation / GPS – defines the set of capabilities that provide for the representation of position information through the use of attributes such as elevation, latitude, and longitude coordinates.
CAD	<ul style="list-style-type: none"> • CAD - defines the set of capabilities that support the design of products with computers.
Knowledge Discovery	<ul style="list-style-type: none"> • Data Mining - defines the set of capabilities that provide for the efficient discovery of non-obvious, valuable patterns and relationships within a large collection of data. • Modeling – defines the set of capabilities that develop descriptions to adequately explain relevant data for the purpose of prediction, pattern detection, exploration or general organization of data. • Simulation – defines the set of capabilities that utilize models to mimic real-world processes.
Business Intelligence	<ul style="list-style-type: none"> • Demand Forecasting/Mgmt. – defines the set of capabilities that facilitate the prediction of sufficient production to meet an organization’s sales of a product or service. • Balanced Scorecard – defines the set of capabilities that support the listing and analyzing of both positive and negative impacts associated with a decision. • Decision Support and Planning – defines the set of capabilities that support the analyze information and predict the impact of decisions before they are made.
Reporting	<ul style="list-style-type: none"> • Ad Hoc – defines the set of capabilities that support the use of dynamic reports on an as needed basis. • Standardized / Canned –defines the set of capabilities that support the use of pre-conceived or pre-written reports. • OLAP - defines the set of capabilities that support the analysis of information that has been summarized into multidimensional views and hierarchies.

SOFTWARE DEVELOPMENT AND INTEGRATION SERVICES

The Software Development and Integration Services Domain consist of the capabilities that provide communication between hardware/software applications and the activities associated with deployment of software applications.

Table 12: Software Development and Integration Services Domain Description

Service Types	Service Components
Software Development and Integration	<ul style="list-style-type: none"> • Legacy Integration – defines the set of capabilities that support the communication between newer generation hardware/software applications and the previous, major generation of hardware/software applications. • Enterprise Application Integration – defines the set of capabilities that support the redesigning of disparate information systems into one system that uses a common set of data structures and rules. • Data Integration – defines the set of capabilities that support the organization of data from separate data sources into a single source using middleware or application integration as well as the modification of system data models to capture new information within a single system. • Instrumentation and Testing – defines the set of capabilities that support the validation of application or system capabilities and requirements. • Software Development – defines the set of capabilities that support the creation of both graphical and process application or system software.

SECURITY MANAGEMENT SERVICES

The Security Management Services Domain consists of the capabilities that protect an organization’s information and information systems.

Table 13: Security Management Services Domain Description

Service Types	Service Components
Security Management	<ul style="list-style-type: none"> • Identification and Authentication – defines the set of capabilities that support obtaining information about those parties attempting to log on to a system or application for security purposes and the validation of those users. • Access Control – defines the set of capabilities that support the management of permissions for logging onto a computer, application, service or network; includes user management and role/ privilege management. • Cryptography - Support the use and management of ciphers, including encryption and decryption processes, to ensure confidentiality and integrity of data. • Digital Signature Management – defines the set of capabilities that supports the use and management of electronic signatures to support authentication and data integrity; includes public key infrastructure (PKI). • Intrusion Prevention - Includes penetration testing and other measures to prevent unauthorized access to a government information system. • Intrusion Detection – defines the set of capabilities that support the detection of unauthorized access to a government information system. • Incident Response - provides active response and remediation to a security incident that has allowed unauthorized access to a government information system.

Table 13: Security Management Services Domain Description

Service Types	Service Components
Security Management	<ul style="list-style-type: none"> • Audit Trail Capture and Analysis – defines the set of capabilities that support the identification and monitoring of activities within an application, system, or network. • Certification and Accreditation - supports the certification and accreditation (C&A) of information systems, as described in NIST SP800-37. • FISMA Management and Reporting - supports management and reporting of compliance with the Federal Information Security Management Act of 2002. • Virus Protection - provides anti-virus service to prevent, detect, and remediate infection of government computing assets.

The Collaboration Services Domain consists of the capabilities that allow for the concurrent, simultaneous communication and sharing of content, schedules, messages, and ideas within an organization.

Table 14: Collaboration Services Domain Description

Service Types	Service Components
Collaboration	<ul style="list-style-type: none"> • Email - defines the set of capabilities that support the transmission of memos and messages over a network. • Threaded Discussions – defines the set of capabilities that support the running log of remarks and opinions about a given topic or subject. • Document Library – defines the set of capabilities that support the grouping and archiving of files and records on a server. • Shared Calendaring – defines the set of capabilities that allow an entire team as well as individuals to view, add and modify each other’s schedules, meetings and activities. • Task Management – defines the set of capabilities that support a specific undertaking or function assigned to an employee.

COMMUNICATION SERVICES

The Communications Services Domain consists of the capabilities that provide communication between hardware/software applications and the activities associated with deployment of software applications.

Table 15: Communication Services Domain Description

Service Types	Service Components
Communications	<ul style="list-style-type: none"> • Real Time / Chat – defines the set of capabilities that support the conferencing capability between two or more users on a local area network or the Internet. • Instant Messaging – defines the set of capabilities that support keyboard conferencing over a Local Area Network or the Internet between two or more people. • Audio Conferencing – defines the set of capabilities that support audio communications sessions among people who are geographically dispersed. • Video Conferencing – defines the set of capabilities that support video communications sessions among people who are geographically dispersed. • Event / News Management – defines the set of capabilities that monitor servers, workstations and network devices for routine and non-routine events. • Community Management - defines the set of capabilities that support the administration of online groups that share common interests. • Computer / Telephony Integration - supports the connectivity between server hardware, software and telecommunications equipment into a single logical system. • Voice Communications – defines the set of capabilities that provide telephony or other voice communications.

SEARCH SERVICES

The Search Services Domain consists of the capabilities that provide for the probing and lookup of specific information and data from information and data sources.

Table 16: Search Services Domain Description

Service Types	Service Components
Search	<ul style="list-style-type: none"> • Query – defines the set of capabilities that support retrieval of records that satisfy specific query selection criteria. • Precision / Recall Ranking – defines the set of capabilities that support selection and retrieval of records ranked to optimize precision against recall. • Classification – defines the set of capabilities that support selection and retrieval of records organized by shared characteristics in content or context. • Pattern Matching – defines the set of capabilities that support retrieval of records generated from a data source by imputing characteristics based on patterns in the content or context.

SYSTEMS MANAGEMENT SERVICES

The Systems Management Services Domain consists of the capabilities that support the administration and upkeep of an organization’s technology assets, including the hardware, software, infrastructure, licenses, and components that comprise those assets.

Table 17: Systems Management Services Domain Description

Service Types	Service Components
Systems Management	<ul style="list-style-type: none"> • License Management – defines the set of capabilities that support the purchase, upgrade and tracking of legal usage contracts for system software and applications. • Remote Systems Control – defines the set of capabilities that support the monitoring, administration and usage of applications and enterprise systems from locations outside of the immediate system environment. • System Resource Monitoring – defines the set of capabilities that support the balance and allocation of memory, usage, disk space and performance on computers and their applications. • Software Distribution – defines the set of capabilities that support the propagation, installation and upgrade of written computer programs, applications and components. • Issue Tracking – defines the set of capabilities that receive and track user-reported issues and problems in using IT systems, including help desk calls.

6.3 ESA TRANSITION AND SEQUENCING PLANNING SUMMARY

Considerations for “go forward” requirements and implications for the T&S Plan have been organized in two focus areas:

- Stabilize – to address urgent needs to stabilize the legacy environment of the State’s application solutions.
- Rationalize and Integrate – to modernize the overall solutions architecture by “right-sizing” the number and scope of the future set of solutions and implementing the long-term integration strategies.

Activities will take place in these areas in parallel, but the activity emphasis moves from urgent and immediate actions to strategic and long-term.



6.3.1 STABILIZE

6.3.1.1 ADDRESS CURRENT “FLAGSHIP” OPPORTUNITIES

Consistent with recommendations in the Final Report, the CIO and OIMT will pursue opportunities that exist with current funded systems development projects to lay enterprise foundations for solutions and infrastructure. As OIMT continues to move forward on development of the enterprise future state vision and architecture and in understanding in greater detail the scope of current funded initiatives, opportunities to jointly establish portions of enterprise solutions and infrastructure will be sought after. Opportunities may exist for potential reuse or consolidation with other efforts, in establishing enterprise standards or practices, or implementing key components of the future state enterprise infrastructure. Examples are outlined below in Table 18.

Table 18: Opportunities for Flagship Projects to Lay Enterprise Foundations

Service Types	Key Project Description	Implications for the Enterprise
DHS	New MedQuest Eligibility System (Affordable Care Act) Pending Review million new eligibility system to increase timeliness and transparency, electronically verify information, and interface with health insurance exchange. Replaces current 23 year old system.	Establish and leverage enterprise application integration capabilities
DHS	Benefit, Employment, and Support Services Division BPR Project BPR evaluation of the existing financial assistance and SNAP eligibility process, redesign work flow processes for efficiencies in issuing benefits; address document imaging and e-forms and portable devices to allow DHS staff to be more mobile in addressing routine tasks (e.g. child care licensing) and for responding to emergency disasters (e.g. emergency food stamps); explore the possibility of expanding the concept of telecommuting with the availability of portable devices.	Establish and leverage enterprise capabilities in BPR methodology, mobile apps, and telecommuting
AG	Hawai'i Integrated Justice Information Sharing Program (HIJIS) Strategic initiative to build enterprise-wide integrated information sharing capabilities between justice agencies and other government entities throughout the State to improve public safety and enhance the efficiency of operations.	One of the largest, most successful information sharing initiatives in the State – pattern for broader adoption
DOH	Hawai'i Health Data Warehouse Strategic initiative to standardize the collection and management of Hawai'i's health data; dedicated to providing useful data to support public health professionals, the community and health agencies to become more effective in the application of health data.	One of the most successful data sharing initiatives in the State – pattern for broader adoption
DOTAX	Tax Modernization Strategic initiative to explore ways to streamline and modernize tax processing electronically so that it is more cost effective and efficient.	Position enterprise for broader Financial Management improvements
HHSC	Health IT Health information technology initiative to improve the quality and efficiency of health care through electronic health record (EHR).	Establish and leverage enterprise application integration capabilities
DBED/DCA	Hawai'i Broadband Initiative A major economic development initiative to provide statewide access to affordable ultra, high-speed Internet by 2018. Positions Hawai'i to be the first state in the nation with 1 gigabit per second broadband connectivity at every public school, every public library, and every public university and college campus by using about Pending Review of federal monies received through the American Recovery and Reinvestment Act (ARRA).	Leverage connectivity for State offices at remote islands and improvements for State NGN

6.3.1.2 LEGACY APPLICATION SOLUTION UPGRADES

As the State modernizes its solution platforms, there will be a number of compelling drivers to re-platform sets of applications. Some notable reasons would be the age and condition of the platform, such as the legacy mainframe applications; or that a platform may be eliminated such as Lotus Domino. This initiative would assess and stabilize critical applications. An analysis of the overall applications portfolio will identify the top risk areas. Projects will be authorized to plan and work through conversions, upgrades, and refreshes to stabilize the applications. Examples include:

- Continue work underway to implement near-term enhancements to the legacy payroll system to automate EFT to minimize demands for check printing.
- Stabilize the email system versions and enhance overall enterprise capabilities including addressing a global address list and shared calendaring.
- Migrate current Lotus Domino applications to a standard enterprise solution pattern for web applications.

The portfolio management process and program is being established along with other IT/IRM programs in OIMT such as the EA program. The applications perspective of the portfolio management process will include considerations for the appropriate life cycle of all applications software and plan for its replacement at the proper time. Create application

technology lifecycle management and refresh plans. This initiative is included in the ETA, Section 7 below.

6.3.2 RATIONALIZE AND INTEGRATE

6.3.2.1 IMPLEMENT ERP SYSTEM

The State is moving forward with implementation of an enterprise-wide ERP system that will replace the large majority of the current “central” systems within the Enterprise Support Services band. The conceptual solutions architecture has established a notional set of current systems that should be replaced by the ERP system. The ERP implementation is a critical foundational component of the future strategy. As stated in the Final Report, the proliferation

of many applications within the current state architecture is the result of the significant issues that the Departments have with the common central systems. A significant percentage of the goals and objectives related to business and IT/IRM transformation can be accomplished through a successful ERP system implementation. The plan for ERP implementation is specified in more detail in Appendix A.

6.3.2.2 IMPLEMENT OTHER ENTERPRISE SOLUTIONS

Additional significant opportunities exist for standardizing on common systems to support enterprise needs. Specific investment initiatives should be considered for the following critical areas, and the working groups in alignment with the technology domains within the ETA provide additional detail on these initiatives.

ENTERPRISE EMAIL SYSTEM

Evaluate options for upgrade or replacement of the current email system to address a number of current issues such as the lack of a global address list or shared calendaring and to enhance the overall future enterprise capabilities for greater collaboration, migration towards smartphones and tablets, and greater efficiency and cost savings in from Total Cost of Ownership including future provisioning models “as a service”.

ENTERPRISE COLLABORATION SOLUTION

Establish standard collaboration solutions across the State adopting technology platforms such as Microsoft SharePoint or Lotus Domino Quickr (in conjunction with the email system initiative). Implement necessary technical underpinnings and connectivity for cross-departmental workgroup and project collaboration.

IDENTITY MANAGEMENT SOLUTION

Establish a standard solution for management of user account identity and authorized roles and access permissions integrated with standard user directory services and enterprise services for authentication.

ENTERPRISE DASHBOARD SOLUTION

Establish a standard management-level dashboard reporting solution with supporting data aggregation and summarization capabilities. Implement “rolling up” program-level information for project and operational performance, and institute processes for projects and operations to begin reporting.

OPEN GOVERNMENT SOLUTIONS

Establish a State of Hawai`i data.gov internal and public-facing web site to facilitate the sharing of “master data sets” as defined above. Support internal-facing (for State use as well as application integration through web services layered on top of XML data sets) and external, public-facing (for publishing public-domain master data sets). Establish an internal-facing web site to facilitate sharing of “master data sets” for application integration through web services layered on top of XML data sets.

KNOWLEDGE MANAGEMENT SOLUTION

Establish enterprise processes and system for knowledge management. Utilize for IT services knowledge management initially, but consider use and application in other service areas. For IT services, ensure that all documentation regarding IT environments; IT system and server configurations; and known problems, workarounds, solutions, and resolution scripts are all stored within the knowledge management repository. Ensure that IT workers at all levels use the knowledge management repository for environment and work instruction documentation.

CUSTOMER SERVICE SOLUTION (REQUEST AND INCIDENT REPORTING)

In conjunction with organizational changes to standardize on shared service centers such as an Enterprise IT Service Desk or other back office functions related to the ERP implementation, establish an enterprise-level service desk or call center solution with tracking for resolution of all customer or user service and support requests, incidents, and event resolution.

ENTERPRISE SYSTEM MANAGEMENT SOLUTION

Establish and implement an enterprise systems management solution, such as the SolarWinds product used in some organizations today. The enterprise systems management solution would automate basic availability (systems, service, and server uptime); capacity management (CPU, disk space, bandwidth, etc.); and security and data center operations. The solution would perform life cycle tracking of all events related to these areas and integrate event management information with the customer service solution.

6.3.2.3 ESTABLISH STANDARD ENTERPRISE SOLUTION PATTERNS

The State of Hawai`i will establish standard enterprise patterns for kinds of common solutions such as web applications, mobile applications, data analytics applications, and web services. As discussed above, the desired outcomes in establishing the patterns are as follows:

- Simplify and standardize to capitalize on staff expertise, reduce support costs, and to facilitate reusable code and data across the environment.
- Rapidly baseline current assumptions regarding sunset, legacy, preferred, and standard application platforms, architectural stacks, and technologies, and develop standards and guidance

regarding future technology decisions, specifically with respect to application architecture, design, and implementation for use and adoption across the Departments, Divisions, and programs; and create a communication plan to “market” the standards and guidance within each Department. Upgrade needed human resource skills for growth including both advanced training programs for staff and putting in place contractor resources.

- Leverage successful models, such as HIC’s work for DLNR or Ocean IT’s mobile app development for DOD, and adjust as needed to minimize the approaches used.

The State will approach the adoption of solution patterns in an evolutionary manner that moves the State through what are defined as four different Operating Levels as described in Table 19 below.

Table 19: Solution Pattern Operating Levels Indicating Evolution of Adoption within the Enterprise

Service Types	Level Characteristics
Opportunistic	At this initial level the state is looking for projects to attach to the initiative and include the definition of pattern artifacts in the project scope. The idea is to attach to projects that are on task to create applications that are prototypical of one of the solution patterns, and to capture and document the best practice guidelines being used by that project.
Tactical	At this level, projects will be selected that might benefit from one or more of the documented solution patterns. The initiative will attach these projects and offer pattern guidance and validate and improve the pattern guidance.
Strategic	At this level, use of pattern guidance should be relatively routine part of the development process. The initiative will be more focused on interacting with projects to determine the patterns they are using and incorporate any feedback, rather than offering counseling and guidance.
Managed	At this level the set of solution patterns are essentially complete and the initiative is focused on tracking the use of the patterns and recognizing the need for new patterns as technology advances.

Tracking the state’s progress through these four operational levels will facilitate the ongoing process of selling and obtaining funding for the Solution Patterns initiative by providing some quantifiable measurement of the adoption of and use of the patterns across the enterprise. Within this implementation framework, the State should continue to review, refine, and expand its set of enterprise solution patterns.

The initial set of priority patterns are outlined below and expanded in the ETA in Section 7.

ENTERPRISE WEB APPLICATION SOLUTION PATTERN

Standardize on common solution methods, architectures, and technologies for web applications development. The most common in use today within the State include the Linux/Apache/MySQL/PHP or Python (LAMP) stack, the Windows stack (Windows\IIS\SQL Server\.NET), and the Java web application stack (Linux or Solaris/Tomcat/JSP).

ENTERPRISE MOBILE APPLICATION SOLUTION PATTERN

Establish a standard mobile applications solution pattern and approach with standard methods, skill development, contractor resources, and tools/technologies. Conduct in conjunction with adoption of preferred smartphones and tablets in the future state technology architecture. Since mobile application development has a very small footprint in the State at this time, this initiative will need to analyze, pilot, and invest/implement in a standard approach, capabilities, and tools for developing mobile applications.

ENTERPRISE DATA ANALYTICS APPLICATION SOLUTION PATTERN

Establish a standard data analytics solution pattern and approach with standard methods, skilled resources, and tools. Evaluate and leverage, as appropriate, notable implementations of end-user data access systems to make critical data available for analysis and decision making, specifically: FAMIS Data Mart, DOH Data Warehouse, and Juvenile Justice Information System (JJIS).

ENTERPRISE APPLICATION INTEGRATION WEB SERVICE SOLUTION PATTERN

Establish a standard enterprise solution for application integration that includes standard approaches, methods, knowledge/expertise, skilled resources, and tools/technologies to enable and support web services implementation and use. Evaluate and leverage notable implementations of application data integration through advanced capabilities (e.g., SOA, specifically DOH Services Implementation and HIC).

COMMUNITY APPLICATION SOFTWARE “STORES”, REPOSITORIES, AND DIRECTORIES

In conjunction with establishing these standard application solution patterns, establish capabilities to facilitate application software subscription, download, or common source code reuse. There are two primary considerations: an app store to subscribe and download standard apps, and shared source code or web services for reuse in application development.

- App Store – anticipate future mobile apps for the State and establish “app stores” for internal marketing of existing application capabilities and the ability for organizations to reuse those applications – a version of an internal “apps store” catalog.
- Community Source Repository – anticipate reuse of considerable portions (services/components) of application code such as single sign on or payment processing. Ability to leverage shared source code across trusted communities within or outside the State using a SourceForge type collaboration environment. Include trusted specifications, component code, or application code from other states.
- Web Services Directory – anticipate future enterprise web services for the State and establish web service directories using industry standards such as UDDI (Universal Description, Discovery, and Integration) specifications.

6.3.2.4 IMPLEMENT ENTERPRISE APPLICATION INTEGRATION SERVICES

The State of Hawai‘i will achieve integration strategies across its enterprise and LOB application solutions through the implementation of an integration services layer within the ESA. Similar to the solution pattern implementation described above, these enterprise services, the State will approach the adoption of a services oriented applications development approach in an evolutionary manner that moves the state through the four different Operating Levels as outlined in Table 20.

Table 20: Services-Oriented Operating Levels Indicating Evolution of Adoption within the Enterprise

Operating Level	Level Characteristics
Opportunistic	At this initial level the state is beginning to prototype and defines its services-oriented development policies and procedures. Pilot projects are being selected based on their suitability for refining those policies and procedures, and for their suitability in proving out required technology elements of the EA. The focus is on selecting and investing in projects that will produce quick success and bolster the efforts to sell and fund an ongoing enterprise application integration initiative.
Tactical	At this level, rudimentary policies, procedures, and technology components are in place and are being refined based on lessons learned. Projects are being selected that focus the effort to build low level cross-cutting services that can be used by multiple lines of business. It is at this level that the details around versioning, testing, and deployment of services are being fleshed out.
Strategic	At this level, policies, procedures, and technology components are well established and the focus on investment in services-oriented development is on the retirement of legacy applications and infrastructure using the SOA model that builds replacement software incrementally using the technique of service composition.
Managed	At this level not only are the policy, procedure and technical components established and in widespread use, but there is an active and robust measurement and management program in place that tracks the use of developed services and focuses service development to improve performance and extend re-use opportunities.

Tracking the state’s progress through these four operational levels will facilitate the ongoing process of selling and obtaining funding for the enterprise integration initiative by providing some quantifiable measurement of the adoption of services-oriented principles across the enterprise.

Rather than define and build out a full governance and technology stack upon which to build SOA compliant services, the state will take an approach that provides for investment in projects that can incrementally fill out gaps in the EA, and incrementally bring governance processes and technology onboard. Consequently the selection of projects for SOA investment will be a critical success factor for the SOA implementation. Industry best practice research indicates that highly successful SOA based projects

can be roughly categorized into three different value categories:

- **SOA Integration Projects**
SOA Integration Projects employ industry open and standardized service technologies (XML, WSDL, etc.) to provide synchronization of data flow among applications, most notably between custom written applications and COTS software packages. The use of open and standard service technologies and design approaches often result in a much improved cost profile over older point-to-point custom interfaces or more traditional EAI software, e.g. SAP XI, Tibco, BizTalk, IBM MQSeries, MS MSMQ, etc.
- **New Composite Application Projects**
New custom written applications are largely Web based and consequently are well positioned to make use of SOA

service level components. Existing legacy applications, on the other hand, are not generally well-suited to service composite solutions because of their dependence on proprietary technologies and their highly stovepipe design focused on automating specific business processes. Identifying new applications that can benefit from a SOA approach of development of low level and composite services will provide for applications that are more maintainable, and that provide opportunities for component reuse by other applications.

- **Mainframe/Legacy Modernization Projects**

Mainframes and associated legacy applications often consume the lion’s share of an organization’s IT budget. Retiring those applications and associated

infrastructure can be a daunting and long term proposition, high in cost and full of risk. An incremental approach that can be used is to build out new user facing applications that leverage the existing legacy applications by interfacing with SOA wrapped services that abstract the functionality of the underlying legacy application. Creating these wrappers provides a migration path toward applications with new user facing technologies that continue to use the legacy functions of the existing applications. Over time, these new user facing applications built as a composition of services can be redirected toward new back-end services that replace the legacy functionality.

Unlike traditional approaches that use a rigorous waterfall approach to infrastructure build out, the SOA framework here is expected to be built out incrementally. It provides the State with the ability to select projects that can contribute to the SOA build out, regardless of the SOA operating level that is in play. Over time the state will realize a flexible SOA infrastructure and a rich inventory of services that provide for effective maintainability and high re-use.

Consistent with the notional set of enterprise services included in the Conceptual Solutions Architecture, the initial set of priority services are outlined below and included in the ETA, Section 7.

SUPPORT SERVICES — SECURITY — IDENTITY AND ACCESS MANAGEMENT

Establish a standard set of authentication and single sign on services for use by all enterprise applications.

DIGITAL ASSET SERVICES — DOCUMENT/RECORDS MANAGEMENT

Establish common services for identification and submission of digital content to be managed as an official document or record. Investigate current capabilities that exist: KOFAX and/or IBM FileNet within DOT, B&F, (and the Judiciary), AG, DAGS, DOTAX.

BUSINESS ANALYTICS SERVICES — GEOSPATIAL

Establish common services for linking and visualizing State data with geospatial data. Investigate current capabilities such as ARCGIS within DOD, DAGS, DOT, DBEDT, DLNR, DOH, HDOA, AG, DOE, and UH.

BUSINESS ANALYTICS SERVICES — DASHBOARD REPORTING

Establish common services for reporting performance data against measures that need to be reported in a common dashboard reporting solution.

BACK OFFICE SERVICES — ERP

Establish common services within the financial management and human resource management domains in conjunction with the ERP implementation.

PROCESS AUTOMATION SERVICES — WORKFLOW

Establish common services to support enterprise workflow across application solutions.

PROCESS AUTOMATION SERVICES — CASE MANAGEMENT

Establish common services to support a case management life cycle and data reuse across application solutions.

CUSTOMER SERVICES — EVENT/ INCIDENT/REQUEST REPORTING

Establish common services to support reporting of events, incidents, or requests that need to be tracked in a common customer service solution.



7.0 ENTERPRISE TECHNOLOGY ARCHITECTURE

ENTERPRISE TECHNOLOGY ARCHITECTURE

The ETA is defined as a “logically consistent set of principles, practices, standards, and guidelines that are derived from business requirements and that guide the creation of an organization’s technical infrastructure.” For the State of Hawai`i, the ETA represents the technology infrastructure environment that must support the ESA in terms of the Enterprise Mission Systems, Enterprise Support Systems, and Enterprise Services bands.

The following sections describe the current state of the ETA, the future state vision, and the gap closure activities that will be represented in the T&S Plan. In addition, the working documents that have been created by the various Technology Working Groups are available in a separate Supplemental Addendum to this document. A hyperlink to this addendum and the specific working group information is provided where appropriate.



7.1 ETA CURRENT STATE

The current state of the ETA, identified as part of the Final Report, is very decentralized because it supports a very decentralized ESA and EIA. The rationale for this decentralization is the same as described previously in the EBA, EIA, and ESA (i.e., funding sources, lack of standards provided by an EA, historic lack of a State CIO and governance). Figure 27 depicts the ETA and the lack of integration and alignment statewide.

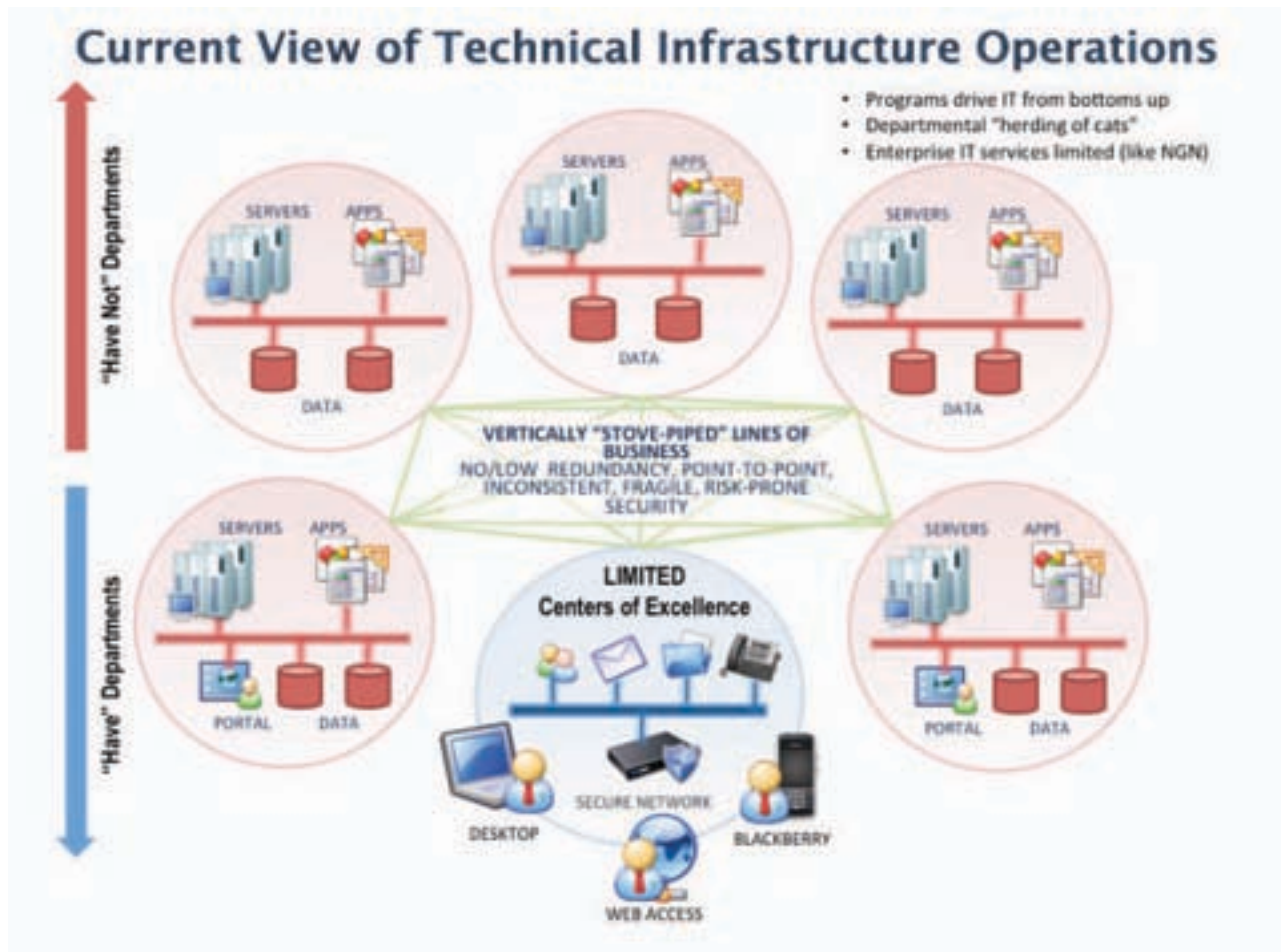


Figure 27: Current State ETA

The current state of technology within the State are summarized in Table 21 and organized by architectural domains associated with the ETA. In some instances, a number of Departments have strong technical solutions in place, those instances have been identified in the table but overall represent a very small portion of IT and still do not adhere to a consistent approach when viewed enterprise wide. The current state technology device type data within the EA repository includes approximately 6400 different product types being used at present. And currently the State has approximately: 15 server rooms (based on a < 500 square feet measure), five server closets (based on < 200 sq. ft.), and three data centers performing hosting services. Both of these factors indicate the opportunity for consolidation and consistency.

Table 21: Technical Architecture Domain/Sub-Domain and Current State of Technology Details

Technical Architecture Domain	Sub-Domain	Current Environment Details
Collaboration and Messaging	Email	Lotus Notes – most pervasive across all Departments, departments running 6.0, 6.5, 7.0 and 7.5
		Some instances of Exchange (Employee Retirement System (ERA), Employee and Union Trust Fund (EUTF), DOE, DOH, Attorney General (AG)-HCJDC)
		UH is migrating to Google Mail (Cloud-based)
	Broadcast, User Messaging, and Social Media	Emerging interest in and use of Twitter, Facebook (Governor’s and Lieutenant Governor’s Offices, Department of Hawaiian Home Lands (DHHL))
		Broadcast messaging products used in State Civil Defense and University of Hawai‘i (UH)
	Collaborative Workspaces	No standard enterprise solution selected for collaboration
		SharePoint purchased for use in DOE, DOH, Budget and Finance (B&F), Office of Hawai‘i an Affairs (OHA)
		Minimal use of Lotus/Domino for collaboration
		UH is utilizing Google Apps
		DOT is utilizing Lotus/Domino TeamRoom
Information Management	Document Management	No standard enterprise solution
		Document and imaging system components KOFAX and IBM FileNet being used in Department of Transportation (DOT), B&F, OHA, Department of Accounting and General Services (DAGS)
		Adobe and Microsoft Office products are prevalent across all Departments
		Global 360 Imaging and Workflow software are implemented and used by Department of Commerce and Consumer Affairs (DCCA)
		AG and Department of Business Economic Development and Tourism (DBEDT) are utilizing DropBox
	Data Management	Oracle, SQL Server, MySQL, Adabas, APPX, DB2
		Crystal Reports is used in DOTAX
	Analysis, Visualization and Reporting	Oracle Discoverer is used by DOT
	GIS	ARCInfo used in DOD, DAGS, DOT, DBEDT, Department of Land and Natural Resources (DLNR), DOH, Department of Agriculture (HDOA), AG, DOE, UH

Table 21: Technical Architecture Domain/Sub-Domain and Current State of Technology Details

Technical Architecture Domain	Sub-Domain	Current Environment Details
Application Environments	Application Interaction and Integration	Enterprise Services Bus technologies used in DOH and HIJIS
		IBM Rational Architect
	Client Server Applications	PowerBuilder is implemented.
	Web Applications	Java, .Net, PHP, Perl, Oracle Forms used across the State
	Mobile Applications	Emerging need identified with only Department of Defense (DOD) having a non-public-facing one, MERCI
	Embedded Systems	Control systems for DOT
Infrastructure	Directory Services	External DNS servers reside on the Information and Communications Services Division (ICSD) network
		Most Departments have internal DNS servers
		Centralized Active Directory does not exist; numerous Departments deploy Active Directory to manage local infrastructure
	Enterprise Systems Management (configuration, performance, capacity, availability, licensing, patching)	No enterprise-wide fault, configuration, performance, or capacity management tools exist in the State
		Each Department is responsible for monitoring and managing its own infrastructure
		Decentralized annual software license management
	Servers and Storage	Very diverse with no consistency in terms of vendor products
	Hosting Environments, Cloud, and Data Center	Server-hosted environment at ICSD
		Very diverse with no consistency in terms of vendor products
	Disaster Recovery	DLNR has an installation with DRFortress
		HIC recently migrated to SystemMetrics Endeavor data center
		ICSD uses Veritas and Tivoli to perform tape and data backups
	Unified Communications	ICSD-managed video conference center established to support, schedule, and troubleshoot
		Contains multiple video bridges for large conference support
		DBEDT utilizes Skype to communicate with non-State business prospects
Majority of the State utilizes Hawaiian Telcom (HATS) contract for Centrex phone services		
Some key systems exist as do small pockets of VoIP		
Many employees utilize their personal cellular and/or smartphones or iPhones for non-office voice service		
Network	Wired	ICSD-managed Cisco-based MPLS network is structured to provide services to all Departments
		Each Department supports internal LAN with mixed vendor networks
	Wireless	No Wi-Fi policy or enterprise solution is available to the Departments
		Departments have deployed Wi-Fi independently where required
		“Rogue” access points exist as end users install consumer WiFi devices

Table 21: Technical Architecture Domain/Sub-Domain and Current State of Technology Details

Technical Architecture Domain	Sub-Domain	Current Environment Details
Network	Radio	Robust Radio Frequency (RF)-based network is in place; however, it is a single threaded organization with one person in charge of all infrastructure
End User Computing	Desktops, Laptops, and Mobile Devices	Departments have discretion to buy desktop/laptop devices (most use Western States Contracting Alliance [WSCA] vehicle)
		No standard operating system or enterprise image exists
		All purchasing and warranty support is done at the Department level
	Many employees utilize their personal Smartphones or iPhones for non-office email service	
	User Productivity Software	Operating system is being driven by legacy applications; new PCs ship with Windows 7 but in many cases the Departments must downgrade them to Windows XP to run native legacy applications
User Presentation	No standard offerings exist for users to select software; the State is not leveraging enterprise-level discounts for common tools	
Peripherals	Printers, fax support. Each department is purchasing individual and workgroup peripherals	
Information Assurance and Privacy	Anti Virus/Spam	All Departments have endpoint security deployed via Symantec or similar offerings
	Security (Authentication, Authorization, Credentials, etc.)	There is no governance standard at the State level for secure authentication
		There is no hard-drive encryption policy
		Virtual Firewall and IPS deployed on NGN connections to each Department
	Some Departments engage third parties for penetration testing and security policy creation	
	Privacy	Lacking common PII controls to manage and monitor the electronic release of PII data via means such as email
Security Policy	Departments have standalone security devices which do not comply to a standard set of rules	
	ICSD has virtual firewall on departmental edge of NGN which protect the backbone network	

7.2 ETA FUTURE STATE

The future state vision for the State of Hawai`i's ETA enables rapid deployment of new services to the Departments, employees, and citizens. It supports the EBA, EIA, and ESA. As the ETA future state is implemented the following items should guide all decisions:

Guiding Principles for Implementing the ETA Future State

- Align Business and Technology - A Department's business and IT staffs understand its business functions and the role of technology in supporting these business functions. They jointly have the responsibility for defining IT needs and ensuring that the systems provide defined business benefits and that these systems are simultaneously aligned from a technical perspective with the ETA standards.
- Design for Sharing - Facilitating information sharing (within the Departments, the LOB, and across the enterprise) is a key consideration for all IT implementation actions.
- Incorporate Security Elements in Every Design - Designs for all new systems must include security (e.g., access and protection) requirements from the outset to ensure that the State is not vulnerable to threats.
- Design for Growth - Ensure the technical infrastructure investments accommodate growth to create the lowest total cost of ownership while creating the greatest flexibility for future growth.
- Design for Performance and Reliability Metering – Implement technology to capture performance measurements to support management and analysis of the IT environment.

7.2.1 ELEMENTS OF THE ETA FUTURE STATE VISION

Given the vision and tenets cited above, Figure 28 illustrates the key technical elements of the future state vision.

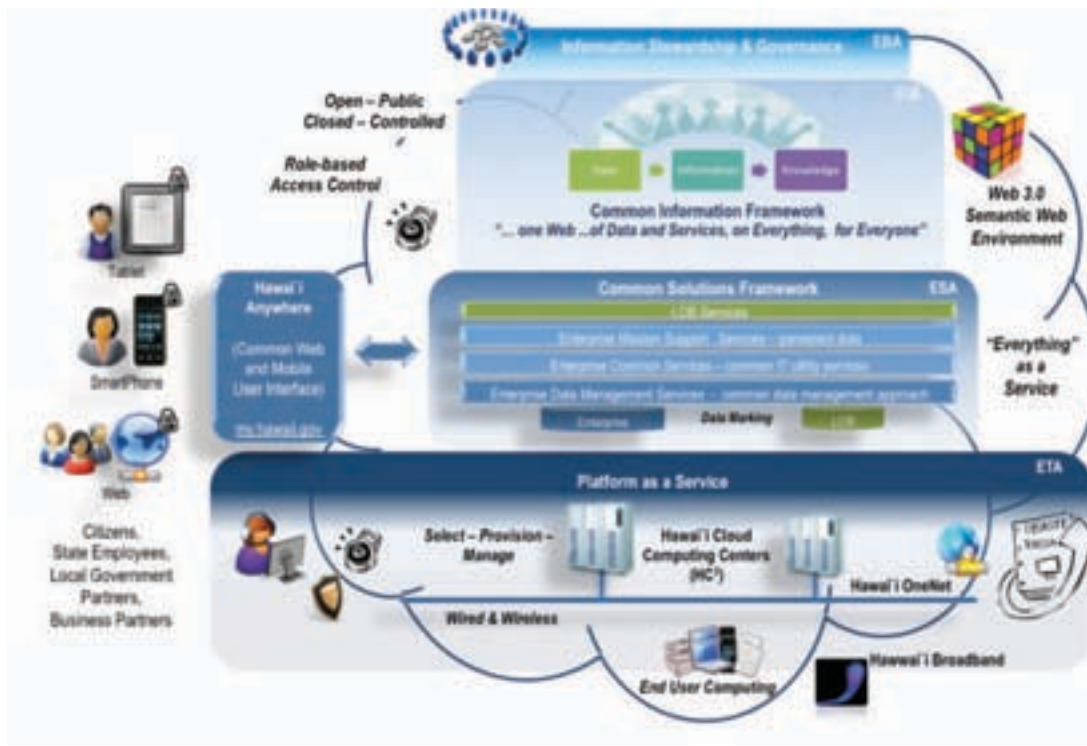


Figure 28: ETA Future State Vision for Hawai'i

The Strategic Plan, EBA, EIA, and ESA of the EA document a vision for the use of organization and governance, information, solutions, and technology within the State. The following defines the key attributes of the ETA layer:

- **Information Sharing:** Every Department can exchange and access information electronically, both internally within government and externally throughout the State, nation, and world in a secure manner and as authorized. ETA sets the technology standards for sharing information.
- **Collaboration:** Formal and informal groups work to break down barriers and provide consistent practices to share technology investments to support the delivery of business functions. ETA describes collaborative environments and content management approaches that brings together data and information to support physical and virtual collaboration across Hawai'i.
- **Convergence:** Every dollar expended on IT is maximized through enterprise cooperation, coordination, and resource sharing. Supporting this convergence, the ETA describes the technology targets and the preferred future state technologies while identifying those technologies that have reached end-of-life must be retired as quickly and smartly as possible. In addition, the ETA identifies emerging technologies for research and proof of concept analysis.

The technology areas depicted in Figure 28 represent critical pieces of the overall technology domain. Each technology domain will be described in detail later in the ETA document but the following describe new levels of services and convergence going forward.

7.2.1.1 INFRASTRUCTURE: HAWAII CLOUD COMPUTING CENTERS (HC3)

The HC3 represents the infrastructure environment after the consolidation of the majority of Departmental applications and servers into a common set of special purpose data centers. The HC3 facilities provide hosting, virtualization, cloud computing, storage management, and disaster recovery services for the State. The upfront design of the HC3 facilitates public/private partnerships constructed to provide services to business inside and outside Hawai'i. The HC3 includes two data center facilities in Oahu (one State-owned and one non-State owned) to immediately support State computing requirements. To further leverage geographic separation of services, and to best serve the communities outside of Honolulu County, additional public/private facilities in each of the other three counties will provide enhanced services while leveraging consolidation, virtualization, common IT service management and the use of cloud computing throughout Hawai'i.

7.2.1.2 ONE NETWORK FOR HAWAII (ONENET)

New network technologies are creating a revolution in technology that are fueling information access and communications needs. The Internet, as a global networking infrastructure, continues to make the world a smaller and more demanding place. Wireless computing paves the way for an “anytime, anywhere connected” networking environment. This has introduced an “always-connected” citizen community that has extensive requirements for mobility computing. Recent advances in convergence technologies not only promote the convergence of a single physical IP infrastructure, but also introduce convergence of feature-rich services that can be provided in a secure, reliable, cost effective manner to meet the State’s mission. A singled network, OneNet, fulfills the network needs of all State Departments to employees and citizens in the State of Hawai‘i with guaranteed performance levels.

7.2.1.3 ADAPTIVE COMPUTING ENVIRONMENT (ACE)

The Adaptive Computing Environment (ACE) establishes a consistent configuration for computing devices across the State using pre-approved vendors. State employees can order standard systems that are engineered to operate most efficiently in the OneNet environment. Choices are provided based on job classification for mobile/tablet solutions, laptop/desktop or a strictly virtual environment for certain work. These systems require fewer support resources than non-standard configurations, enhance overall support effectiveness, and reduce total cost of ownership. The State uses a multi-year lease cycle for computing assets to ensure personal computing assets periodic refresh of technology for every Department to minimize asset issues, and shifts maintenance support of the hardware to the vendor.

7.2.1.4 INFORMATION ASSURANCE AND PRIVACY

The State has a fully integrated Security Operations Center (SOC) and Computer Security Incident Response Center (CSIRC) to

- provide uninterrupted security services while improving security incident response times,
- reduce security threats to the State, and
- enable quicker, well-coordinated notification to all State Departments regarding security threats or issues.

The SOC applies ITIL practices and processes including incident, problem, change, configuration management, release management, and security management. Data mining and digital dashboard capabilities provide instant visibility into the security of the State enterprise. Security incident data mining capability enables the State to analyze and prevent future security incidents. Proactive monitoring of email and data services precludes the release of Personally Identifiable Information (PII) or the loss/leakage of other sensitive data sets which may compromise the State or an individual Department.

7.2.1.5 ENTERPRISE OPERATIONS

A single interactive Help Desk using technologies such as Voice over Internet Protocol (VoIP), live chat, video conferencing, and remote management tools provides service to the State user community. Users speak with their Help Desk representative directly as well as desk side technicians, as appropriate. The use of the remote management software enables Help Desk staff to demonstrate solutions “live” for the client. The implementation of customer service improvements including a fully developed three-tiered service model enhances Help Desk response time for problem resolution and creates an increased number of completed calls while maintaining high quality service.

Enterprise Operations also includes the provision of field support staff with

tools such as smartphones, scanners, and tablets or laptops. These tools will allow dynamic access to the Incident Management System and the technical Knowledge Base and reduce times resolving issues and providing service for the users.

Enterprise Operations also includes a “help desk” capability that extends beyond IT by providing the full scope of Enterprise Services band (discussed as part of the ESA).

7.2.1.6 COLLABORATION AND MESSAGING

Efficient communications and information access between the State and citizens is critical to the success of any program or service. Convergence technologies associated with collaboration and messaging play a pivotal role in bringing about a powerful and revolutionary change and render many devices obsolete (e.g., traditional telephone handset, facsimiles). Online convergence services provide integrated services in a single environment including:

- Integrated Multi-Media Online Communications Services: A common interface provides communications services including voice to data to video. This service is provided by an online application environment.
- Collaboration and Conferencing Services: An integrated solution provides voice, video, and Web collaboration services are provided via robust VoIP solutions.
- Multimedia Content and Information Services: OneNet provides quick and efficient access services to media rich and diverse content by authorized users anywhere, any time. Seamless Transition Communication Services: With mobility dominating the landscape, non-interruption of services is a must. In the course of using a service, such as voice services, a mobile user transitions from one environment to another without any service interruption.

The following section contains the details of one of the key elements, Information Technology Services Management (ITSM) proposed for the future state of the ETA. This section is organized with the following elements:

- Definition – A brief statement to set perspective and define the need for the domain or sub-domain architecture.
- Current State – A description of current Strengths, Weaknesses, Opportunities, and Threats (SWOT) for the domain.
- Future State – A description of the future state vision for the domain or sub-domain.
- Best Practices – A comprehensive listing of the best practices to guide the implementation of the ITSM.
- Transition & Sequencing Plan Summary – A list of initiatives and activities required to fully implement ITSM within the State.

7.2.1.7 IT SERVICES MANAGEMENT (ITSM) FRAMEWORK

The future state for IT services management, and even a broader scope of a strong service management discipline across all business services provided by the State, is based upon the adoption of mature industry models and best practices such as the IT Infrastructure Library (ITIL) for ITSM, the ISO 20000 standard for ITSM, and the Capability Maturity Model – Integrated (CMMI) for Services. The goal is to align services with the customer needs. Through the creation of service level agreements and the associated performance measurement, customers know what to expect from service providers and have the assurance that the service expectations are met.

CURRENT STATE SWOT FOR ITSM

The current state or As Is environment for ITSM in the State of Hawai`i is characterized in the Final Report in detail. In summary, SAIC rated the State’s enterprise ITSM maturity at a Level 1 (service management processes initiated) where 50% of the time the

environment is reactive to technology-based problems. Within the various Departments and specifically the “have” organizations, SAIC found operational examples of Level 2 (service-focused environments with aspects of repeatable processes) with definite movement toward Level 3 (customer focused environments with defined processes).

FUTURE STATE VISION FOR ITSM

The future state eliminates stove-piped IT services and infrastructure by employing state-wide IT Service Management (ITSM). IT governance for the State employs a philosophy of managing IT services through the use of industry best practices for the improvement of business functions.

ITSM is the philosophy of managing IT services, through the use of industry best practices for the improvement of business functions. The goal of ITSM is to:

- align services with the needs of the customer;
- improve the quality of IT services whatever way the customer expresses quality and value,
- reduce the long-term cost of service provisioning.

SERVICE MANAGEMENT

The future state vision for service management ensures that these industry best practices include the broader scope of the State’s 35 lines of business and approximately 200 defined business services provided to 1.4 million citizens/residents by over 40,000 employees. Service delivery team members (including vendors) focus on providing services as needed when and where needed at the appropriate level of quality and cost while always ensuring the alignment with the customer or business requirements.

The fundamental elements of this service management discipline answer the following key questions:

- Service Definition – What are our products and services?

- Service Excellence – Have we defined what service excellence means to our customers?
- Service Performance Measurement – What are our measures, and how are we measuring them?

The role of IT, specifically the solutions/systems and supporting infrastructure, is woven very deeply into business service success. The predominant customer experience with a business service and his or her impression of it is defined through the IT solutions with which they interact. Therefore, it becomes imperative for us to understand the IT systems that we have and how they map to these LOBs and business services. Managing the overall portfolio of services, and the associated IT systems and investments is critical. Again, additional key questions regarding these systems?

- How well are these systems supporting the employee and/or citizen?
- What are the mission critical or mission essential services, and associated systems?
- Have we categorized the priority and criticality of our systems and protected them accordingly?

Our service management discipline should incorporate the continuous feedback from our customer base regarding their expectations and satisfaction with the delivery of services. And it should include the two-way communications regarding the service levels to be expected to “level set” the customer expectations. This is the essence of a service level agreement.

The customer should have a simple solution for contacting the State regarding any issue with the receipt of services – being able to contact a Service Desk through a standard phone number, or Web site, or email, text, or tweet.

ITSM

The starting point for realizing the future state vision is to adopt an ITSM framework to manage IT service provision. OIMT will adopt a tailored ITIL-compliant service management model as a best practice for establishing enterprise-level IT services. The elements of the vision include:

- Implementing an ITIL-based systems management infrastructure
- Proactive system monitoring to improve up-time and user experience
- Consolidation of all service support and operations through a Service Management Operations Center
- A one stop shop (service desk) for services anytime and anywhere with 24x7x365 support, access, and availability, and secure remote access for problem resolution

- A knowledgebase as a cornerstone component where IT staff can share problem resolutions and environment knowledge to enhance everyone’s productivity and efficiency in providing service support
- Empowered users with a self-help portal that is characterized by:
 - access into the knowledgebase where anyone can obtain assistance in compliance to information sensitivity
 - the ability to check the status an inquiry/request/problem, with transparency on who was last assigned the ticket
 - information about systems accessible anytime and anywhere
 - An overall IT service delivery environment characterized by timely response and feedback from the service providers and positive customer satisfaction

Figure 29 illustrates the ITSM future state process model.

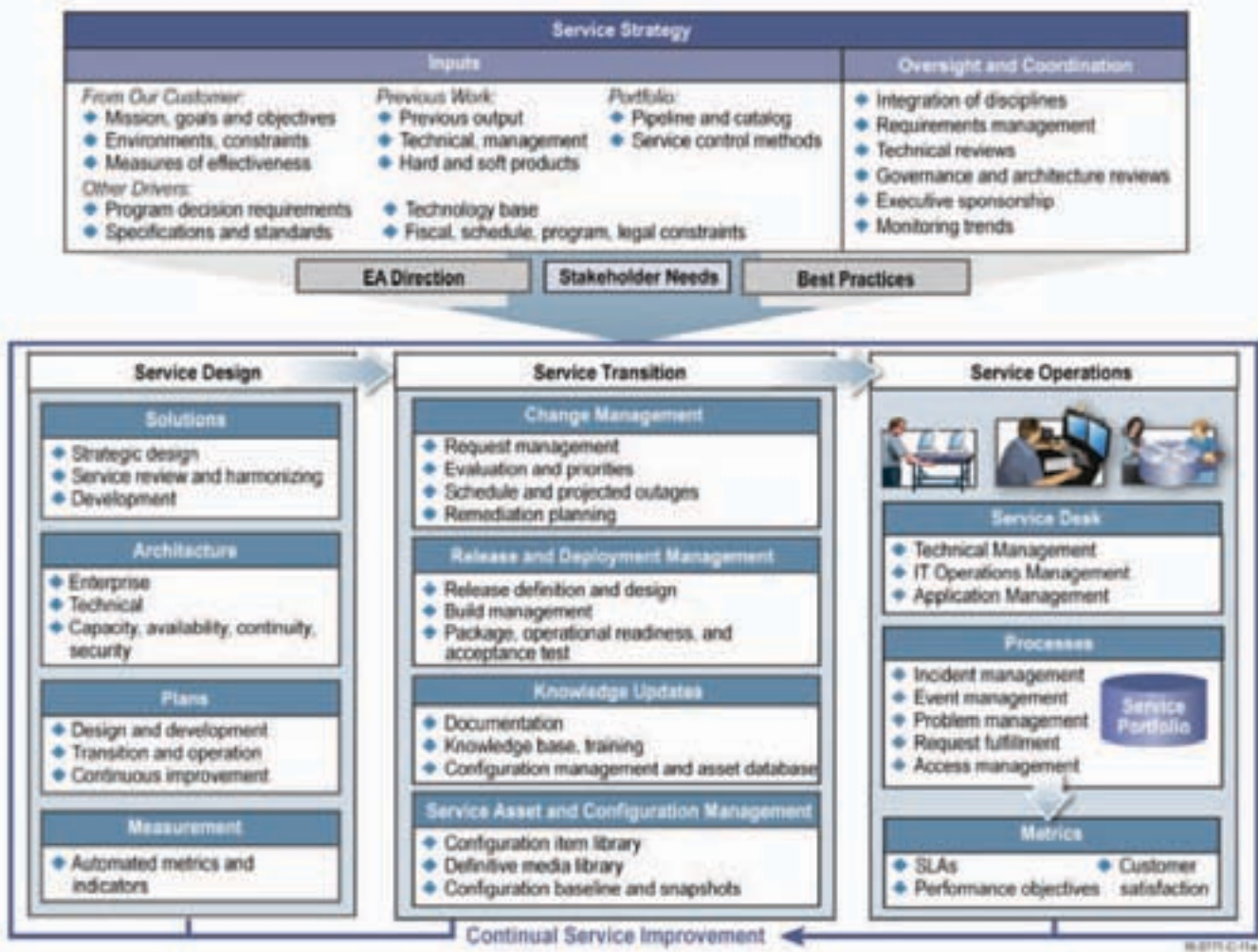


Figure 29: Future State Vision for the ITSM Model

ITSM BEST PRACTICES

Table 22 outlines the best practices to be adopted in ITSM as part of this vision. The practices are organized by the ITIL Version 3.0 life cycle phases

Table 22: Future State ITSM Best Practices

ITSM Life Cycle Phase	ITSM Process Area	Best Practices
Service Strategy	Service Portfolio Management	<ul style="list-style-type: none"> • Full life cycle of new and planned services, broader than the Service Catalog • Includes life cycle of planning for new services
	Service Portfolio Management	<ul style="list-style-type: none"> • Includes validating demands for new and current services from all customers • Customer service reps would be great approach for this
	Financial / Budgeting and Accounting Management	<ul style="list-style-type: none"> • Includes funding model and accounting for all planned and current services • Address “fee for service” planning and accounting
Service Strategy	Service Level Management	<ul style="list-style-type: none"> • Service level agreements and operating level agreements
	Service Catalog Management	<ul style="list-style-type: none"> • Active service catalog with automated rapid provisioning
	Availability and Capacity Management	<ul style="list-style-type: none"> • Proactive analysis of availability and capacity trends and planning and designing response through supply chain
	Service Continuity Management	<ul style="list-style-type: none"> • Proactive analysis, planning, policy, and design of service continuity solutions
	Information Security Management	<ul style="list-style-type: none"> • Proactive analysis, planning, policy, and design of information security framework and technologies
	Supplier Management	<ul style="list-style-type: none"> • Supply chain components of service catalog
Service Transition	Knowledge Management	<ul style="list-style-type: none"> • Most critical capability in all of ITIL V3 – all functions and organizations using a common knowledge management system • All processes, functions, and organizations incorporate knowledge capture
	Change Management	<ul style="list-style-type: none"> • Common enterprise Request For Change (RFC) process • enterprise Change Advisory Board (CAB) • Forward Schedule of Change
	Configuration and Asset Management	<ul style="list-style-type: none"> • Federated Configuration Management Data Base (CMDB) • Integration with enterprise asset management processes
	Release Management	<ul style="list-style-type: none"> • Enterprise level process for approved RFCs • Release, deployment, validation, and testing
Service Operations	Incident Management	<ul style="list-style-type: none"> • Full incident response model that drives response group and logic from incident categorization • Tailored response from High Priority outages requiring immediate notification and 24x7 response team to lower priority Tier 1 response
	Event Management	<ul style="list-style-type: none"> • Enterprise systems management capability – tracking all devices/components, up-time, resource usage • Automate the linkage of events from Enterprise Systems Management to the Incident Management
	Problem Management	<ul style="list-style-type: none"> • Most important discipline to identify and capture solutions for new, recurring problems and push resolutions to lowest tier
	Access Management	<ul style="list-style-type: none"> • Automation of account resets, account requests and associated approval workflows
	Request Fulfillment	<ul style="list-style-type: none"> • Multi-channel request capability, (800 number, text, email, Tier 0 Web request, mobile app, tweet, etc.) • Service catalog integration and rapid provisioning models (Select-Provision-Manage)

ETA TRANSITION AND SEQUENCING PLANNING SUMMARY FOR ITSM

In terms of the transition and sequencing plan for ITSM the tasks and activities are identified in relation to the service elements that are inherent to the ITSM. Additionally, outcomes and deliverables as well as dependencies are provided to guide the implementation activities. Table 23 provides additional detail on the initiatives required to ensure the successful implementation of the ITSM in conjunction with the implementation of the “new” enterprise infrastructure.



Table 23: ITSM Implementation Actions

ITSM Initiatives	Tasks/Actions	Outcomes / Deliverables	Dependencies
ITSM Program Development	<ul style="list-style-type: none"> • Survey enterprise for existing service management operations (what do we have?), capacity evaluation / assessment / requirement • Communication planning and execution • Training/consulting in ITIL • Certification program (initiation/planning) • Curriculum development including University (UHM, HPU, Chaminade, CC, etc.) 	<ul style="list-style-type: none"> • ITSM Implementation Plan including organizational change, architecture, implementation, operations and maintenance • ITSM Organization • ITSM Consulting and Training Contractor • ITSM Training Program • Certification/training program roll-out • Curriculum development including University (UHM, HPU, Chaminade, CC, etc.) 	<ul style="list-style-type: none"> • Confirm staffing included within People and Organization Plan – FTE for Program Communications and Training
Service Portfolio Development	<ul style="list-style-type: none"> • Use as a basis for planning and expanding the new OIMT enterprise services to be offered including their definition, price/cost/funding structure, and service level agreements; leverages and re-purpose ICSD’s service catalog work. • Establish services cost build-ups and pricing structures as part of overall funding strategy for OIMT. • Adapt new services/product/technology evaluation and insertion methodology for services portfolio management. 	<ul style="list-style-type: none"> • Service Portfolio / Catalog including funding model with fee for service • New service / technology introduction methodology 	<ul style="list-style-type: none"> • Confirm staffing included within People and Organization Plan – FTE for Portfolio and Funding Model development • Conduct in advance of rolling out new enterprise IT services
Customer Liaison Implementation	<ul style="list-style-type: none"> • Establish customer liaison or customer relationship management role within OIMT and include services input and demand planning as part of the overall responsibilities. • Validate demands for new and current services from Departments • Facilitate and support LOB portfolio management activities 	<ul style="list-style-type: none"> • Customer Liaisons staffed 	<ul style="list-style-type: none"> • Confirm staffing included within People and Organization Plan – FTE for Customer Liaisons – ramp up over multi-year period to 12 representatives

Table 23: ITSM Implementation Actions

ITSM Initiatives	Tasks/Actions	Outcomes / Deliverables	Dependencies
IT Service Accounting System Implementation	<ul style="list-style-type: none"> • Develop needed IT services cost measurement and accounting processes and systems 	<ul style="list-style-type: none"> • Enterprise IT Services Accounting System deployed and operational 	<ul style="list-style-type: none"> • Leverage State ERP Financial Management module when operational; consider interim or pilot capability till that point
Service Portfolio Oversight	<ul style="list-style-type: none"> • On-going service portfolio oversight • Services funding model oversight • New service / product / technology evaluation / insertion oversight 	<ul style="list-style-type: none"> • On-going service portfolio 	<ul style="list-style-type: none"> • Confirm staffing included within People and Organization Plan – FTE for Portfolio and Funding Model development
On-going Customer Relationship Management	<ul style="list-style-type: none"> • On-going department customer liaison / customer relationship management 	<ul style="list-style-type: none"> • On-going customer relationships 	<ul style="list-style-type: none"> • Confirm staffing included within People and Organization Plan – FTE for Customer Liaisons – ramp up over multi-year period to 12 representatives
SERVICES			
On-line Service Catalog Implementation	<ul style="list-style-type: none"> • Service Catalog Management • Publish services catalog-level information regarding all production services through the OIMT web site in conjunction with services portfolio management discussed above. • Include IT hardware products defined/authorized based on the technical architecture. • Expand service catalog capabilities in the future to include on-line requests and provisioning, e.g., use of a web form to request a virtual server and an automated provisioning system that implements the virtual server for the requester in near real-time. 	<ul style="list-style-type: none"> • Published Service Catalog • On-line request and rapid provisioning capability implemented 	<ul style="list-style-type: none"> • Enterprise IT Hardware / Software Procurements
Service Level Reporting Implementation	<ul style="list-style-type: none"> • Service Level Management and Reporting • Develop a program plan for service-level measurement and reporting in conjunction with services portfolio management. • Identify all required service-level measures and measurement methods and techniques/tools. • Implement service-level reporting systems and summary dashboards for OIMT. 	<ul style="list-style-type: none"> • Enterprise service level dashboard and reporting capabilities operational 	<ul style="list-style-type: none"> • Depends on enterprise analytics capabilities

Table 23: ITSM Implementation Actions

ITSM Initiatives	Tasks/Actions	Outcomes / Deliverables	Dependencies
Enterprise IT Services Analytics Implementation	<p>Service Availability and Capacity Management</p> <ul style="list-style-type: none"> • Implement end-to-end service monitoring system and measure up-time and response-time for critical applications, databases, processes, servers, storage devices, and networks. Leverage existing SolarWinds Orion toolset as the foundation. • Profile server and storage inventory data to include capacity attributes. • Implement server and storage monitoring systems to track and trend usage data. • Integrate demand planning and usage trend analysis into ongoing capacity management plan. <p>Service Security Management</p> <ul style="list-style-type: none"> • Integrate security operations monitoring and event response with enterprise operations center approach. • Establish standard security monitoring solutions, approaches, and reporting. Leverage ArcSight and other existing products. 	<ul style="list-style-type: none"> • Availability, capacity, continuity, and security event analytics 	<ul style="list-style-type: none"> • Depends on Enterprise Systems Management Implementation below in Service Operations • Integrate with Information Assurance and Privacy program
Service Supplier Management Implementation	<p>Service Supplier Management</p> <ul style="list-style-type: none"> • Documenting and maintaining relationship with third-party suppliers when used. • Measuring supplier performance. • Ensuring that suppliers participate in service request and incident management. • Providing supplier reimbursement based on service fulfillment. • Benefits include integrated service delivery team, corrective action, and dispute resolution. 	<ul style="list-style-type: none"> • Extension of enterprise service level dashboard and reporting capabilities to include supplier tier • Extension of service operations system to include suppliers 	<ul style="list-style-type: none"> • Depends on Service Level Reporting Implementation
SERVICE TRANSITION			
IT Service Knowledge Management System Implementation	<p>Knowledge Management</p> <ul style="list-style-type: none"> • Establish enterprise processes and a system for knowledge management. • Ensure that all documentation regarding environments, asset configuration, known problems, workarounds, solutions, user requests for service, and resolution scripts are stored within the knowledge management repository. • Ensure that IT workers at all levels use the knowledge management repository for environment and work instruction documentation. • Begin by ensuring that OIMT central services use this approach. 	<ul style="list-style-type: none"> • IT services knowledge management system deployed and operational 	<ul style="list-style-type: none"> • Depends on enterprise collaboration service • Depends on enterprise knowledge management service / system approach
Federated CMDB Implementation	<p>Configuration and Asset Management</p> <ul style="list-style-type: none"> • Implement federated Configuration Management Data Base (CMDB) – base federation on existing enterprise systems management tools, and build appropriate linkages/services to aggregate asset and configuration perspectives • Augment configuration management actions with appropriate Add, Change, Delete authorization • Integrate asset management transactions with enterprise asset management services • Integrate supply chain transactions with enterprise supply chain services 	<ul style="list-style-type: none"> • Federated CMDB deployed and operational 	<ul style="list-style-type: none"> • In parallel with enterprise infrastructure deployment

Table 23: ITSM Implementation Actions

ITSM Initiatives	Tasks/Actions	Outcomes / Deliverables	Dependencies
<p>Service Transition (Change Management) System Implementation</p>	<p>Enterprise Change Management</p> <ul style="list-style-type: none"> Record, plan, route, review, and approve changes associated with a configuration item. Provide adequate capacity to support change. Ensure that change meets security, availability, and continuity requirements. Convene a change review board with a balance of technical expertise and authority. Create an emergency change review process. Communicate planned service outages through a schedule of change and transition project portfolio. Perform post implementation reviews, project lessons learned, and impact of change on incident volume. <p>Transition Project Management</p> <ul style="list-style-type: none"> Address project management and oversight of all key elements of a service/product/technology insertion with well-planned roll-out and upgrades to existing service/product technology including communications to and involvement of all key stakeholders in schedule decisions and transition execution, and impact analysis, planning, and mitigation. <p>Release, Validation, Testing, Deployment, and Evaluation Management</p> <ul style="list-style-type: none"> Establish enterprise standards and procedures for execution of releases to the production environment. Ensure adequate impact analysis and testing to mitigate impact on the production environment. Ensure appropriate deployment plans are developed, tested, and executed including roll-back procedures. 	<ul style="list-style-type: none"> Service Transition System deployed and operational 	<ul style="list-style-type: none"> In parallel with new enterprise service implementation In parallel with Federated CMDB
SERVICE OPERATIONS			
<p>Enterprise Service Desk Implementation</p>	<ul style="list-style-type: none"> Establish Tier 1 Service Desk Function and ITIL Service Operation processes Incident Management Provide/restore service as quickly as possible by classifying, prioritizing, routing, and escalating incidents. Establish tier/escalation definitions. Communicate status of incidents. Validate user satisfaction with incident resolution. Request Fulfillment – Capturing requests, distributing requests through workflow and approval, and submitting requests for fulfillment through incident management. Benefits include self-help, automation, and efficiency. Access Management – Include all access requests in central service desk implementation. Problem Management – Establish root cause analysis approach and procedures as part of a problem management process within the service operations program plan. Over time, ensure that all IT critical failures at all levels include a root cause analysis. 	<ul style="list-style-type: none"> Enterprise Tier 1 Service Desk established and operational Service Operations processes 	<ul style="list-style-type: none"> In parallel with deployment of initial enterprise IT services

Table 23: ITSM Implementation Actions

ITSM Initiatives	Tasks/Actions	Outcomes / Deliverables	Dependencies
Service Operations System Implementation	<ul style="list-style-type: none"> Evaluate, select, and implement Integrated Service Operations solution Modules include: <ul style="list-style-type: none"> - Enterprise “Ticketing” - Knowledge management - Self-help Web portal and tools - User Service Request - Integration with federated enterprise systems management tools (event management) - Remote support tool 	<ul style="list-style-type: none"> Integrated Service Operations Solution Integration of Event Management and Incident Management 	<ul style="list-style-type: none"> In parallel with Service Desk implementation Integration with enterprise systems management (event management integration)
Enterprise Systems Management Implementation	<p>Event Management and Enterprise Systems Management</p> <ul style="list-style-type: none"> Enhance operational availability monitoring through monitoring service infrastructure using network and server management tools, such as SolarWinds, CiscoWorks and Tivoli. Automate alerts and forward to an incident management system for automated ticket creation and support staff notification, where they are then tracked to resolution by the Service Desk. Design and implement needed monitors for application and infrastructure events (e.g., a server outage) and initiate appropriate incident notification and resolution processes. 	<ul style="list-style-type: none"> Enterprise systems management deployed and operational Integration of event management with incident management system 	<ul style="list-style-type: none"> In parallel with incident management system In parallel with roll-out of enterprise services
Enterprise Identity Management System Implementation	<p>Access Management</p> <ul style="list-style-type: none"> Establish access management systems to provide self-service options for end users on password management and resets. Establish identity management systems for management of credentials and role-driven access management. 	<ul style="list-style-type: none"> Identify management system deployed and operational Role-based access control operational 	<ul style="list-style-type: none"> Integrate with Information Assurance and Privacy program
CONTINUOUS SERVICE IMPROVEMENT			
ITSM Communications and Training Program Execution	<ul style="list-style-type: none"> On-going ITSM Communications and Training 	<ul style="list-style-type: none"> On-going ITSM Communications and Training 	<ul style="list-style-type: none"> Follows ITSM Program Development
ITSM Continuous Service Improvement Program Execution	<ul style="list-style-type: none"> On-going service monitoring and analysis, corrective action, and continuous improvement initiatives 	<ul style="list-style-type: none"> Service improvements 	<ul style="list-style-type: none"> In parallel with all enterprise service initiatives

Figure 1 provides a roadmap for both development/implementation of an ITSM capability and on-going operations and maintenance across the planning horizon.

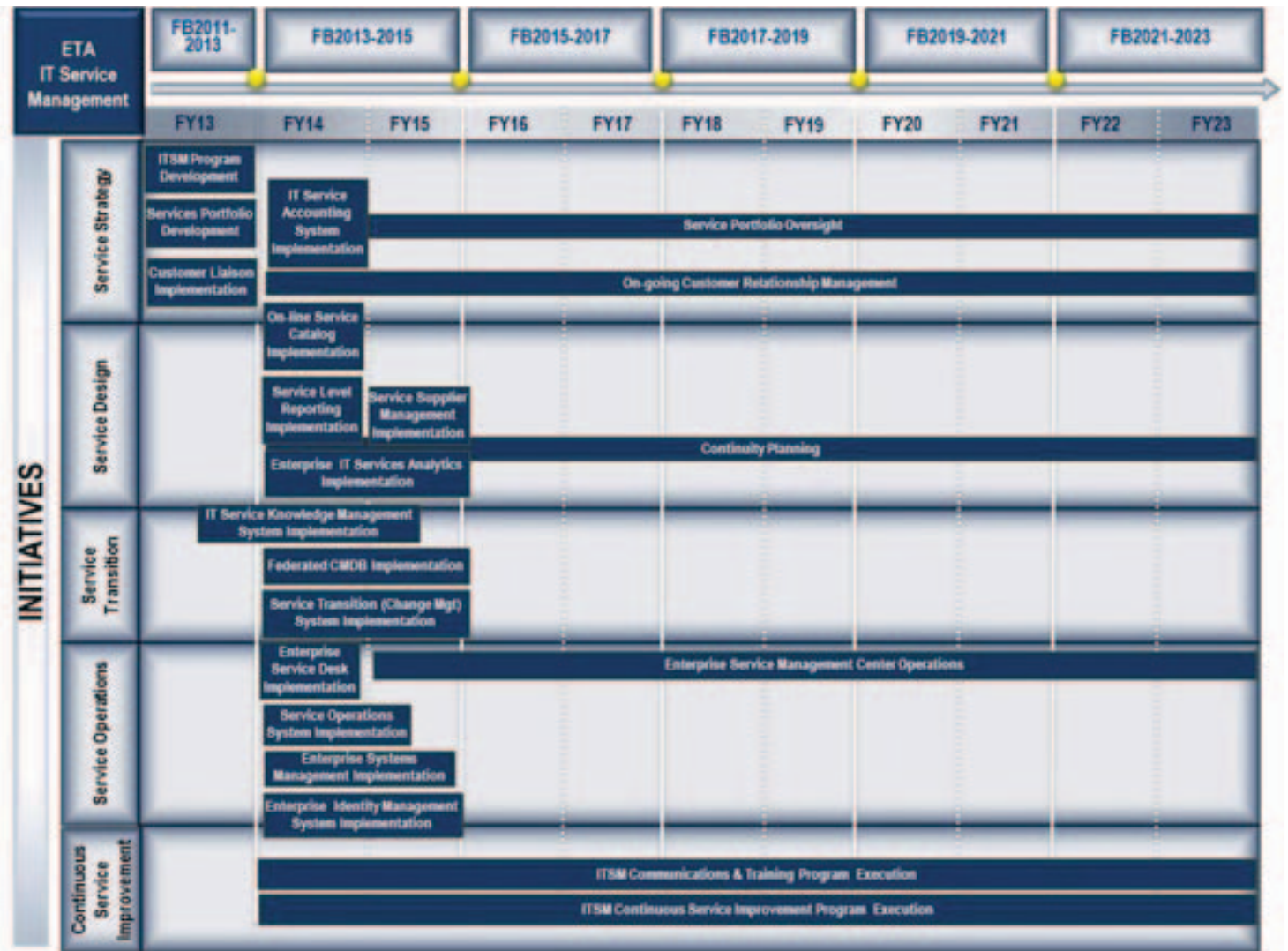


Figure 30: Roadmap for Achieving Future State ITSM

7.2.3 TECHNOLOGY DOMAIN ARCHITECTURE

The ETA embodies a vision or view of the future of IT in the State. It was crafted with the widest possible participation from members of the State's IT community and the population at large. Architectures are not developed to bind organizations to inflexible rules; the goals of the architecture are coordination, simplification, improved performance, and greater efficiency. The ETA is a component-driven, technical framework that categorizes the standards and technologies to support and enable the delivery of services and capabilities. It also unifies existing Departmental technical models and eGov guidance by providing a foundation to advance the reuse and standardization of technology and service components from an enterprise wide perspective. The governance process will resolve any architectural variances that may emerge over time. The ETA will evolve as technology evolves and as new initiatives emerge.

For the technology domain architecture discussed in the following sections, there are references to specific products as current or emerging standards, although the goal was to have a standards-based architecture throughout. In a number of cases, products were chosen as the standard where no widely accepted architectural standard currently existed. Product equivalence determinations relative to the architecture will be made by the governance committees as they review investment requests going forward.

Aligning IT investments to the ETA leverages a common, standardized vocabulary, allowing interdepartmental discovery, collaboration, and interoperability. Departments and the State government benefit from economies of scale by identifying and reusing the best solutions and technologies to support their business functions, mission, and target architectures. The technologies, tools and systems within the State of Hawai`i are organized into seven primary technology domains. These domains are depicted in Figure 1.

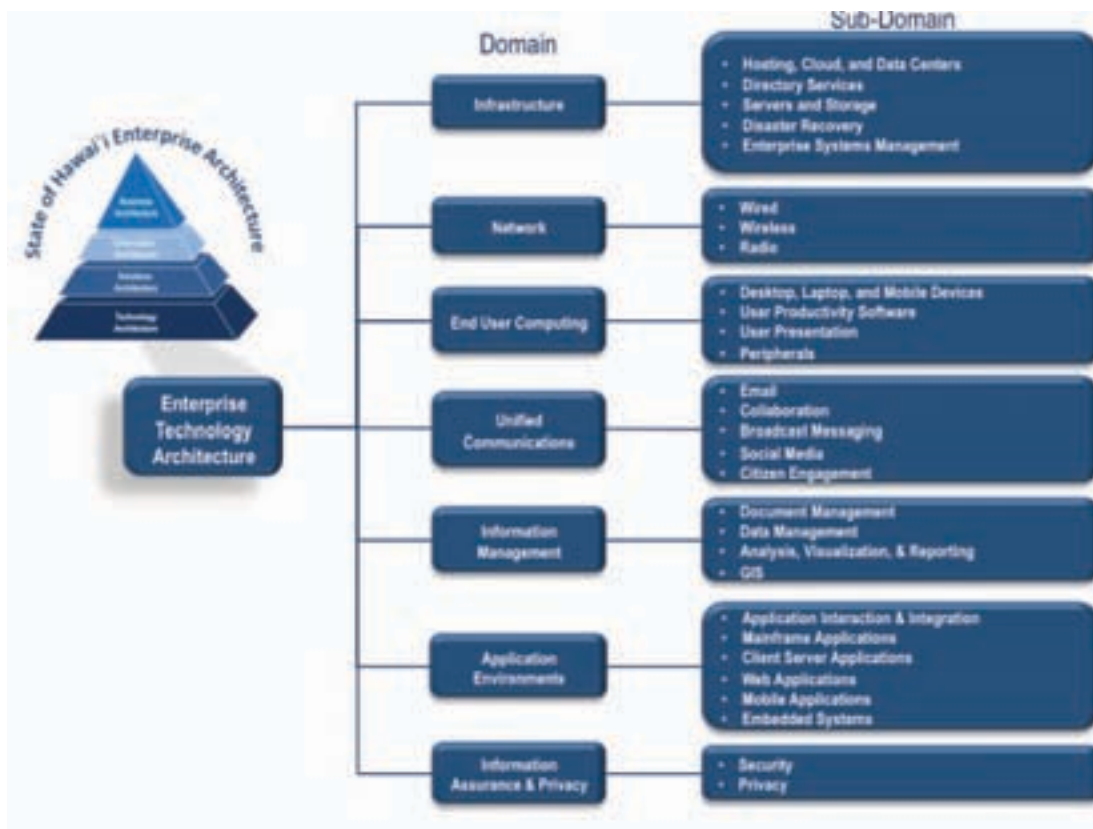


Figure 31: Technology Architectural Domains and Sub-Domains for the State of Hawai`i

The following sections contain the details of the domains and sub-domain that form the ETA for the State of Hawai`i. Each section is structured to support access to the information and technical content required as part of architecting a solution and its accompanying infrastructure and/or as part of the investment selection, control, and evaluation process. Each section is organized with the following elements:

- Definition – A brief statement to set perspective and define the need for the domain or sub-domain architecture.
- Current State – A description of current Strengths, Weaknesses, Opportunities, and Threats (SWOT) for the domain.
- Future State – A description of the future state vision for the domain or sub-domain.
- Guiding Principles – An expression of values to be used in guiding technical choices in any effort. The order of the values does not imply priority or importance but merely assists with consistent technical direction setting.
- Standards – Categorical tables that list current supported products or standards, twilight products or standards, preferred products or standards, and emerging trends within the industry.
- Preferred Products and Standards represent the preferred directions and products that should be considered when making implementation and design decisions. IT investments within the State center on the elements of this category.
- Supported Products and Standards represent the current supported products or standards that will continue to be supported within the State's technical infrastructure for the foreseeable future. This column may designate supported standards by Department as needed. Rationale or historical reasons may be included when there is a broad set of choices.
- Sunset Products and Standards (or technology retirement targets) are those that should not be used for future investment or implementation. This is not to imply that existing resources should be eliminated/replaced, but that the use of these products and services should not be extended in future planning and development. Guidance should be provided on timeframes for when a product should no longer be used.
- Emerging Trends (or newly identified or introduced technologies) include directions and options that need continued monitoring to find applicability within the State IT infrastructure as they mature. Generally the technologies associated with emerging trends are not yet fully production-worthy, but are potential candidates for future investment and implementation. Advanced users of technology, such as academic researchers in the State Universities, are usually the first implementers of these technologies. Continued market acceptance and adaptation will move these solutions toward the ETA's preferred products or standards.
- Transition & Sequencing Summary Plan
- A summary of initiatives that will move the domain from the current state to the identified future state vision.

7.2.3.1 INFRASTRUCTURE DOMAIN

The infrastructure domain represents the physical hardware used to interconnect technology and users. The infrastructure includes transmission media such as telephone lines, cable television lines, satellites, routers, and antennas. Included in the infrastructure domain are any devices, hardware or software, which supports the flow and processing of information.

CURRENT STATE SWOT FOR THE INFRASTRUCTURE DOMAIN

Strategy, architecture, design, implementation, and operation of the State's technical infrastructure are currently distributed across the Departments. As noted in the Final Report, the State's technical infrastructure lacks collaboration on common solutions and standards, and is characterized by a diversity of technologies. As noted in networks, this diversity and distributed management results in a general lack of coordination, compliance to best practices in a comprehensive fashion, and a robust, universal 24/7/365 support model.

The current technical infrastructure environment is characterized by:

- Budget constraints
- Out dated and limited facilities, equipment, and applications; and general lack of tools
- Reactive management versus proactive
- Cumbersome procurement process
- Lack of standardization (hardware, software, processing, etc.) and direction and multiple technology platforms (hardware/software/OS); fragmented infrastructure
- Lack of adequate engineering and operations support staff and lack of training of our technical staff
- Lack of willingness of staff to accept changes
- Lack of inter-departments coordination collaboration/cooperation/communication

- Poor location of primary State data center
- Lack of COOP and DR Plan
- 72 hours backup power
- Issues with cooling, power, space and capacity
- Lack of Help Desk Support
- No fully supported wireless access
- Limited Pipe
- Single DNS
- Disparate email systems

Nevertheless, there are significant areas of opportunity as identified by the CIOC and its working groups for starting fresh to bring standardization and economies of scale to benefit the customer base, to include:

- Virtualization technologies are a pivotal means to aide in standardizing computing platforms.
- Volume discounts for hardware and software and coordinated purchasing
- Consolidated Storage
- Statewide wireless (Wi-Fi hotspots)
- Opportunity to leverage resources intra departmentally (databases, applications, staff knowledge, etc.)
- Statewide standards that are enforced to assure compatibility with current environment and to simplify support
- Establishment of an enterprise private state governmental cloud.
- 24 x7 x365 support

FUTURE STATE VISION FOR THE INFRASTRUCTURE DOMAIN

The future state vision for the Infrastructure Domain is based on input from the Computing and Storage Working Group and has the following major elements:

- Technology should “Just Work” for whomever, wherever, whatever, whenever using any device of choice to interface with the IT information required.
- Desirable outcomes include:
 - Technology that is effective in supporting customers' missions
 - Technology that is easy to use (give users the “Easy Button”)
 - Technology that is easily adapted to changing business needs
 - Technology that empowers the end user
- Outcomes that are measurable
- Hawai`i First and Cloud First – the State has a vision for a premiere data center capability and technical infrastructure that is hosted here in Hawai`i, with the cloud computing paradigm as the cornerstone.
- Five Islands – Hawai`i First, Mainland Offload – the cloud computing solution will be a joint private/public cloud capability featuring fully meshed computing centers distributed across the 5 major islands with load balanced provisioning, with additional computing capacity offloaded to public cloud capability on the mainland.
- Private Cloud – the Hawai`i Cloud Computing Center will feature a private cloud capability with virtual environments supported by rapid provisioning (minutes). Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.
- One clock source – all computing centers and servers will operate from a synchronized clock source.

- Mainframe Reconfiguration – the Mainframe assets across the State and Local governments will be reconfigured to provide redundancy and backup support; and the future state will leverage zLinux as a preferred platform.
- Technology Refresh – a technology refresh plan will be a major component resulting in servers being refreshed every 4 years; and end user devices every 3 years.
- Select-Provision-Manage – an on-line Service Catalog will contain standard virtual server platforms and end user computing devices for user selection and rapid provisioning.
- Virtual Desk Top – user interface devices will be thin client with exceptional bandwidth and server side compute capabilities.
- Service Management – automated enterprise systems management capabilities and ITSM best practices will improve overall quality while saving operational costs.
- SLAs – service level expectations will be defined within service level agreements, and service performance will be regularly reported against those measures.
- Sustainability – the data centers and technical infrastructure will be engineered consistent with Green IT best practices with features such as auto shutdown and alternative fuel and power sources.

- Acquisition – new enterprise level contracts will streamline the supply chain connected through the service catalog to enable rapid provisioning of standard devices.
- Rights management services – enterprise rights management services will enable consistent role-based access controls across the solutions and infrastructure.

IT services for the State of Hawai'i reside in central data centers that will provide high bandwidth connectivity, redundancy, and rapid provisioning of new services. This assures the high level of interconnectivity between IT systems, workloads, and facility infrastructure required for the departments to remain agile and adapt to changing business and regulatory environments in the future; therefore, future data centers will be designed to deliver desired service levels in a flexible environment that reduces complexity and increases operational efficiency.

The following is a “notional” high level drawing for the proposed New Primary Data Center for the State of Hawai'i, including hosting services, the Hawai'i OneNet infrastructure, storage, compute, backup/recovery, and cloud devices are illustrated in Figure 1.

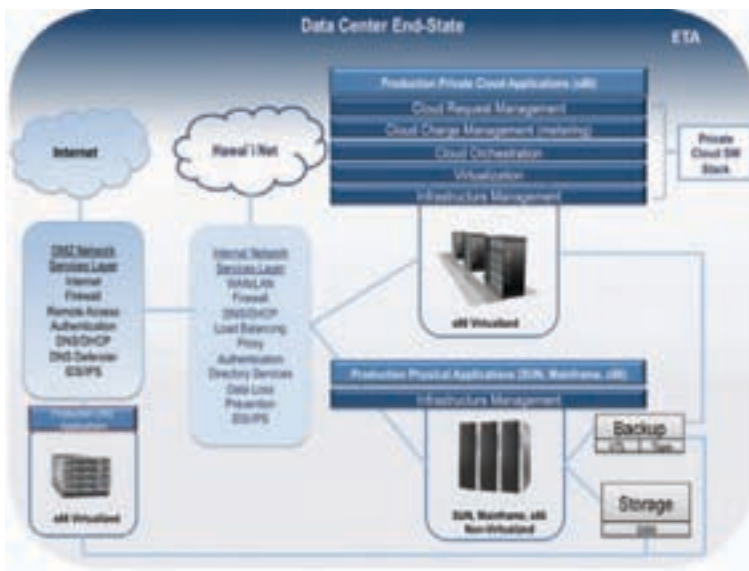


Figure 32: Data Center Future State View

Guiding Principles for Infrastructure Domain

1. IT is an enterprise-wide resource. IT investments will be aligned with the strategic goals of the state of Hawai'i through planning and architecture processes.
 - a. Reduce implementation and support costs, through a consistent enterprise-wide approach to IT solutions.
 - b. Consolidate or integrate existing systems and technical infrastructure.
 - c. Provide the IT foundation to support the business processes of state entities and local governing authorities.
2. State IT infrastructure and architecture will support the state's long term business, strategies and plans.
 - a. Align and optimize IT resources with changing needs of state entities and local governing authorities. Enable the effective implementation of state business strategies.
 - b. Highlight and promote the value of IT to executives and policy makers.
3. State IT solutions that deliver products and services to stakeholders will leverage the shared technology infrastructure by providing an infrastructure and architecture which will enable the state to respond to agency changes in technology and business requirement to increase the consistency, accessibility, and sharing of data and ensure interoperability by eliminating technology silos.

HOSTING, CLOUD, DATA CENTER SUB-DOMAIN

In terms hosting, cloud, and data center environment, IT services for the State of Hawai'i will reside in central data centers (new or repurposed) that provide high bandwidth connectivity, redundancy, and rapid provisioning of new services. The data center environment will be based on the TIA-942 Telecommunications Infrastructure Standards for Data Centers. The TIA-942 covers Site Space and Layout, Cabling Infrastructure, Tiered Reliability, and Environmental considerations. Table 24 provides a partial list of data center requirements.

Table 24: Key Criteria and Requirements for the State of Hawai'i Data Center

Data Center Criteria	Minimum Notional Requirements
Internal Network Backbone Speed	100+gb Minimum
Connection to Current State Next Generation Network	Multiple Multiprotocol Label Switching connections
External Internet Connections Speed	T1 or larger Digital lines
Multiple Trusted Internet Carriers	2 or more ISP Trusted Internet Connection providers
Multiple Network Backbones	Production/Test/Development environments
Loading Dock/moving	Handle Semi-trailers and forklifts
Traffic Impact	Minimize any necessary changes to local traffic patterns
Building accessibility	Disabled access to all areas, Americans with Disabilities Act (ADA) compliant
Emergency Services	Easy accessibility by Fire/Police/Sheriff/EMS services
Building Foundation	Able to support 1,000 pounds per SF
Physical Security (Guards, Alarms, Video Surveillance)	24/7/365 guard force and monitoring, card key access, person traps and fencing
Uninterruptible Power Supply	4 hrs. minimum to critical systems
Backup power generator(s)	Critical system support (1Mw)
Adequate fuel supply for generators	Daily tank top off deliverables
Facility Power load requirement	1.5 Mw, with multiple substations
Cooling requirements	1 Mw @ 72 degrees F with 70% humidity
IT Systems Monitoring (network, cyber security, servers)	24/7/365 Network/Security Operations Center, Shared Services and Help Desk Support personnel
Land	25 or more acres, includes parking and secure perimeter
Location	Facility must be located outside the flood zones

The following further characterizes the future state for the hosting, cloud, and data center environment:

Table 25: Future State Characteristics for the Hosting, Cloud, and Data Centers

Area	Characteristic
IT Core Infrastructure Fully Provisioned	<ul style="list-style-type: none"> • Facility is in place • Data Center room is built and ready including raised floor • Fully redundant power including Generators, UPS, Power Busses and PDUs • Fully redundant cooling including redundant Chillers and Compressors • Fire suppression using desired technology with appropriate zoning and monitoring • Redundant communications penetrations, risers and distribution frames • Physical Security Infrastructure
Power	<ul style="list-style-type: none"> • Power is the most critical design element for data centers <ul style="list-style-type: none"> – Power exhaustion occurs prior to space exhaustion – Resiliency and proximity to multiple sources • Every equipment refresh drives increased power and reduced space usage power sources critical • Minimum 24-30" raised floor, 350 w/SF for new data centers being built today • Thermal challenges now exist at all levels of the data center: chip, server, cabinet, data center and facility
Cooling	<ul style="list-style-type: none"> • Energy Usage Profile varies based on whether cooling is localized or via centralized chiller plant • Centralized plants are considerably more efficient than distributed plants, resulting in lower electrical operating costs • Centralized plants are initially more expensive and require more space to deploy • Sizing of cooling supply is directly related to average energy density at a facility bulk load • Increasing incidence of asymmetric design for cooling distribution to accommodate spot loads well above planned average energy density
Servers	<ul style="list-style-type: none"> • Blades demand higher electrical draw and greater heat than 1U servers, but more thermally efficient for the desired processor density • Equipment strategy drives data center requirements significantly impacting power and cooling requirements • SAN implementations remove low energy density disks from cabinets, allowing for more energy dense processors and increasing cabinet level thermal loads • CPU density is driven by ever increasing business volumes and computational complexity
Storage	<ul style="list-style-type: none"> • Increasing integration from vendors, e.g. Cisco MDS • Storage market has been driven to significantly increase rate of development for replication technologies • Connectivity between the servers and storage will be provided via SAN fabric with switches comprising the core of the fabric designed to handle large port counts and reduce the need for multiple aggregation switches. This allows servers to connect to storage through a common connection point. • There will be a greater focus on storage efficiency technologies such as dynamic or thin provisioning, dynamic tiering, archiving, and the extension of these technologies to existing assets with storage virtualization.

As part of the future state vision for the hosting, cloud, and data center sub-domain will evolve into the HC3. Going forward the HC3 facilities will provide hosting, virtualization, cloud computing, storage management, and disaster recovery services for the State. The initial planning and design of the HC3 environment will facilitate public/private partnerships so that services to business inside and outside Hawai'i can be accommodated.

The HC3 will include two data center facilities in Oahu to immediately support State computing requirements. To further

leverage geographic separation of services, and to best serve the communities outside of Honolulu County additional public/private facilities in each of the other three counties will provide enhanced services while leveraging consolidation, virtualization, common IT service management and the use of cloud computing throughout Hawai'i.

Cloud computing is the next “pay-as-you-go” utility model. As depicted in Figure 1, the cloud computing paradigm has four Deployment Models, three Service Models, and five Essential Characteristics.

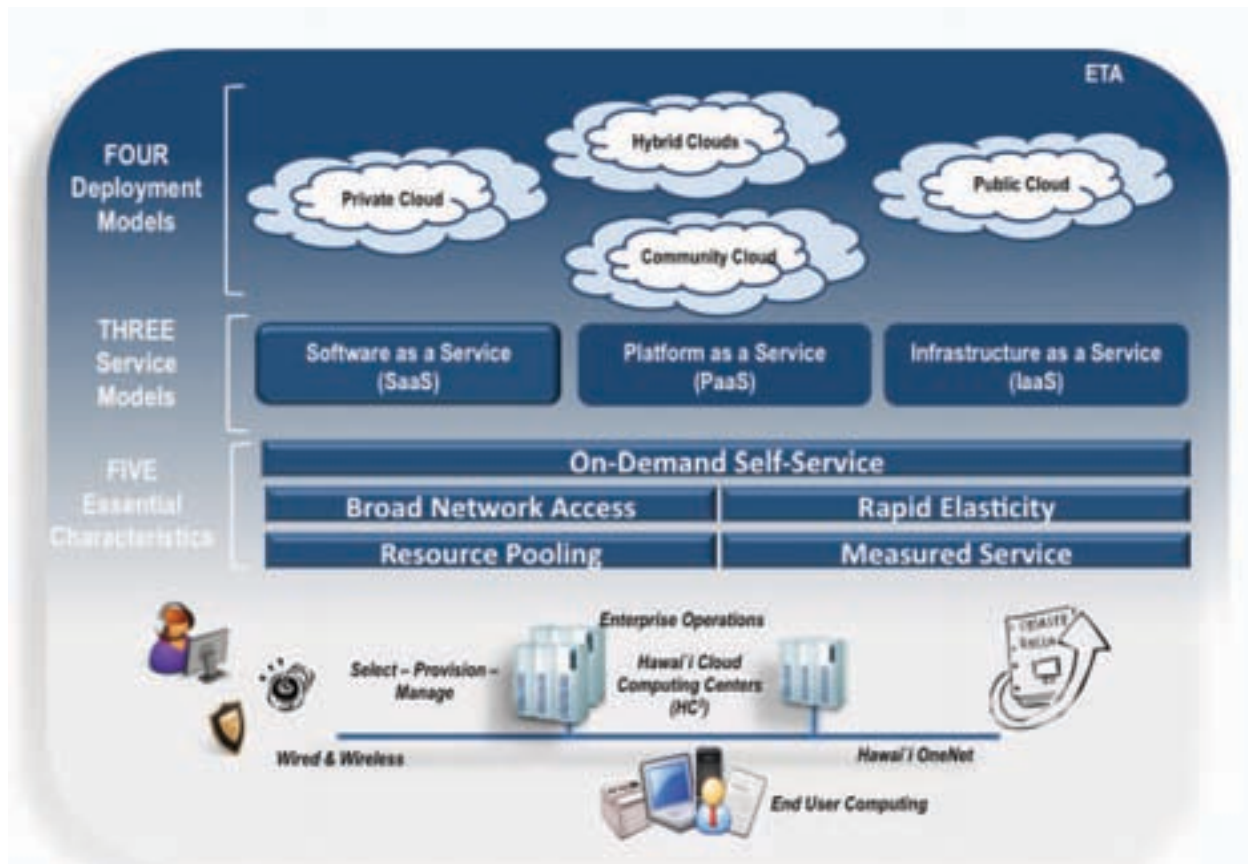


Figure 33: Cloud Computing Paradigm

The four deployment models which the cloud model is composed of: include private cloud, community cloud, public cloud, and hybrid cloud. Below are definitions of each deployment model.

- Private cloud -- The cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premise or off premise.
- Community cloud -- The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party and may exist on premise or off premise.
- Public cloud -- The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.

- Hybrid cloud -- The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

There are three basic service delivery models that together create the ‘Cloud’ which categorizes vendors and services provided according to Cloud Computing Architecture types:

- Software as a Service (SaaS): Software deployment model whereby a provider licenses an application to customers for use as a service on demand
- Platform as a service (PaaS): Delivery of computing platform and solution stack as a service

- Infrastructure as a Service (IaaS): Delivery of computer infrastructure (typically a platform virtualization environment) as a service

The five essential characteristics of the cloud include:

- Is accessible via Internet protocols from any computer.
- Is always available and scales automatically to meet demand.

- Offers Web or programmatic control interfaces.
- Enables full customer self-service on demand
- Offers location independent resource pooling.

Figure 1 depicts the segments within the Cloud infrastructure and an example of what each segment could contain.

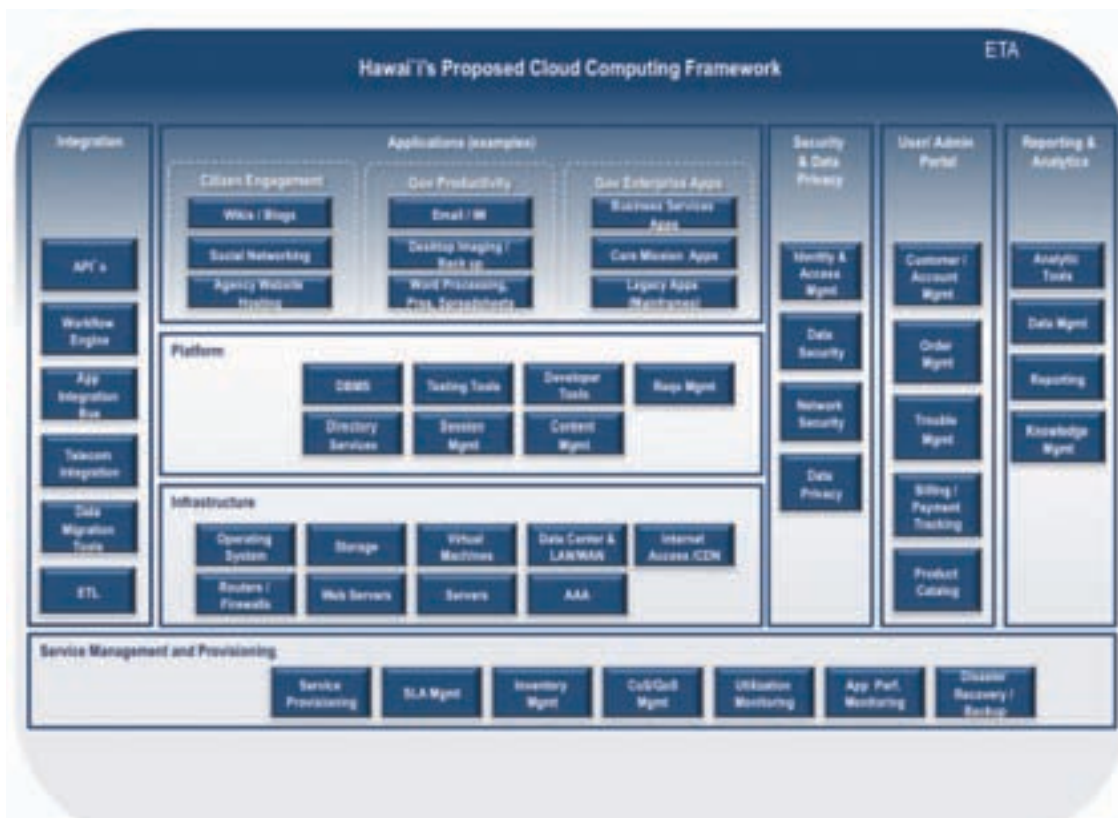


Figure 34: Proposed Cloud Computing Framework for the State of Hawai'i

The essential implementation steps to assess, design, transition, and operate the State of Hawai'i cloud computing environment are described below:

Guiding Principles for the Cloud Computing Domain

- **On-demand self-service.** A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service's provider.
- **Broad network access.** Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, laptops, and PDAs).
- **Resource pooling.** The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of

the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, network bandwidth, and virtual machines.

- **Rapid elasticity.** Capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out and rapidly released to quickly scale in. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.
- **Measured Service.** Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and and policy makers.

The Cloud Service Life Cycle for the State of Hawai`i will contain four implementation phases and a series of activities. There are outlined below:

1. Strategy and Assessment – activities include:

- a. Providing orientation/training on cloud computing and vendors’ capabilities, experience, and approach
- b. Understanding customer culture, organization, and environment
- c. Defining, communicating, and obtaining acceptance of charter including: constraints (time, resources, scope) and deliverables
- d. Assessing current-state
- e. Assessing if cloud makes good mission/business sense
- f. Assessing what capabilities, services, or use cases cloud will address
- g. Assessing risk (security, cost, schedule, etc.)
- h. Assessing if a cloud solution is feasible
- i. Assessing cloud readiness
- j. Developing an operational vision/strategy (initial concept of operations)
- k. Developing and recommending cloud solution roadmap/timeline and obtaining acceptance of deliverables

2. Design – activities include:

- a. Selecting strategic partnerships and suppliers (using cloud partner ecosystem)
- b. Defining roles and responsibilities in support of cloud operations, updating the service organization structure in support of cloud operations, and identifying cloud support communications and training (organizational and cultural change management)
- c. Defining g services, service levels, and metrics for iCloud on-demand self-service service catalog / Cloud portal/store front; and ii) Cloud measured service. Engineer mission/business, service, and management policies, processes, and procedures for cloud broad network access, cloud resource pooling, and cloud elasticity
- d. Technology:
 - i. Updating current-state baseline collected during the strategy phase.
 - ii. Developing/documenting requirements leveraging methodology’s cloud requirements set.
 - iii. Completing analysis (alternatives, technologies, brands) and assessing cloud brokerage (intermediation, aggregation, and arbitration

- iv. Assessing service/application and licensing capability with virtualization/cloud and orchestration.
- v. Assessing service/application architecture for benefits from cloud automation.
- vi. Assessing and design integration of cloud with existing landscape.
- vii. Finalizing definition future-state architecture: vendor’s cloud reference architecture, cloud model, cloud type, cloud security.
- viii. Completing initial and detailed design: Cloud Network element design, Cloud Storage element design, Cloud Compute element design.
- ix. Completing traceability assessment of design to requirements.
- x. Documenting bill of materials.

3. Transition – activities include:

- a. Documenting transition and communicating the project plan/schedule
- b. Acquiring bill of materials
- c. Implementing, testing, and documenting infrastructure (network, compute, storage, virtualization), cloud services (self-service, charge back, measured service, cloud operating environment, and orchestration), and cloud storefront (catalog, portal, provisioning, management of workflow, approvals, financial controls
- d. Integrating multi-cloud management and monitoring systems with customer systems
- e. Engaging cloud brokerage, if appropriate (intermediation, arbitrage, aggregation)
- f. Bundling applications for migration and scheduling migration events
- g. Migrating application and services to cloud
- h. Transforming organization (roles and responsibilities, knowledge transfer, and training)
- i. Facilitating creation/update of customer policies, processes, procedures for operations

4. Operation – activities include:

- a. Ensuring available, reliable, and functional cloud service that meets requirements and demand resulting in higher user satisfaction
- b. Measuring cloud service performance
- c. Recovering cloud service operational costs
- d. Optimizing and integrating the production support team

- e. Provisioning of cloud service rapidly
- f. Responding to business/mission changes through a cloud services architect role
- g. Documenting operating procedures facilitating disaster recovery, cross-training, etc.

Figure 1 provides a notional view of the State of Hawai'i Cloud Computing Framework.

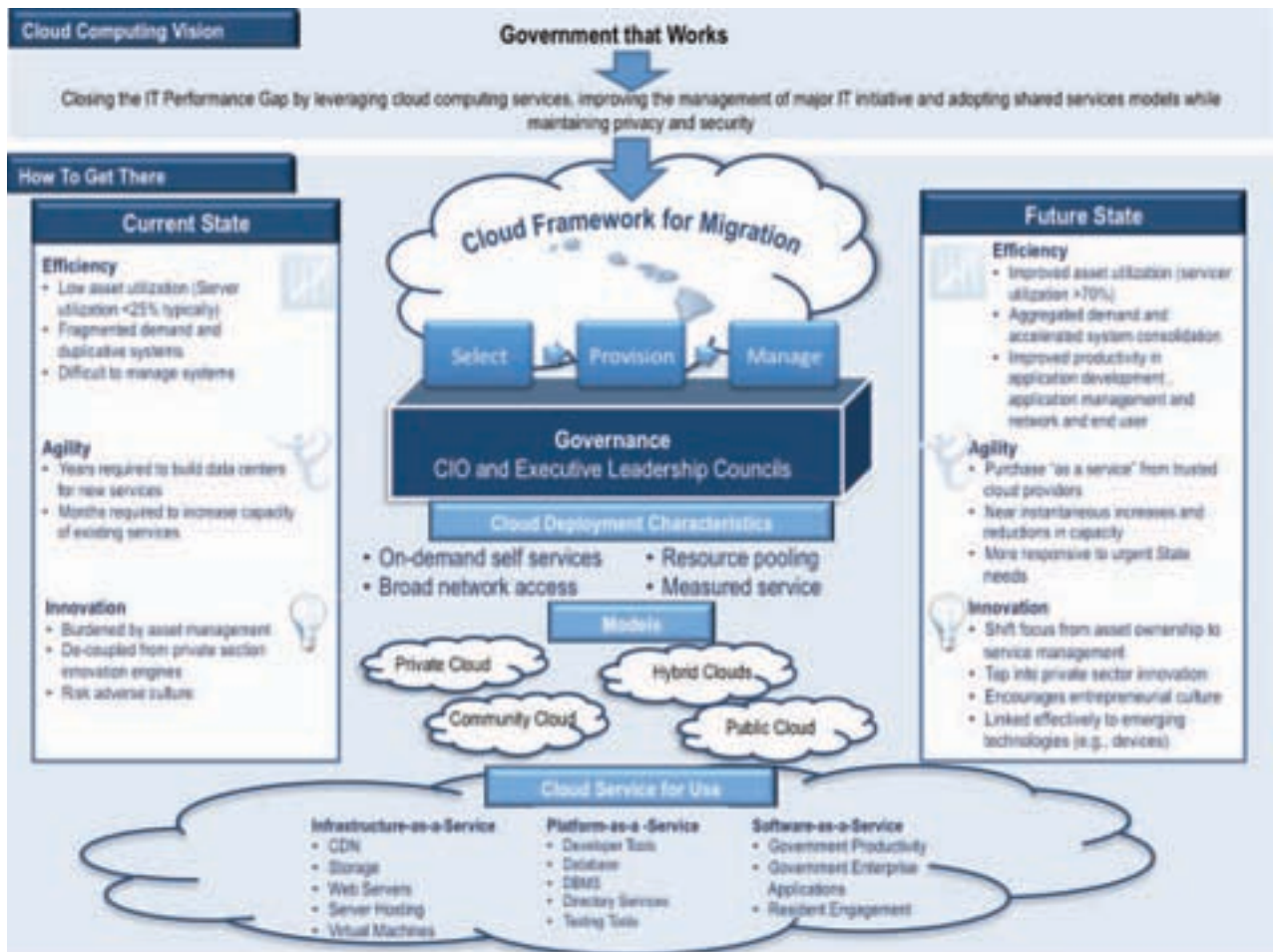


Figure 35: Notional View of Cloud Computing Framework

Table 26 represents the hosting, cloud, and data center sub-domain description.

Table 26: Hosting, Cloud, and Data Center Sub-Domain Description

Infrastructure Hosting, Cloud and Data Center Sub-Domain	Sunset Products / Standards	Current Supported Products/ Standards	Preferred Products / Standards	Emerging Trends
Data Center Facility Site and Construction	Urban location	Non-flood plan, above grade	ANSI/TIA-942 or TIA-942 (2005, 2008, 2010) Uptime Institute (1995) Tier structure	Movement toward Tier 3 Data Centers based on Design Documents, Constructed Facility, and Operational Sustainability
Cloud Services Reference Model		National Institute of Science and Technology. http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf . Revised 24 July 2011.		NIST 500 and 800 publications

DISASTER RECOVERY SUB-DOMAIN

Disaster recovery options are identified to ensure the ability to continue required operations post disaster.

BACKUP - RESTORE

The backup environment design will implement leading technologies to provide data protection services. The design provides a diverse platform topology containing a software suite that integrates and manages disparate physical storage mediums for the sole purpose of protecting State of Hawai`i data.

The selection of a single backup will resolve several cross-disciplinary design requirements. The backup/restore product will implement a distributed client-server application that provides data protection support for the State of Hawai`i's enterprise servers. The solution will consist of a master server with associated software components, media servers with associated software components managing storage devices and client software that provides the capability to backup, restore and archive files or directories, and volumes or partitions that exist on State of Hawai`i data center enterprise servers.

The following describes the future state of the backup-restore environment:

- Backup - Restore System Inputs and Outputs
- During a backup or archive, the client sends backup data across the dedicated backup network to a server. The server manages the type of storage and retention period that is specified in the backup policy.
- During a restore, users can browse, and then select the files and directories to recover. The backup/restore product finds the selected files and directories and restores them to the disk on the client via the dedicated backup network.
- Policies determine when backups occur. Policies include schedules for automatic, unattended Backups of the clients (server-directed backups). Policies also define when to back up and restore files manually (user-directed operations).
- Administrators can set up periodic or calendar-based schedules to perform automatic, unattended backups for clients across a network. An administrator can carefully schedule backups to achieve systematic and complete backups over a period of time, and optimize network traffic during off-peak hours.

BACKUP – RESTORE SYSTEM BEHAVIOR

Backup system behavior will be predicated on recovery capability—there is no such thing as a “backup service level.” Two key concepts will underpin all recovery service levels:

- Recovery Point Objective (RPO) - The most recent state to which an application or server can be recovered in the event of a failure. The RPO is directly linked to the frequency of the

protection process; if the application is protected by backups alone, then it means how often a backup is run.

- Recovery Time Objective (RTO) - The time required to recover the application or server to the RPO from the moment that a problem is detected. Many factors influence the RTO including the provisioning of hardware and the roll-forward time for application transaction logs—but one constant factor is the time needed to restore the data from the backup or snapshot that forms the RPO.

Figure 1 provides a notional view of a multi-Site Data Center Disaster Recovery framework for the Hawai`i COOP/DR solution.

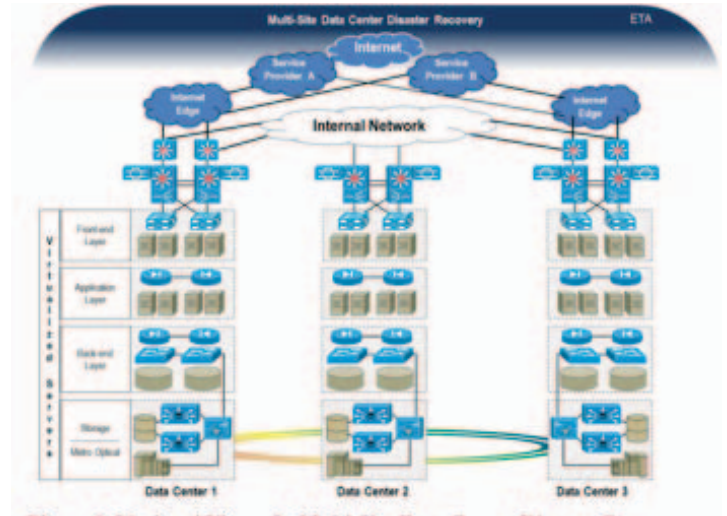


Figure 36: Notional View of a Multi-Site Data Center Disaster Recovery Environment

In addition, the future state vision from Infrastructure Working Group regarding disaster recovery and continuity of operations plan (COOP) includes the following elements:

- Data Recovery/COOP
 - Real time backup and point in time recovery
- Time to restore requirements
- Protection of mission critical applications including: Financials, Revenue Collection, Accounting, Human Resources, Welfare, Health, Benefits and Pension Administration
- Load balancing between the primary and secondary sites
- DR/COOP
- Load Balanced Data Centers
- Fault Tolerance, hot site, active-active
- Loss of connectivity between island data centers (radio, microwave)
- Loss of connectivity to mainland
- Backup power
- Test DR/COOP plans
- Long term fueling issue (IT and Procurement)
- Alternative power technology (fuel cell, geothermal, wind, etc.)

Table 27 represents the description of the Disaster Recovery Sub-Domain.

Table 27: Disaster Recovery Sub-Domain Description

Infrastructure Hosting, Cloud and Data Center Sub-Domain	Sunset Products / Standards	Current Supported Products/ Standards	Preferred Products / Standards	Emerging Trends
Off Island Storage		Iron Mountain	<ul style="list-style-type: none"> • Automatic Disparate array replication • Bandwidth optimization • Consistency Sets 	Cloud based solutions for “active-active” and “active-passive”
Application Recovery		Real time load balance	End-to-end redundancy High fault tolerance SATA FireWire (IEEE-1394)	Image-based or snapshot technology RAID 6 SATA FireWire (IEEE-1394) LTO-3
Network Connectivity		Dual path multi-provider	Dual path multi-provider	No single point of failure

SERVICES AND STORAGE SUB-DOMAIN

The services and storage sub-domain represent the hardware and operating systems where enterprise applications and systems reside. These platforms will be scalable, highly fault tolerant, and designed with failover capabilities for mission critical applications. Figure 1 is a notional representation of a data center storage environment that will be considered in the new Hawai'i data center implementation.

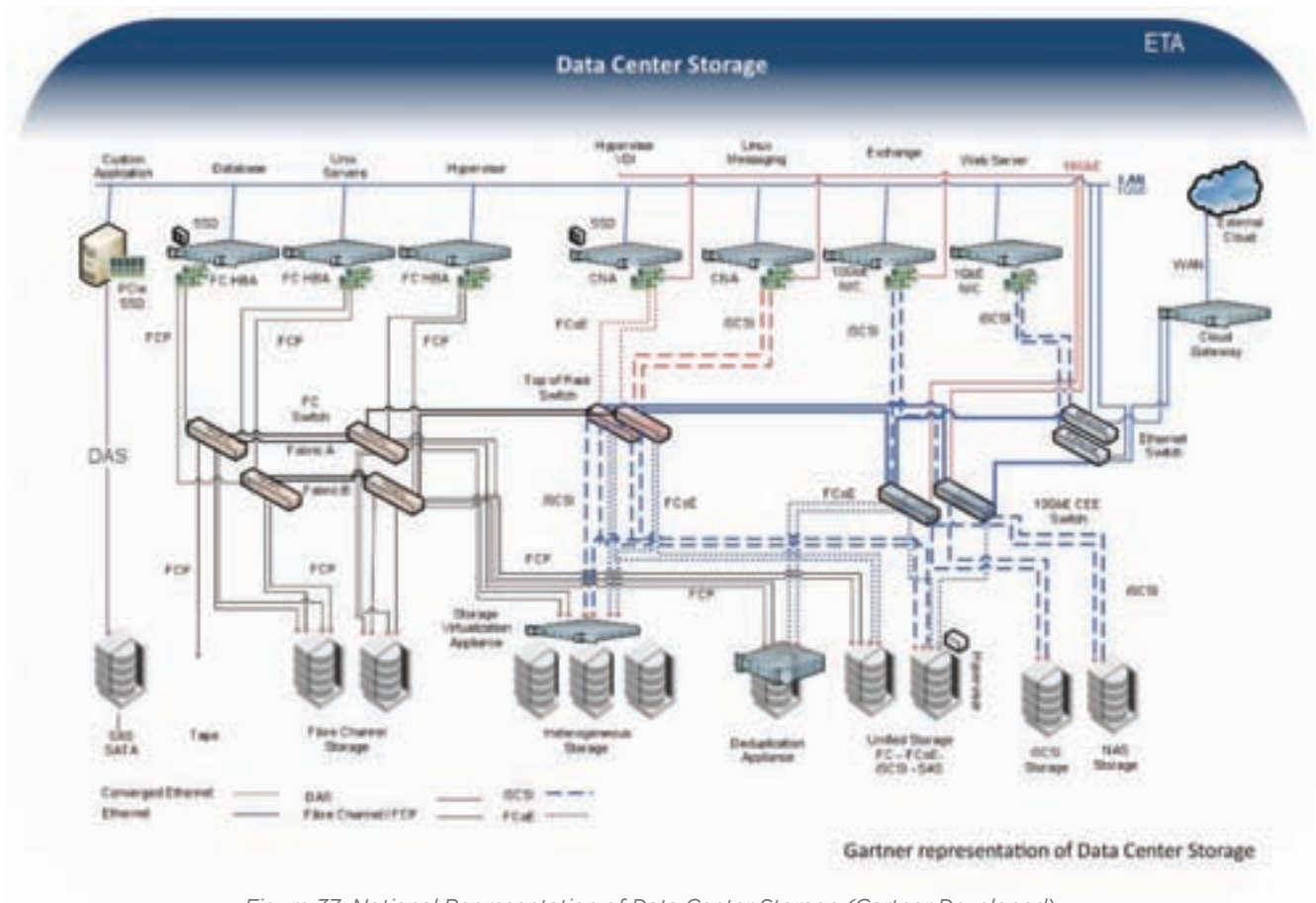


Figure 37: Notional Representation of Data Center Storage (Gartner Developed)

Table 28: Servers and Storage Sub-Domain Description

Infrastructure Hosting, Cloud and Data Center Sub-Domain	Sunset Products / Standards	Current Supported Products/ Standards	Preferred Products / Standards	Emerging Trends
Mainframe Platforms	OS/390, Z/OS release 9 and below	Z/OS	ERP product suite; Virtualization to fullest extent	Specialty blades; green equipment; Big Data analytics; Virtualization
Server Operating System	Windows 2003 and below, NT4, Novell Netware, Solaris 8, AIX 5.3 and below	Solaris 9 and above, AIX 6.1 and above, Windows 2008 and above	Windows Server 8, Solaris 11	Windows Server 8, Solaris 11
Server Platforms	Compaq, 3rd party	Dell, HP, IBM, Sun	Cloud virtualization	Converged solutions such as Cisco UCS
Server Virtualization Platforms		VMware, Citrix	“cloud” integrated platform	“cloud” integrated platform
Storage Platforms		EMC, IBM, NetApp	SAN	SAN
Storage Platforms (Backup) Enterprise		StorageTek,	SAN	SAN
Storage Platforms (Backup) Enterprise Software		IBM Tivoli Storage Manager	SAN	SAN
Storage Platforms (Backup) End User		Minimal		Cloud based storage, security and retrieval

DIRECTORY SERVICES SUB-DOMAIN

The services and storage sub-domain represent the hardware and operating systems. Directory services are software systems that store, organize, and provide access to information (e.g., names, contact information, computer hardware). The resulting directory will be used by other systems to identify users and process information flows related to a person or group of persons. The future state will include directory services at the enterprise level for authentication and communications. Table 29 represents this sub-domain.

Table 29: Directory Services Sub-Domain Description

Infrastructure Hosting, Cloud and Data Center Sub-Domain	Sunset Products / Standards	Current Supported Products/ Standards	Preferred Products / Standards	Emerging Trends
Enterprise Directory Services	Novell	Lightweight Directory Access Protocol (LDAP) version 3, MS Active Directory Domain Services	X.500; Lightweight Directory Access Protocol (LDAP) version 3, MS	Active Directory Domain Services
Web Authentication		SiteMinder	802.11i authentication and encryption Digital certificates; Public key infrastructure	Emerging PaaS; graphical authentication techniques; image-based authentication

ENTERPRISE SYSTEMS MANAGEMENT SUB-DOMAIN

Enterprise systems management refers to the activities, methods, procedures, and tools that pertain to the operation, administration, maintenance, and provisioning of networked systems.

- Operation deals with keeping the network (and the services that the network provides) up and running smoothly. It includes monitoring the network to spot problems as soon as possible, ideally before users are affected.
- Administration includes tracking of resources in the network and how they are assigned and it includes all the “housekeeping” that is necessary to keep the networked systems under control.
- Maintenance is concerned with performing repairs and upgrades (e.g. when equipment must be replaced, when a router needs a patch for an operating system image, when a new switch is added to a network). Maintenance also involves

corrective and preventive measures to make the managed network elements run “better” such as adjusting device wconfiguration parameters.

- Provisioning is concerned with configuring resources in the network to support a given service. For example, this might include setting up the network so that a new customer can receive voice service.

Data for enterprise systems management will be collected through several mechanisms, including agents installed on infrastructure, synthetic monitoring that simulates transactions, logs of activity, sniffers and real user monitoring. Table 30 describes this sub-domain further.

Table 30: Enterprise Systems Management Sub-Domain Description

Infrastructure Hosting, Cloud and Data Center Sub-Domain	Sunset Products / Standards	Current Supported Products/ Standards	Preferred Products / Standards	Emerging Trends
LAN Diagnostics		WireShark, TCPdump		
LAN Monitor		SolarWinds Orion, SNMP compliant	IEEE 802 LAN/MAN Standards Committee	Correlation and alarm de-duplication with impact analysis of alarms
LAN Performance		SolarWinds Orion		IPFIX or RMON
LAN Reporting		MRTG		SLA portal reporting
WAN Diagnostics		Cisco Works, Sniffer, WireShark, Ethereal		Network based with auto data log capability
WAN Monitor		SolarWinds Orion, SNMP compliant		Correlation and alarm de-duplication with impact analysis of alarms
WAN Performance		MIB, SolarWinds,		Synthetic modeling with proactive threshold model
WAN Reporting		MRTG		SLA portal reporting
Intrusion Detection		Snort		Stack based intrusion detection systems
Intrusion Prevention		Cisco IPS		Integrated Network/Wireless/Host based prevention in network.
Security Diagnostics		Vulnerability scanners, Nessus		Integrated data Loss prevention platform

Table 30: Enterprise Systems Management Sub-Domain Description

Infrastructure Hosting, Cloud and Data Center Sub-Domain	Sunset Products / Standards	Current Supported Products/ Standards	Preferred Products / Standards	Emerging Trends
Security Monitor		ArcSight		Integrated Security information and event management
Security Performance		ArcSight		Integrated Security information and event management
Security Reporting		ArcSight		Integrated Security information and event management
Application Performance				Synthetic modeling with proactive threshold model

ETA TRANSITION AND SEQUENCING PLANNING SUMMARY FOR INFRASTRUCTURE DOMAIN

The following provides a list of the key projects and initiatives required to achieve the future state for the infrastructure domain.

Develop and Construct or Build Out a Primary and Backup Data Center Environment

Plan and create two new data centers (primary and a backup or disaster recovery site) with the participation of both the technology and business organizations. This activity will require a committed team that has technical depth in a number of areas:

- Complex Project Management
- Information Assurance and Security
- Business Relationship Management
- Technology Infrastructure
- Application Development, Database Management and Operations
- Application Testing
- Data Replication
- Systems Migration
- Systems Consolidation

Other required planning activities include:

- Performing a complete analysis of current servers and their utilization so they can be more effectively leverage in the new environment;



- Virtualization planning to reduce number of physical servers and to drive improvements in Disaster Recovery
- Consolidation planning for database servers, where appropriate
- Consolidation of storage onto SAN
- Reduction of the applications footprint by lowering the number of servers per application
- Identification of applications that require transformation
- Reduction of capital requirements for Technology Solutions
- Creation a systems standardization plan
- Migration to a standardized platform (Cloud, Server Type, OS, Database, etc.) where appropriate
- Server refresh cycle planning.
- Develop an overall DR approach.
- Determine where the primary data center should reside.
- Perform a high-level cost analysis of bringing State facilities up to an acceptable level of performance versus cost of hosting services with an accredited and certified third-party facility.

Due to the criticality of the hosting, cloud, and data center sub-domain, a number of initiatives will be launched to make key determinations relative to the environment prior to the actual development. The following represent these activities and actions in detail.

Define Primary Data Center and DR Strategy Based on Three Alternatives

This initiative formalizes the strategy for the creation and location of the Primary Data Center and how disaster recovery will be addressed within the State. The following three alternatives have already been identified for further consideration.

- Remain in Kalanimoku
- Considerations - substantial expenditure to address cooling, airflow, structural inefficiencies, power distribution, and UPS requirements; flooding concerns; alternative locations within the building on the second or third floor to reduce the threat of flood water entering the basement.
- Utilize third-party facilities as a primary and DR data center configuration

- Considerations - how to leverage a third-party facility as a co-location site for servers, storage, and network equipment; management adjustments; configuration and deployment for servers and applications; certified in environmental controls, power, 24x7 services, and physical security; near-term and long-term needs.

- Blended strategy between a third party and State facilities.

- Considerations - utilization of a third-party location as the primary data center while retaining an existing or new State facility for DR needs or vice versa.

The strategy serves as the launching point for the other initiatives described below. The estimated cost of this initiative is Pending Review.

CONSOLIDATE DATA CENTERS

This initiative builds off the direction set by the Primary Data Center and DR Strategy and addresses the consolidation of services, hardware, and physical data centers. The consolidation planning begins by using the Federal Data Center Consolidation Initiative (FDCCI) to classify the existing facilities and their overall footprint as illustrated in Table 31.

Table 31: Server Closets, Server Rooms, and Data Centers by Department

Departments	Server Closet (<200 sq. ft.)	Server Room (< 500 sq. ft.)	Data Center (> 500 sq. ft.)
CSEA (AG)		X	
HCJDC (AG)		X	
B&F	X		
DAGS (non-ICSD)	X		
DBEDT	X		
DCCA		X	
DHHL		X	
DHRD		X	
DHS		X	
DLIR		X	
DLNR		X	
DOD		X	
DOE			X
DOH		X	
DOT		X	
DOTAX		X	

⁴The FDCCI definition of computing space - any room devoted to data processing servers, i.e., including server closets (typically < 200 sq. ft.) and server rooms (typically < 500 sq. ft.) within a conventional building, just like larger floor spaces or entire buildings dedicated to housing servers, storage devices, and network equipment are defined as data centers (typically >500 square feet)."

Table 31: Server Closets, Server Rooms, and Data Centers by Department

Departments	Server Closet (<200 sq. ft.)	Server Room (< 500 sq. ft.)	Data Center (> 500 sq. ft.)
HDOA	X		
PSD		X	
UH			X
ICSD			X
GOV/LT GOV	X		

Table 27 represents the description of the Disaster Recovery Sub-Domain.

Table 32: Estimated Costs to Complete a Data Center Consolidation

Fiscal Year	Est. Total Hrs	Est. Hawai'i IT Labor Cost	Equipment and Hardware	Est. Leases	Est. Other	Est. Total Cost
13	Pending Review	Pending Review	Pending Review	Pending Review	Pending Review	Pending Review
14	Pending Review	Pending Review	Pending Review	Pending Review	Pending Review	Pending Review
15	Pending Review	Pending Review	Pending Review	Pending Review	Pending Review	Pending Review
16	Pending Review	Pending Review	Pending Review	Pending Review	Pending Review	Pending Review
17	Pending Review	Pending Review	Pending Review	Pending Review	Pending Review	Pending Review
18	Pending Review	Pending Review	Pending Review	Pending Review	Pending Review	Pending Review
19	Pending Review	Pending Review	Pending Review	Pending Review	Pending Review	Pending Review
20	Pending Review	Pending Review	Pending Review	Pending Review	Pending Review	Pending Review
21	Pending Review	Pending Review	Pending Review	Pending Review	Pending Review	Pending Review
22	Pending Review	Pending Review	Pending Review	Pending Review	Pending Review	Pending Review
23	Pending Review	Pending Review	Pending Review	Pending Review	Pending Review	Pending Review
Total	Pending Review	Pending Review	Pending Review	Pending Review	Pending Review	Pending Review

Table 33: Projects and Initiatives Associated with Data Center Consolidation

Fiscal Year Activity	Description of Tasks
Activity FY13	Description
Planning and Project Management	<ul style="list-style-type: none"> • Gather Requirements • Create the Engineering Design team structure and membership • Build and Maintain the Risk Matrix • Establish and Train to the Standard Engineering Design Process • Establish Business Management to handle IT procurement, contract, negotiation activities • Perform “Design Week” preliminary design activities, with vendor consulting support
Analysis of Alternative (AoA) for Cloud solution	<ul style="list-style-type: none"> • Prepare RFI/RFP • Perform Analysis of Alternatives (Trade Study) • Perform Procurement and Negotiation • Cloud Training and Certification
AoA for Non-State Owned Data Center Site and preliminary design of initial infrastructure	<ul style="list-style-type: none"> • Prepare RFI/RFP • Perform Analysis of Alternatives • Perform Procurement and Negotiation • Design Cage Build out • Design Cable/Cabinet Build out • Design Circuit plans for WAN, internet, MetroE, MPLS
Activity FY14	Description
Planning and Project Management	<ul style="list-style-type: none"> • Update the Risk Matrix • Establish and Train to the Standard Engineering Design Process • Establish Business Management to handle IT procurement, contract, negotiation activities
Cloud solution	<ul style="list-style-type: none"> • Cloud Training and Certification
Non-State Owned Data Center Equipment Installation and Implementation	<ul style="list-style-type: none"> • Issue final design and final Bills of Materials (BOMs) • Procurement and Installation • Foundation - Network Engineering • Foundation - Network Security • Foundation - Network Services • Traditional - Storage • Traditional - Physical Compute • Traditional - Backup • Cloud solution • Infrastructure Testing • Operations & Maintenance
Activity FY15	Description
Planning and Project Management	<ul style="list-style-type: none"> • Update the risk matrix • Empower business management to handle IT procurement, contract, negotiation activities
Cloud solution	<ul style="list-style-type: none"> • Cloud Training and Certification
Non-State Owned Data Center O&M	<ul style="list-style-type: none"> • Operations and Maintenance • Test Continuity of Operations

Table 33: Projects and Initiatives Associated with Data Center Consolidation

Fiscal Year Activity	Description of Tasks
Activity FY16	Description
Planning and Project Management	<ul style="list-style-type: none"> • Update the Risk Matrix • Empower Business Management to handle IT procurement, contract, negotiation activities
Non-State Owned Data Center O&M	<ul style="list-style-type: none"> • Operations and Maintenance • Load level with Secondary Site • Test Continuity of Operations
Activity FY17	Description
Planning and Project Management	<ul style="list-style-type: none"> • Update the Risk Matrix • Empower Business Management to handle IT procurement, contract, negotiation activities
Non-State Owned Data Center O&M	<ul style="list-style-type: none"> • Operations and Maintenance • Load level with Secondary Site • Test Continuity of Operations
Activity FY18	Description
Planning and Project Management	<ul style="list-style-type: none"> • Update the Risk Matrix • Empower business management to handle IT procurement, contract, negotiation activities
Non-State Owned Data Center O&M	<ul style="list-style-type: none"> • Operations and Maintenance • Define Technology Refresh Cycle for Hardware • Load level with Secondary Site • Test Continuity of Operations • Operations and Maintenance
Activity FY19	Description
Planning and Project Management	<ul style="list-style-type: none"> • Update the Risk Matrix • Empower Business Management to handle IT procurement, contract, negotiation activities
Non-State Owned Data Center O&M	<ul style="list-style-type: none"> • Operations and Maintenance • Load level with Secondary Site • Test Continuity of Operations
Activity FY20	Description
Planning and Project Management	<ul style="list-style-type: none"> • Update the Risk Matrix • Empower Business Management to handle IT procurement, contract, negotiation activities
Non-State Owned Data Center O&M	<ul style="list-style-type: none"> • Operations and Maintenance • Load level with Secondary Site • Test Continuity of Operations
Activity FY21	Description
Planning and Project Management	<ul style="list-style-type: none"> • Update the Risk Matrix • Empower Business Management to handle IT procurement, contract, negotiation activities
Non-State Owned Data Center O&M	<ul style="list-style-type: none"> • Operations and Maintenance • Load level with Secondary Site • Test Continuity of Operations

Table 33: Projects and Initiatives Associated with Data Center Consolidation

Fiscal Year Activity	Description of Tasks
Activity FY22–23	Description
Planning and Project Management	<ul style="list-style-type: none"> • Update the Risk Matrix • Empower Business Management to handle IT procurement, contract, negotiation activities
Non-State Owned Data Center O&M	<ul style="list-style-type: none"> • Operations and Maintenance • Load level with Secondary Site • Test Continuity of Operations

DEVELOP SECONDARY DATA CENTER (STATE OWNED FACILITY)

The development of a secondary data center includes the build out of a mirrored production environment, while also serving as the recovery site for the primary data center. Maximum protection for the State’s continuity of operations will be addressed with the near-line data backup and recovery capability at the primary data center coupled with the mirrored production workloads at the secondary data center coupled with off-site backup capabilities to the outer islands as well as the Mainland. In turn, this effectiveness requires an alignment of business continuity planning with articulated business goals. Effective disaster recovery and business continuity planning depends on the State’s ability to identify critical processes and technologies, maintain and recover functionality after a planned or unplanned event, and balance the risks with the costs of continuity efforts.

For example, Dell provisions more than 100 percent capacity for each application so that it can split application load balancing across multiple data centers. Each application has 75 percent of required capacity in each data center— lending each application 150 percent of its nominal capacity requirement. Not only does this load-balancing strategy translate to high-performance applications, but it also helps ensure that disaster recovery and failover capabilities are being tested every moment of every day. This way, when Dell needs to implement its disaster recovery plan, the company knows it will work because it is already part of the existing load-balancing strategy .

Table 34: Estimated Costs to Develop Secondary Data Center

Fiscal Year	Est. Total Hrs	Est. Hawai'i IT Labor Cost	Equipment and Hardware	Est. Leases	Est. Other	Est. Total Cost
13	Pending Review	Pending Review	Pending Review	Pending Review	Pending Review	Pending Review
14	Pending Review	Pending Review	Pending Review	Pending Review	Pending Review	Pending Review
15	Pending Review	Pending Review	Pending Review	Pending Review	Pending Review	Pending Review
16	Pending Review	Pending Review	Pending Review	Pending Review	Pending Review	Pending Review
17	Pending Review	Pending Review	Pending Review	Pending Review	Pending Review	Pending Review
18	Pending Review	Pending Review	Pending Review	Pending Review	Pending Review	Pending Review
19	Pending Review	Pending Review	Pending Review	Pending Review	Pending Review	Pending Review
20	Pending Review	Pending Review	Pending Review	Pending Review	Pending Review	Pending Review
21	Pending Review	Pending Review	Pending Review	Pending Review	Pending Review	Pending Review
22	Pending Review	Pending Review	Pending Review	Pending Review	Pending Review	Pending Review
23	Pending Review	Pending Review	Pending Review	Pending Review	Pending Review	Pending Review
Total	Pending Review	Pending Review	Pending Review	Pending Review	Pending Review	Pending Review

⁵<http://www.dell.com/downloads/global/power/ps1q06-20060124-CoverStory.pdf>

Table 35 represents the initiatives and projects for the Secondary Data Center.

Table 35: Projects and Initiatives Associated with Secondary Data Center

Fiscal Year Activity	Description of Tasks
Activity FY13	Description
Planning and Project Management	<ul style="list-style-type: none"> • Update the Risk Matrix • Empower Business Management to handle IT procurement, contract, negotiation activities
Analysis of Alternative (AoA) for State Owned Data Center Site	<ul style="list-style-type: none"> • Engage Architect Engineer • Engage process for Site Evaluation, Site surveys, building retrofit management, permitting, etc. • Engage appropriate Hawaiian Home Lands, as necessary
Activity FY14	Description
Planning and Project Management	<ul style="list-style-type: none"> • Update the Risk Matrix • Establish Business Management to handle IT procurement, contract, negotiation activities
Analysis of Alternative (AoA) for State Owned Data Center Site	<ul style="list-style-type: none"> • Engage Architect Engineer • Engage process for Site Evaluation, Site surveys, building retrofit management, permitting, etc. • Engage appropriate Hawaiian Home Lands, as necessary • Submit proper documentation to DAGS • Complete necessary documentation and receive approval to proceed with construction
Activity FY15	Description
Planning and Project Management	<ul style="list-style-type: none"> • Update the Risk Matrix • Establish and Train to the Standard Engineering Design Process • Establish Business Management to handle IT procurement, contract, negotiation activities
State Owned Data Center Infrastructure Design activities	<ul style="list-style-type: none"> • Work with Architect Engineer • Work with Site Evaluation, Site surveys, building retrofit management, permitting, etc. • Work with appropriate Hawaiian Home Lands, as necessary • Complete necessary documentation and receive approval to proceed with construction • Infrastructure design for Cage, Cable plant, Cabinets, Circuits • Begin Construction/Retrofit
Activity FY16	Description
Planning and Project Management	<ul style="list-style-type: none"> • Update the Risk Matrix • Establish and Train to the Standard Engineering Design Process • Establish Business Management to handle IT procurement, contract, negotiation activities
State Owned Data Center Construction and Design activities	<ul style="list-style-type: none"> • Complete Construction/Retrofit • Issue final design and final Bills of Materials (BOMs) • Procurement and Installation • Foundation - Network Engineering • Foundation - Network Security • Foundation - Network Services Traditional - Storage • Traditional - Physical Compute • Traditional - Backup • Cloud solution • Infrastructure Testing • Operations & Maintenance

Table 35 represents the initiatives and projects for the Secondary Data Center.

Table 35: Projects and Initiatives Associated with Secondary Data Center

Fiscal Year Activity	Description of Tasks
Activity FY17	Description
Planning and Project Management	<ul style="list-style-type: none"> • Update the Risk Matrix • Empower Business Management to handle IT procurement, contract, negotiation activities
State Owned Data Center O&M	<ul style="list-style-type: none"> • Operations and Maintenance • Load level with Primary Site • Test Continuity of Operations
Activity FY18	Description
Planning and Project Management	<ul style="list-style-type: none"> • Update the Risk Matrix • Establish Business Management to handle IT procurement, contract, negotiation activities
State Owned Data Center O&M	<ul style="list-style-type: none"> • Operations and Maintenance • Load level with Primary Site • Test Continuity of Operations
Activity FY19	Description
Planning and Project Management	<ul style="list-style-type: none"> • Update the Risk Matrix • Establish Business Management to handle IT procurement, contract, negotiation activities
State Owned Data Center O&M	<ul style="list-style-type: none"> • Operations and Maintenance • Load level with Primary Site • Test Continuity of Operations
Activity FY20	Description
Planning and Project Management	<ul style="list-style-type: none"> • Update the Risk Matrix • Establish Business Management to handle IT procurement, contract, negotiation activities
State Owned Data Center O&M	<ul style="list-style-type: none"> • Operations and Maintenance • Load level with Primary Site • Test Continuity of Operations
Activity FY21	Description
Planning and Project Management	<ul style="list-style-type: none"> • Update the Risk Matrix • Establish Business Management to handle IT procurement, contract, negotiation activities
State Owned Data Center Construction and Design activities	<ul style="list-style-type: none"> • Define Technology Refresh Cycle for Hardware
Activity FY22–23	Description
Planning and Project Management	<ul style="list-style-type: none"> • Update the Risk Matrix • Establish Business Management to handle IT procurement, contract, negotiation activities
State Owned Data Center O&M	<ul style="list-style-type: none"> • Operations and Maintenance • Load level with Primary Site • Test Continuity of Operations

CREATE THREE ISLAND DATA CENTERS (STATE OWNED FACILITIES)

Once the Primary and Secondary sites are fully implemented, this initiative resolves access issues to the outer islands by providing all the islands of that State with access to affordable ultra, high-speed Internet by 2018. This will position Hawai'i to be the first state in the nation with 1 gigabit per second broadband connectivity at every public school, every public library, and every public university and college campus by using about Pending Review of federal monies received through the American Recovery and Reinvestment Act (ARRA). This will provide the opportunity to leverage connectivity for State offices at remote islands and improvements for State NGN.

In addition, Hawai'i is unique among the 50 States in that it is remote, susceptible to emergencies and catastrophic events that would not affect the contiguous States, and removed from the contiguous States creating latency issues therefore, providing satellite data center sites that are fully meshed and networked with the Primary and Secondary Sites on Oahu will provide the State of Hawai'i with continuity of government and operations.

The three island data centers initiative will include consideration of "Docking Centers" format where the "Data-Center-In-A-Box" system can plug in. The "Docking Center" would provide cooling, power, and network connectivity to the "Data-Center-In-A-Box", along with staff workspace. This approach minimizes the need to build multiple large data centers and provide a mobile Data Center where or when needed.

Table 36: Estimated Costs for Development of the Third Data Center

Fiscal Year	Est. Total Hrs	Est. Hawai'i IT Labor Cost	Equipment and Hardware	Est. Leases	Est. Other	Est. Total Cost
17	Pending Review	Pending Review	Pending Review	Pending Review	Pending Review	Pending Review
18	Pending Review	Pending Review	Pending Review	Pending Review	Pending Review	Pending Review
19	Pending Review	Pending Review	Pending Review	Pending Review	Pending Review	Pending Review
20	Pending Review	Pending Review	Pending Review	Pending Review	Pending Review	Pending Review
21	Pending Review	Pending Review	Pending Review	Pending Review	Pending Review	Pending Review
22	Pending Review	Pending Review	Pending Review	Pending Review	Pending Review	Pending Review
23	Pending Review	Pending Review	Pending Review	Pending Review	Pending Review	Pending Review
Total	Pending Review	Pending Review	Pending Review	Pending Review	Pending Review	Pending Review

Table 37: Projects and Initiatives Associated with Development of the Third Data Center

Fiscal Year Activity	Description of Tasks
Activity FY17	Description
Planning and Project Management	<ul style="list-style-type: none"> • Update the Risk Matrix • Empower Business Management to handle IT procurement, contract, negotiation activities
AoA for Three Island State Owned Data Center Site	<ul style="list-style-type: none"> • Engage Architect Engineer • Engage process for Site Evaluation, Site surveys, building retrofit management, permitting, etc.
Activity FY18	Description
Planning and Project Management	<ul style="list-style-type: none"> • Update the Risk Matrix • Empower Business Management to handle IT procurement, contract, negotiation activities
AoA for Three Island State Owned Data Center Site	<ul style="list-style-type: none"> • Engage Architect Engineer • Engage process for Site Evaluation, Site surveys, building retrofit management, permitting, etc. • Engage appropriate Hawaiian Home Lands, as necessary • Submit proper documentation to DAGS • Complete necessary documentation and receive approval to proceed with construction

Fiscal Year Activity	Description of Tasks
Activity FY19	Description
Planning and Project Management	<ul style="list-style-type: none"> • Update the Risk Matrix • Empower Business Management to handle IT procurement, contract, negotiation activities
AoA for Three Island State Owned Data Center Site	<ul style="list-style-type: none"> • Engage Architect Engineer • Engage process for Site Evaluation, Site surveys, building retrofit management, permitting, etc. • Engage appropriate Hawaiian Home Lands, as necessary • Submit proper documentation to DAGS • Complete necessary documentation and receive approval to proceed with construction • Infrastructure design for Cage, Cable plant, Cabinetry, Circuits
Activity FY20	Description
Planning and Project Management	<ul style="list-style-type: none"> • Update the Risk Matrix • Empower Business Management to handle IT procurement, contract, negotiation activities
Three Island State Owned Data Center Site Infrastructure Design and Build Activities	<ul style="list-style-type: none"> • Engage Architect Engineer • Engage process for Site Evaluation, Site surveys, building retrofit management, permitting, etc. • Engage appropriate Hawaiian Home Lands, as necessary • Submit proper documentation to DAGS • Complete necessary documentation and receive approval to proceed with construction
Activity FY21	Description
Planning and Project Management	<ul style="list-style-type: none"> • Update the Risk Matrix • Empower Business Management to handle IT procurement, contract, negotiation activities
Three Island State Owned Data Center Site Infrastructure Design and Build Activities O&M	<ul style="list-style-type: none"> • Operations and Maintenance • Load level with Primary Site • Test Continuity of Operations
Activity FY22–23	Description
Planning and Project Management	<ul style="list-style-type: none"> • Update the Risk Matrix • Empower Business Management to handle IT procurement, contract, negotiation activities
Three Island State Owned Data Center Site Infrastructure Design and Build Activities O&M	<ul style="list-style-type: none"> • Operations and Maintenance • Load level with Primary Site • Test Continuity of Operations

MIGRATE APPLICATIONS FROM THE CURRENT DATA CENTERS TO THE PRIMARY DATA CENTER

Once the Primary Data Center is implemented during FY14 (see Primary Data Center development initiative above), the next

activity will be migrating applications from the current data centers to the Primary Data Center, where data redundancy and disaster recovery considerations have been implemented as a high priority.

Table 38: Estimated Costs to Perform Application Migration

Fiscal Year	Est. Total Hrs	Est. Hawai'i IT Labor Cost	Equipment and Hardware	Est. Leases	Est. Other	Est. Total Cost
14	Pending Review	Pending Review	Pending Review	Pending Review	Pending Review	Pending Review
15	Pending Review	Pending Review	Pending Review	Pending Review	Pending Review	Pending Review
16	Pending Review	Pending Review	Pending Review	Pending Review	Pending Review	Pending Review
Total	Pending Review	Pending Review	Pending Review	Pending Review	Pending Review	Pending Review

Table 39 represents the key project for the Application Migration.

Table 39: Projects and Initiatives Associated with Application Migration

Fiscal Year Activity	Description of Tasks
Activity FY14	Description
Applications Characterization	<ul style="list-style-type: none"> • Issue RFI/RFP • Develop Rules of Engagement between vendor and State of Hawai'i • Develop Project Management function • Perform characterization, interdependencies, and scheduling function
Activity FY15	Description
Applications Characterization	<ul style="list-style-type: none"> • Define Key Migration Execution Roles • Begin migration of applications to Non-State Owned Data Center
Activity FY16	Description
Applications Characterization	<ul style="list-style-type: none"> • Complete migration of applications to Non-State Owned Data Center

DEVELOP A STATE-WIDE ACTIVE DIRECTORY SERVICES ENVIRONMENT

Plan and create a State-wide active directory services environment. Benefits of deploying Active Directory in a Network Operating system (NOS) management role include:

- Ability to centrally manage very large networks.
- Ability to eliminate resource domains, including the hardware and administration they entail.
- Policy-based desktop lockdown and software distribution.
- Ability to delegate administrative control over resources, where appropriate.
- Simplified location and use of shared resources.

- Site topology mirrors network topology.
- Dedicated use domain controllers
- Multiple DNS servers

Active Directory allows administrators to organize elements of a network (such as users, computers, devices, and so on) into a hierarchical, tree-like structure based on the concept of containership. The top level Active Directory container is called a forest. Within forests, there are domains. Within domains there are organizational units (OUs). This is called the logical model because it is designed independently from most physical aspects of the deployment, such as the number of replicas required within each domain and network topology. Estimated cost for this project is Pending Review.

It should be noted that all the above activities are inextricably linked the State of Hawai'i future network, OneNet.

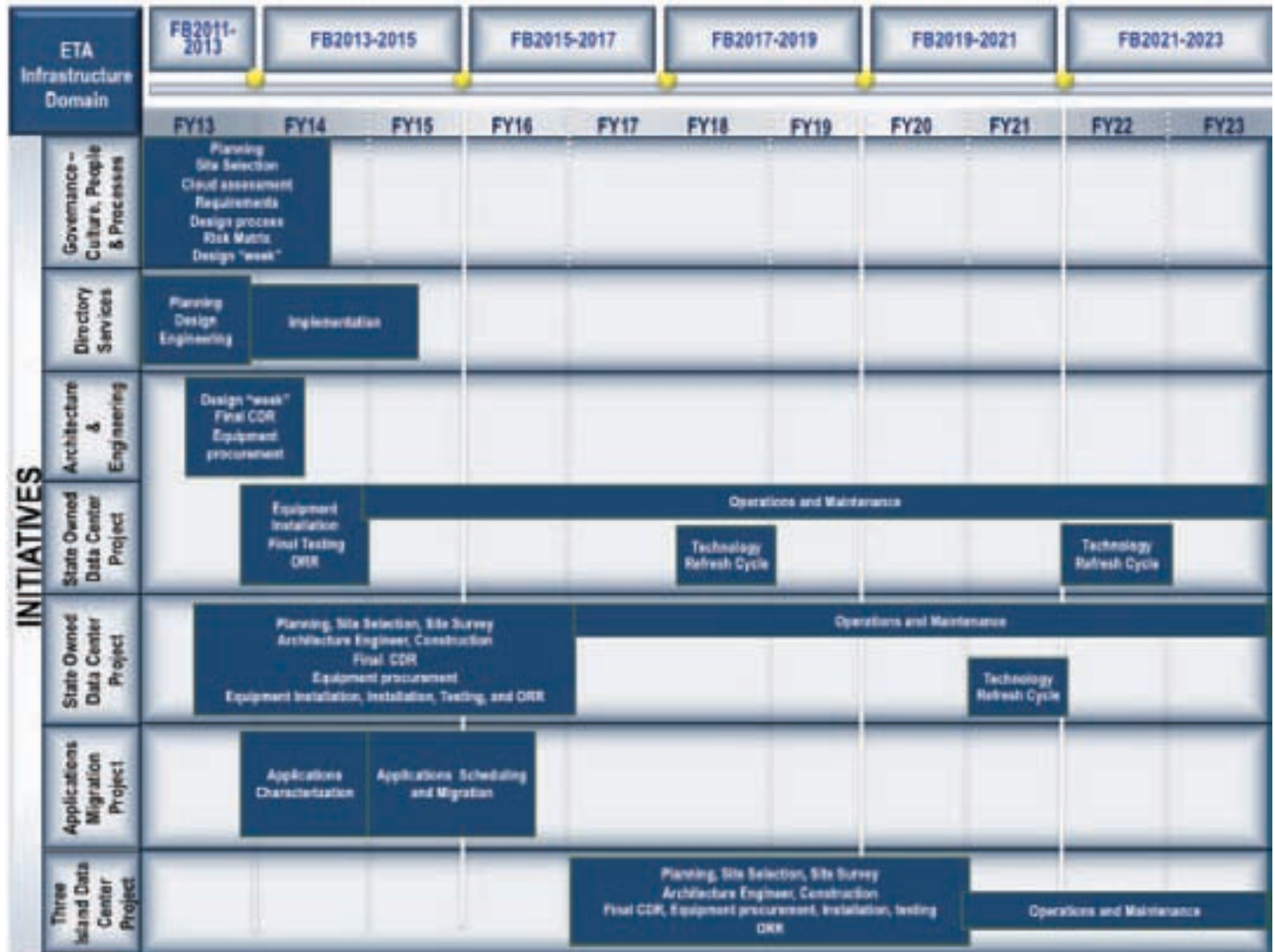


Figure 38: Roadmap to Achieve the Future State for the Infrastructure Domain

7.2.3.2 NETWORK DOMAIN

The Network Domain includes the network for the State and all associated services and technologies. The network consists of both wide-area network (WAN) and local-area network (LAN) components. The WAN extends the network outside buildings and beyond campuses. This is typically created by using circuits and routers to connect geographically separated LANs. The LAN interconnects devices over a geographically small area, typically in one building or a part of a building. The network architecture describes a common, high-performance, reliable, broadband network infrastructure providing data, video and voice communications for the State's distributed information processing and publishing environment.

CURRENT STATE SWOT FOR THE NETWORK DOMAIN

The State currently has specific centers of excellence in networking solutions and management practices. In its entirety, the State lacks collaboration on common solutions and standards, and has limitations on providing consolidated network management. This results in a general lack of: coordination, a centralized knowledgebase, compliance to best practices in a comprehensive fashion, and a robust, universal support model that is 24x7x365. Also, underlying system capacity knowledge is not being tracked and not readily available. In general the demand for network service provision overwhelms the current capacity and resource base.

FUTURE STATE VISION FOR THE NETWORK DOMAIN

The future state vision for the network domain is a single State of Hawai'i network (OneNet) which is deployed to provide every Department and its entire staff on every island with a high speed secure and highly reliable voice, video, and data services. At the heart of the OneNet will be a multi-path, mesh data center solution to provide virtual computing power, cloud-based

application and storage services, and full disaster recovery capabilities.

OneNet, with guaranteed performance levels, will take full advantage of new network technologies and fulfill the needs of all State Departments' employees and citizens in the State of Hawai'i for information access. The Internet, as a global networking infrastructure, continues to make the world a smaller and more demanding place. OneNet will be both wired and wireless and will truly create an "anytime, anywhere connected" networking environment. It will introduce an "always-connected" citizen community. Recent advances in convergence technologies not only promote the convergence of a single physical IP infrastructure, but also introduce convergence of feature-rich services that can be provided in a secure, reliable, cost effective manner to meet the State's mission.

The Network OneNet Working Group provided a detailed breakdown of activities by biennium with requirements as follows:

- 1.** OneNet must be a highly redundant, reliable, and available backbone for the five Data Centers.
- 2.** Data Center Connectivity
 - 2.1.** Data Centers provide POP for Internet and high speed interconnections to other Data Centers.
 - 2.2.** Redundant connections through private providers and State wireless systems i.e. microwave.
 - 2.3.** Integration of private carrier services to critical sites providing redundancy for immediate and surrounding sites.
 - 2.4.** Separate State fiber optic rings.
 - 2.4.1.** Networks based on access to dark fiber and optical Wave Division Multiplexers (WDMs providing additional bandwidth as needs grow.
 - 2.4.2.** Minimum requirements
 - 2.4.3.** 32 wavelengths
 - 2.4.4.** 1 and 10Gbps Ethernet
 - 2.4.5.** 2 to 10Gbps Fiber Channel
 - 2.4.6.** SONET OC-3 to OC-192

- 2.5.** Negotiate with Private carriers for bandwidth (dark fiber, dim fiber, leased circuits, etc.).
- 3.** High availability backbone sites must have the following:
 - 3.1.** 24x7 Access
 - 3.2.** Backup Power
 - 3.3.** Physical Security
 - 3.4.** Potential Candidates:
 - 3.4.1.** Utilize State facilities with existing infrastructure i.e. prisons and hospitals
 - 3.4.2.** Negotiate with the counties to utilize police, fire stations, and other facilities with the appropriate infrastructure.
 - 3.4.3.** Negotiate co-location terms in private carrier facilities and central offices. Benefit of allowing carriers to provided services faster and cheaper.
 - 3.4.4.** Create separate fiber optic ring infrastructure from other INET partners (DOE/UH) that is owned and controlled by the State.
 - 3.4.5.** DOE and UH can be customers of the State's network.
- 4.** Cost recovery based on telecom industry standard practices.
 - 4.1.** Line charges to customers based on subscribed bandwidth as well as optional subscribed services i.e. QoS/CoS.
 - 4.2.** Requirement for higher level of responsiveness (SLAs)
 - 4.3.** Non-recurring charges i.e. for infrastructure builds and engineering services.

Figure 39 depicts Hawai`i's OneNet enterprise network with complete end-to-end governance frameworks and support services. The enterprise LAN will provide users with all services on the private cloud while the WAN will provide redundant high speed links through three different carriers. Network Operations and Security Operations Centers will provide proactive continuous monitoring of the entire network keeping assets secure and available.

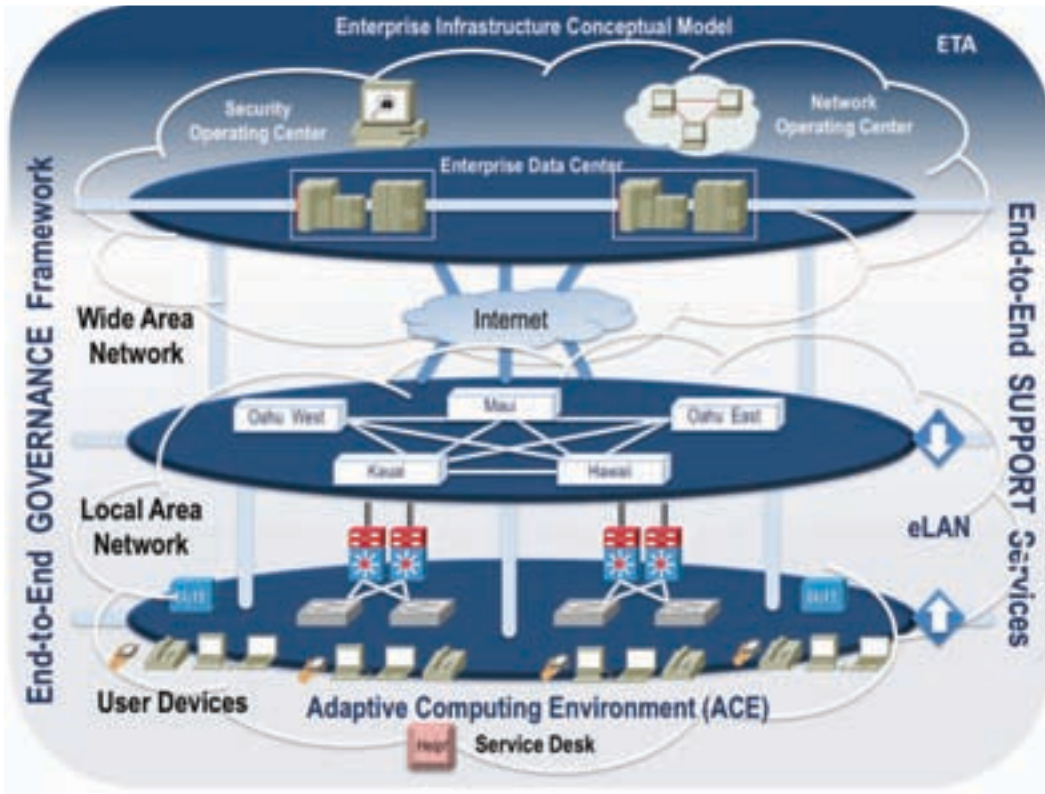


Figure 39: Conceptual Model of the Network Domain Infrastructure

The Hawai`i OneNet, further illustrated in Figure 40, will be modeled after validated designs based on industry standard best practices. The goal of the enterprise network is to provide a unified, common, and centrally managed infrastructure for IT services to run on. Using a common framework, this modular design will be scaled to accommodate different size needs quickly and easily.

For the future state vision the goal will be to have five fully meshed functional shared services centers (SSC) distributed across the islands to provide high availability, redundancy, fault tolerance, data backup and replication, disaster recovery, and always-on services to the State of Hawai`i (Figure 41).

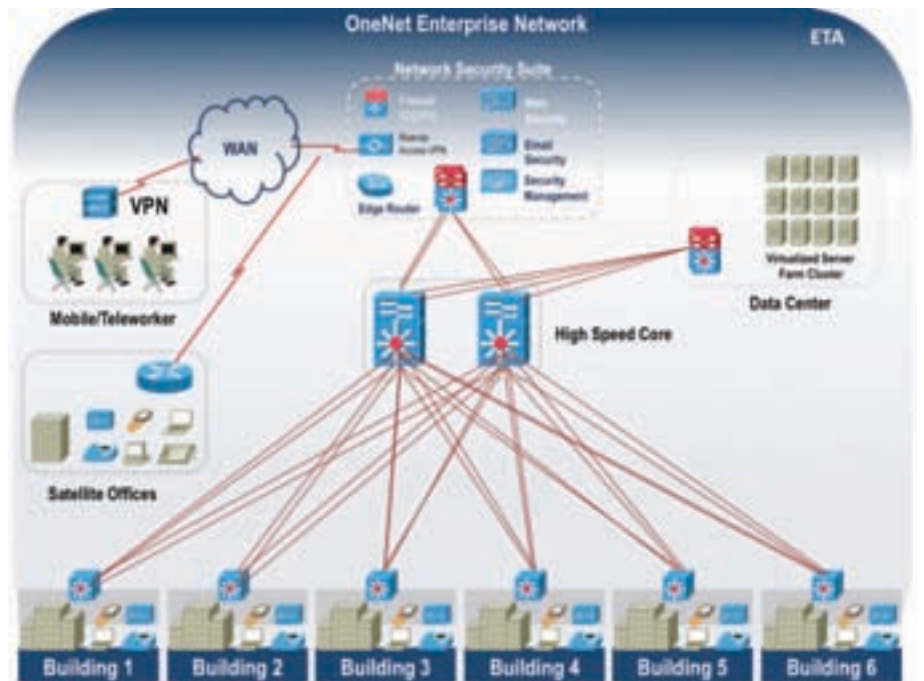


Figure 40: OneNet Future State Vision

Connections between shared services centers will be provided with dedicated high-speed fiber optic lines with service providers and state wireless connections acting as redundant and backup links respectively.

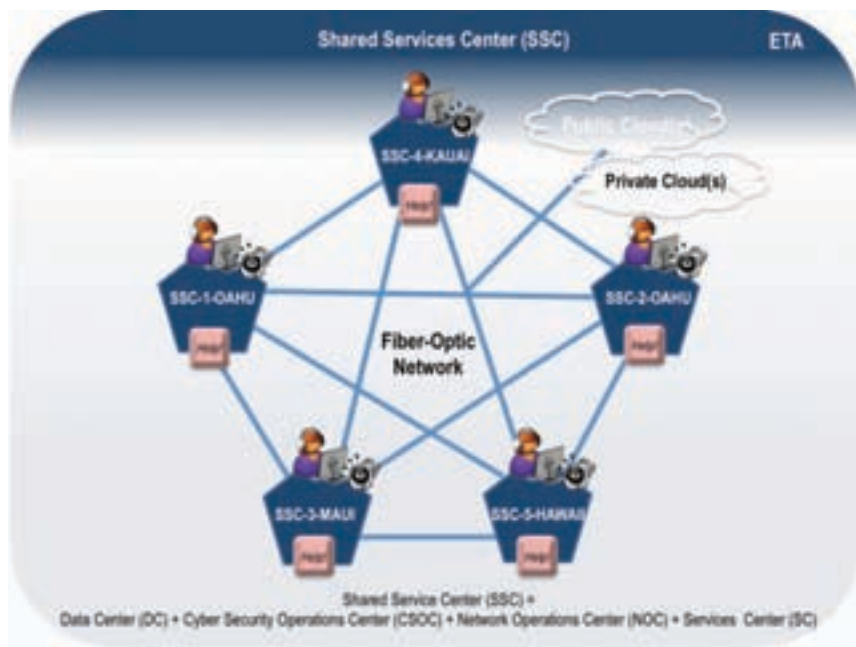


Figure 41: Shared Service Center Vision for the ETA

Guiding Principles for the Network Domain

1. Networks are able to adapt to growth and technology change when they support multiple traffic types (e.g. data, video, voice).

- The increasing investment in network infrastructures dictates that the life span of each additional component or enhancement be as long as possible. This will be accomplished if the design supports both current needs and anticipated growth potential.
- As business expands, networks expand. A flexible, open network design allows a business to minimize the costs and disruptions of configuration management while providing timely and responsive network changes when and where required.

1. Network access is a function of authentication and authorization, not of location.

- All users must obtain authentication via a user identification method consistent with the standards and usage guidelines set by Hawai'i
- Authorization of users must be performed according to the security rules of Hawai'i.
- In order to perform their job functions, users need to access services available from multiple sites within the enterprise, from a variety of public and private networks, and from the Internet.
- Networks are able to adapt to growth and technology change when they support multiple traffic types (e.g. data, video, voice).
- The increasing investment in network infrastructures dictates that the life span of each additional component or enhancement be as long as possible. This will be accomplished if the design supports both current needs and anticipated growth potential.

- As business expands, networks expand. A flexible, open network design allows a business to minimize the costs and disruptions of configuration management while providing timely and responsive network changes when and where required.

2. Network access is a function of authentication and authorization, not of location.

- All users must obtain authentication via a user identification method consistent with the standards and usage guidelines set by Hawai'i.
- Authorization of users must be performed according to the security rules of Hawai'i.
- In order to perform their job functions, users need to access services available from multiple sites within the enterprise, from a variety of public and private networks, and from the Internet.

3. Fully available networks are essential to the enterprise.

- Networks provide an increasingly important and necessary role in the execution of business functions and processes. The availability of the network 7/24/365 must be maintained in a consistent and complete manner up to 5-sigma uptime and availability.
- Networks consist of and rely on many interrelated and highly complex components distributed across a wide geographic area. Failure of any single component can have severe adverse effects on one or more business applications or services.
- Reliable networks contain no single point of failure. Networks are comprised of many components, and are often only as reliable as the weakest link. Therefore, reliability and redundancy must be built into the design, not added-on in an ad hoc manner.

- Bandwidth must be sufficient to accommodate new and expanding applications, different types of data (e.g., voice, data, image, and video), and a variety of concurrent users.
- The network must support software distribution and installation to a widely dispersed user community.
- The network must be designed to minimize latency.

4. Properly designed networks accommodate multi-vendor participation and support common, open, vendor-neutral protocols.

- Open, vendor-neutral protocols provide the flexibility and consistency that allows departments to respond more quickly to changing business requirements.

- Open, vendor neutral networks provide the flexibility and consistency that allows departments to respond more quickly to changing business and regulatory requirements.
- An open, vendor-neutral network to allow the State to choose from a variety of sources and select the most economical network solution without impacting applications and insulates the State from unexpected changes in vendor strategies and capabilities.
- Design applications to be transport-independent.

WIRED SUB-DOMAIN

This sub-domain includes wired WAN and LAN technologies and is described in Table 40.

Table 40: Wired Sub-Domain Description

Infrastructure Hosting, Cloud and Data Center Sub-Domain	Sunset Products / Standards	Current Supported Products / Standards	Preferred Products / Standards	Emerging Trends
Physical Layer			1000BASE-T –IEEE 802.3 (40), 1000BASE-TX – TIA/EIA 854	10GBASE-T - IEEE 802.3an-2006 with Category 6A ANSI/TIA/EIA-568-B.2-10 cables or better, WSON (Wavelength Switched Optical Networks)
Traffic Engineering		MPLS, QOS, COS	MPLS-TE, RSVP-TE	NSIS, MPLS-TP
LAN		SNMP managed switches	SNMPv3 managed multilayer network devices	Multi-chassis capable switches
Remote Access – Physical Layer		Broadband	Broadband, 4G-LTE	5G Pervasive Networks
Remote Access – Protocol Layer		SSL	VPN, SSL VPN	Microsoft DirectAccess
Interior Gateway Protocol			OSPF, IS-IS	Next Generation IGP with IPv6 support
Video Conferencing		H.323	Unified Communications	UCaaS (Unified Communications as a Service)
Video Streaming		MPEG 4	H.264	MPEG-DASH
Remote Management		SNMP, MIB	SNMPv3	Enterprise NCCM (Network Configuration and Change Management) tools

Table 40: Wired Sub-Domain Description

Infrastructure Hosting, Cloud and Data Center Sub-Domain	Sunset Products / Standards	Current Supported Products/ Standards	Preferred Products / Standards	Emerging Trends
Voice	Centrex	VoIP	Unified Communications	IP-PBX, Hosted Voice UCaaS
Mail Gateways		Cloud Based with central filtering	Cloud Email Solution	SaaS Email Hybrid Delivery Solution
Domain Name Servers		Single statewide primary and secondary with geographically separated failover	Distributed DNS NIST Special Publication 800-81 Secure Domain Name System (DNS) Deployment Guide NIST SP800-53	Secure Distributed DNS

WIRED SUB-DOMAIN

This sub-domain (Table 41) includes technologies (e.g., Blue-tooth, WiFi, satellite and cellular) that will be used by employees as required.

Table 41: Wireless Sub-Domain Description

Infrastructure Hosting, Cloud and Data Center Sub-Domain	Sunset Products / Standards	Current Supported Products/ Standards	Preferred Products / Standards	Emerging Trends
WiFi	802.11b/g	802.11n	802.11n	802.11ac, 802.11ad
WiFi- Security	WEP, WPA	802.1x w/ WPA2	WPA2-Enterprise (802.1x / EAP-TLS)	Femtocells
Cellular				
Satellite				
Bluetooth	Versions 1 and 2	Radio defaulted to off unless user activates. Version 3.0 and 4.0	Version 4.0	Pending Review

RADIO SUB-DOMAIN

The radio sub-domain will include any microwave or RF platforms in use for primary or emergency communications inter- and intra- island. Included are the facilities which support the transmission and reception as well as frequency management and required regulatory reporting. In the future today’s system’s limitations will be eliminated for the individuals representing transportation, public health, utilities, and public works, and public safety who rely on it.

The Radio Program mission is to ensure the effective use of Radio and microwave equipment and licensed spectrum, to oversee radio compliance by the Executive Branch, and to fill all State and

Federal legal requirements associated with radio matters. The following further describes the future direction for the Radio Program:

- Creating a Statewide Governance and Implementation process to the support the implementation of an Emergency Communications Plan
- Establishing goals and priorities for addressing deficiencies in the State’s emergency communications structure.
- Monitoring all Agencies’ Radio licensing, procurement, and FCC notices for ensuring statutory compliance.
- Assisting proper fulfillment throughout the State of reviews and reporting requirements for the Radio Program.

- Providing Oversight of Radio Training Programs and other types of outreach for both Agency Radio Officers and for all Departmental radio personnel.
- Coordinating with others in promoting adherence to sound radio practices and procedures within and beyond the Executive Branch.
- Serving as central point of information on radio matters.

The Radio Sub-Domain description provided in Table 42 will not be populated until OIMT and the State of Hawai`i provide a Governance oversight for this sub-domain, which has been started (refer to the additional information and url below this table), but is incomplete. In addition the Radio Sub-

Domain primarily has a Law Enforcement component that links the State, Counties, DOD, and Homeland Security that will remain confidential and will not be part of any published information.

Table 42: Radio Sub-Domain Description

Infrastructure Hosting, Cloud and Data Center Sub-Domain	Sunset Products / Standards	Current Supported Products / Standards	Preferred Products / Standards	Emerging Trends
RF/Microwave Diagnostics				
RF/Microwave Monitor				
RF/Microwave Reporting				
Spectrum Testing				
Spectrum Management Platform				
RF Facilities Structure – exterior				
Data Facilities Structure – interior				
Mechanical Systems – Inside RF facility				
Mechanical Systems – Fire Suppression				
Mechanical Systems – backup power generation				

Radio Sub-Domain Addendum Information

http://idea.hawaii.gov/userimages/accounts/90/907159/panel_upload_18993/SupplementalAddendumRadioSystemsPlan2.0.pdf

ETA TRANSITION AND SEQUENCING PLANNING SUMMARY FOR THE NETWORK DOMAIN

The Network T&S Planning Summary is inextricably tied to the Infrastructure Domain’s activities and initiatives. All the elements of Network Domain planning related to the Data Center, O&M resources, and inter-island communications leases are discussed in the Infrastructure Domain.

Transition and sequencing initiatives and activities for the Network Domain are based on industry best practices and validated designs, includes input from the Network Working Group, and the creation of quarterly performance milestones for IPv6 adoption.



DESIGN AND IMPLEMENT ONENET

This initiative occurs in four phases. Estimated ring separation cost is Pending Review for Oahu, Pending Review per island of Hawaii, Maui, and Kauai for a total of Pending Review total.

Phase I (Years 1-2) –

- Negotiate with Oceanic (Cable Franchise Agreement or independent agreement).
 - At least two route diverse dark fiber connections between the two main Oahu Data Centers
 - Establish separate State rings on each of the major islands of Oahu, Kauai, Maui, and Hawai`i . The design is based on at least one high availability ring per island (2 on Oahu) with subtending rings and spurs connected to sites on the main ring.
 - Additional high speed interisland connectivity (Oceanic currently provides a shared 10Gbps link between the islands for the State, DOE, and UH. Terminations of these connections will be at the designated island’s data center and telecom center.

- As part of standard franchise agreement with Oceanic, request connectivity to interim, private data centers.

- Establish pricing with other carrier between interim data centers on Oahu for network diversity.
- Establish SLA, chargeback process
- Establish basic NOC/SOC 24x7 staffing

Phase II (Years 3-4)

- Establish full NOC/SOC support with 24x7 onsite support.
- Implement Oahu high availability backbone and connectivity to interim data centers.

Phase III (Years 5-6)

- Implement high availability backbone and data center connectivity (1 island)

Phase IV (Years 7-8)

- Implement high availability backbone and data center connectivity (1 island)

Phase V (Years 9-10)

- Implement high availability backbone and data center connectivity (1 island)

PROVIDE VIDEO SUPPORT

Video conferencing includes support for facility specific locations (Video Conference Centers), desktops, and mobile devices. Self-scheduling allows users to schedule conferences without the need for centralized oversight. Deployment of multicast systems allows for organizational wide announcements, training, etc. This initiative includes four phases with an estimated cost of Pending Review.

Phase I (Year 1-2)

- Upgrade existing video conferencing centers that will serve as enterprise models for room conferencing.
- Develop cost recovery plans and acquire automated system for cost recovery

Phase II (Years 3-4)

- Upgrade/acquire additional bridging capabilities to support larger user base including desktops, notebooks, and mobile devices i.e. tablets and smartphones.
- Deployment user based scheduling.

Phase III (Years 5-6)

- Deployment of VoIP and video integration (answer calls via video/voice or simply voice).

Phase IV (Years 7-8)

- Implementation of multicast capabilities on the network
- Acquisition of multicast video equipment

Phase V (Years 9-10)

- Technology refresh

CREATE IP ADDRESSING – REMOVAL OF NETWORK ADDRESS TRANSLATION FROM DEPARTMENTS

This initiative occurs in four phases with an estimated cost of Pending Review

Phase I (Year 1-2)

- Departments will develop their respective transition plans if they are not currently using their NGN assigned addresses.
- ICSD/OIMT to develop removal of NAT Transition Plan.
 - Determine order that departments will migrate off of NAT.
 - Develop policy to determine what traffic is not allowed in and out of departments for security purposes. This allows for transparency and safeguards in the event there is a security event/outbreak at a respective department location and there needs to be the ability to segment quarantine a portion of the network to prevent further outbreak.

Phase II (Years 3-4)

- Migration to NGN assigned addresses by departments not currently in compliance.
- Implementation of NAT Transition Plan for departments in compliance.

Phase III (Years 5-6)

- Implementation of NAT Transition Plan for departments who were required to achieve compliance in Phase II.

CREATE IP ADDRESSING – TRANSITION FROM IPV4 TO IPV6 INITIATIVE

This initiative occurs in five phases with an estimated cost of Pending Review. The key activities include:

- Replacing and/or upgrading equipment and software to be IPv6 ready.
- Training for staff on IPv6.
- Designing the network to allow for renumbering.
- ARIN recommends upstream providers enter into contractual arrangements with their customers stipulating that the address space may have to be returned, requiring all end-sites to be renumbered.
- Obtaining IPv6 address space.
- Replacing/upgrading/procuring OS, software, network management tools, routers, firewalls, etc. to be IPv6 compliant.
- Training for IT staff on IPv6.

Phase I (Year 1-2):

- Determine cost of IPv6 Address Space, Training, and Network Equipment upgrades.
- Obtain IPv6 Address Space.
- Training for staff on IPv6.
- Establish test network/lab for IPv6.

Phase II (Years 3-4):

- Develop IPv4 to IPv6 Transition Plan.
 - Determine how IPv6 addresses will be distributed.
 - Develop order as to which departments will migrate off of IPv4.

Phase III (Years 5-6):

- Replacing and/or upgrading network equipment to be IPv6 ready.
- Procuring IPv6 Management Tools not used in the IPv4 arena.
- Replacing and/or upgrading of operating systems, software, and applications to be IPv6 compliant.

Phase IV (Years 7-8):

- Assignment of IPv6 addresses for existing hosts.
- Assignment of IPv4 and IPv6 addresses to new hosts.

Phase V (Years 9-10):

- Implementation of IPv4 to IPv6 Transition Plan.

DEFINE AND IMPLEMENT COMPREHENSIVE NETWORK SECURITY

*Proper network security controls are required to protect the availability of the OneNet. Network security controls allow for the ability to:

- Segment/quarantine portions of the network in the event there is a security outbreak at a Department attached to the OneNet.
- Provide protection from external and internal threats (Firewall, IDS, IPS, Secure Web Gateways, DLP).
- Perform health checks (e.g., Virus Signatures, Patching Levels, etc.) of devices attempting to connect to OneNet internally or externally.
- Support SSL VPN services.
- Support Role Based Access Control.
- Forensic/Data Retention of network events (logs) at all layers (CDA) for a minimum of two weeks.
- Provide flow based security incident and event monitoring.
- Provide application rate shaping/ flow control.

This initiative occurs in three phases. Estimated is Pending Review independent of the infrastructure costs.

Phase I (Years 1-2):

- Evaluation of existing network security tools (e.g., IPS, Next Generation Firewalls, UTM, NAC, etc.) to determine their role in OneNet.
- Begin the implementation/upgrading of network security tools identified in the evaluation.
 - Guidance/Requirements/Recommendations will be needed from the Information Assurance Branch (IAB).

Phase II (Years 3-4):

- Complete the implementation/upgrading of network security tools.
- Align network security tools with the sequencing plan of the removal Network Address Translation for Departments.

Phase III (Years 5-6):

- Complete the tasks involved with the sequencing plan of the removal of Network Address Translation for Departments.

STAFFING NETWORK SECURITY ORGANIZATION

The ability to support the vision of OneNet is critically dependent upon the ability to recruit, hire, staff and train employees on an ongoing basis. Staffing levels must be sufficient to support Network Operation Centers (NOC) on a 24x7x365 basis. The identification and/or hiring and training additional network security occurs during the next 10 years and the estimated cost is Pending Review.

Phase I (Years 1-2):

- Development of OneNet Support Staff organizational structure:
 - * Oahu
 - Engineering & Design Section (5)
 - Network Security Section (5)
 - Routing & Switching Section (5)
 - Transport Section (5)
 - Data Center (5)
 - Technicians (5)
 - At least two staff employees will be on site during evening and early morning hours.

- Neighbor Islands:
 - Big Island (5)
 - Maui (5) – Supports Molokai and Lanai
 - Kauai (5)

- Development of position descriptions along with:
 - Recruitment above the minimum.
 - Shortage Differential
 - Merit pay with opportunity for advancement.
- Begin the process of filling positions for the OneNet Network Support Staff.
- Provide training for staff positions that are filled. This will include travel expenses for training conducted outside the State of Hawai'i .

Phase II (Years 3-4):

- Continue the process of filling positions for the OneNet Support Staff.
- Provide training for staff positions that are filled. This will include travel expenses for training conducted outside the State of Hawai'i .

Phase III (Years 5-6):

- Continue the process of filling positions for the OneNet Support Staff.
- Provide training for staff positions that are filled and continuous training for existing staff. This will include travel expenses for training conducted outside the State of Hawai'i .

Phase IV (Years 7-8):

- Continue the process of filling positions for the OneNet Network Support Staff.

IMPLEMENT NETWORK LIFE CYCLE METHODOLOGY

To properly maintain OneNet, implementation of a network life cycle methodology and sustainment mechanism is required. This also allows OneNet to become self-sufficient due to the implementation of a Self-Sustainment Model where charge backs are issued to Departments. The funds received will allow for equipment maintenance, upgrades, and refreshes to occur on a scheduled basis. Determination of cost items will be based on current industry standards. This implementation occurs in five phases and will cost approximately Pending Review.

Phase I (Years 1-2):

- Development of Self Sustainment Model (Charge Backs - Model similar to that of private carrier charges)
 - Recovery of NRC, ICB and special builds costs.
- * Bandwidth with enforcement through rate-limiting
 - Drops/Locations
 - Qos/Cos
 - MRC to be a percentage discount from average cost of private carriers.

Phase II (Years 3-4):

- Deployment of network support equipment/structure to support the Self Sustainment Model.

Phase III (Years 5-6):

- Begin the implementation of Self Sustainment Model.
 - Perform analysis of Self Sustainment Model and determine whether charge backs fair, consistent, and adequate
- Refresh of equipment older than 5 years.

Phase IV (Years 7-8):

- Complete implementation of Self Sustainment Model.
- Continue analysis of Self Sustainment Model.
- Implement necessary changes for Self Sustainment Model.
- Refresh of equipment older than 5 years.

Phase V (Years 9-10):

- Continue analysis of Self Sustainment Model.
- Implement necessary changes for Self Sustainment Model.
- Refresh of equipment older than 5 years.

Figure 42 represents the roadmap to achieve the future state vision for the Network Domain.

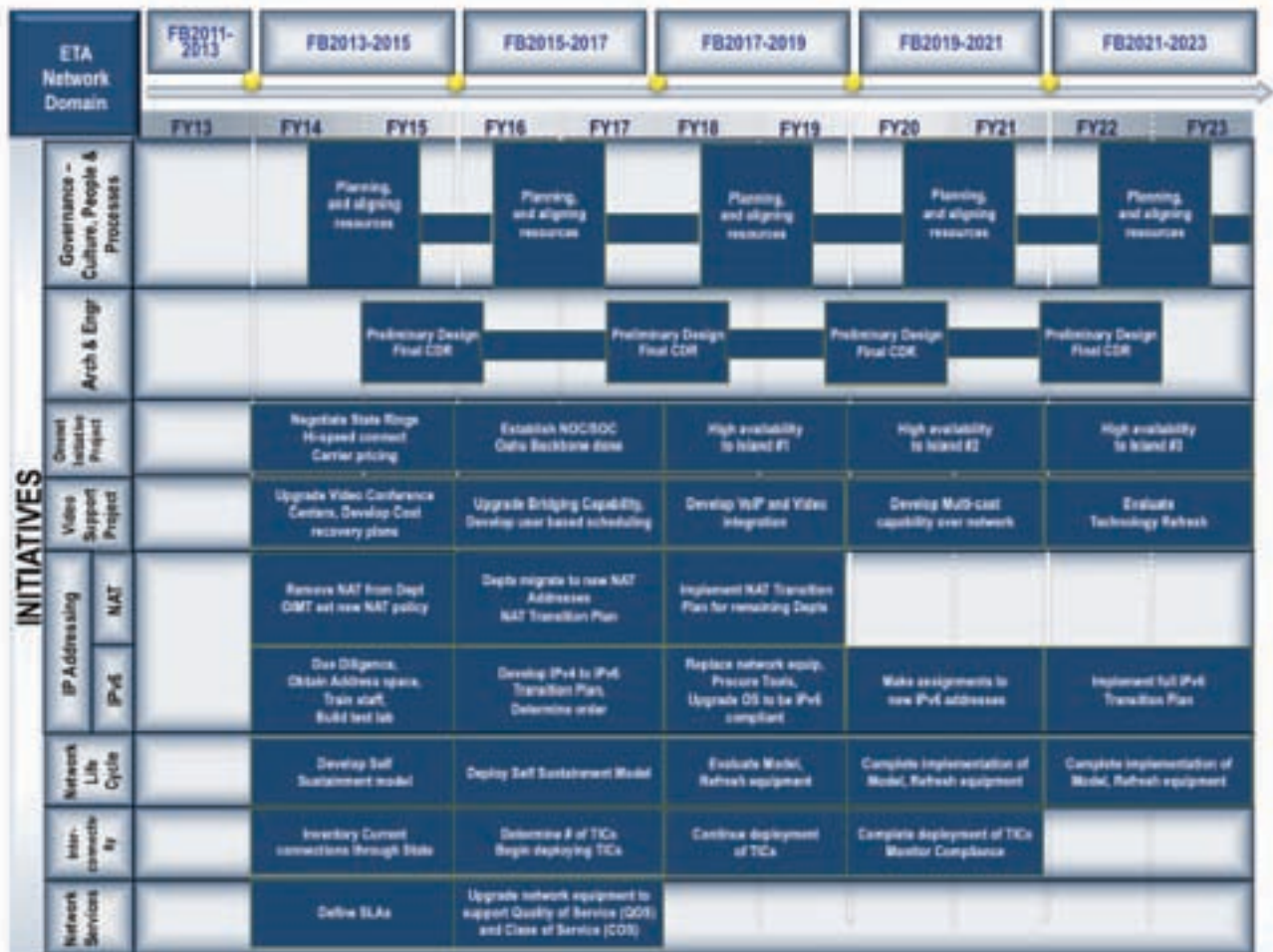


Figure 42: Roadmap for Achieving the Future State Network Domain

7.2.3.3 END USER COMPUTING DOMAIN

The EUC is an agent (human or machine) which consumes services provided by software packages or programs. Generally, end users are dependent on this technology to complete daily work tasks.

CURRENT STATE SWOT FOR THE END USER COMPUTING DOMAIN

The State currently has specific centers of innovation (Hawai'i Public Library System) in providing for end user pilots, bring your own device (BYOD) solutions, and collaborative practices. In its entirety, the State lacks end user computing common solutions and standards. This results in a general lack of coordination, a centralized knowledgebase, compliance to best practices in a comprehensive fashion, and a robust, universal support model that is 24x7x365. This EA document addresses several EUC areas that are in other sections, such as Message and Collaboration Services and End-User Development. Underlying system capacity knowledge is not being tracked and not readily available. In addition, in general the demand for network service provision overwhelms the current capacity and resource base.

FUTURE STATE VISION FOR THE END USER COMPUTING DOMAIN

Incorporation of End-user perspectives is quite complex. This is primarily due to the inability to have a clear boundary for what the term "End-user perspective" represents. Consequently, key concepts such as End-User Computing, End-User Development, and Usability all are related concepts which fall within the boundary of 'End-user perspective'. End-User Computing has been defined as "direct interaction with application software by managerial, professional, and operating level personnel in user departments" (Torkzadeh and Lee, 2003), while other have noted that End-user computing "means that the user of the results of the computing also creates the software specifications necessary to effect the computing itself".

End-User Development has been defined as a set of methods, techniques, and tools that allow users of software systems, who are acting as non-professional software developers, at some point to create, modify or extend a software artefact (Lieberman, Paternò, and Wulf, 2006). The academicians try to define what End-User Computing is while the worldwide hosted virtual desktop (HVD) market will accelerate through 2013 to reach 49 million units, up from more than 500,000 units in 2009, according to Gartner. Worldwide HVD revenue will grow from about Pending Review to Pending Review in 2009, which is less than 1 percent of the worldwide professional PC market, to Pending Review in 2013, which will be equal to more than 40 percent of the worldwide professional PC market.

"PC vendors must prepare for the growth in demand for this client computing architecture by adjusting sales strategies and compensation models or they risk losing expenditure share with enterprise customers," said Annette Jump, research director at Gartner.

Figure 43 depicts how various operating systems, various releases, and various vendors' software can be standardized and consolidated to Virtual Desktop Infrastructure (VDI). VDI extends server virtualization to desktop operating systems that are hosted on virtual machines (VMs) running in a secure datacenter. Users' access to virtual desktops is through open Internet based protocols.



Figure 43: Virtual Desktop Migration

A VMWARE BLOG FROM 6/8/2012 SAYS:

"...the consumerization of IT is a force in IT that can't be stopped. It can be managed, but not stopped (nor should it). Increasingly employees are choosing the devices and the services they want to use to get their jobs done. The people you really want to work for you no longer want to be forced to work on dull corporate issued notebooks or mobile devices. They want to use the same phones and tablets at work as they and their friends do at home.

Let's face it, when it comes to devices - they're no longer viewed as just something to get work done with. They've grown to become a statement, or extension of oneself, or self-image. That is: they're now viewed by many as fashion. Who wants to be seen with a stodgy black notebook when they can have the latest flashy netbook or tablet?

However, the more important trend, at least when it comes to security and regulatory compliance - is happening under the surface of the device. It is how employees are choosing the cloud-based applications they want to use. These impulse application selections means, too often, that proprietary data or data that should be protected actually ends up scattered through many online services and accessed on devices the enterprise doesn't manage."

Figure 44 provides a high level graphic depicting the capability for VDI to protect proprietary data from being scattered through many online services and accessed on devices the State does not manage.

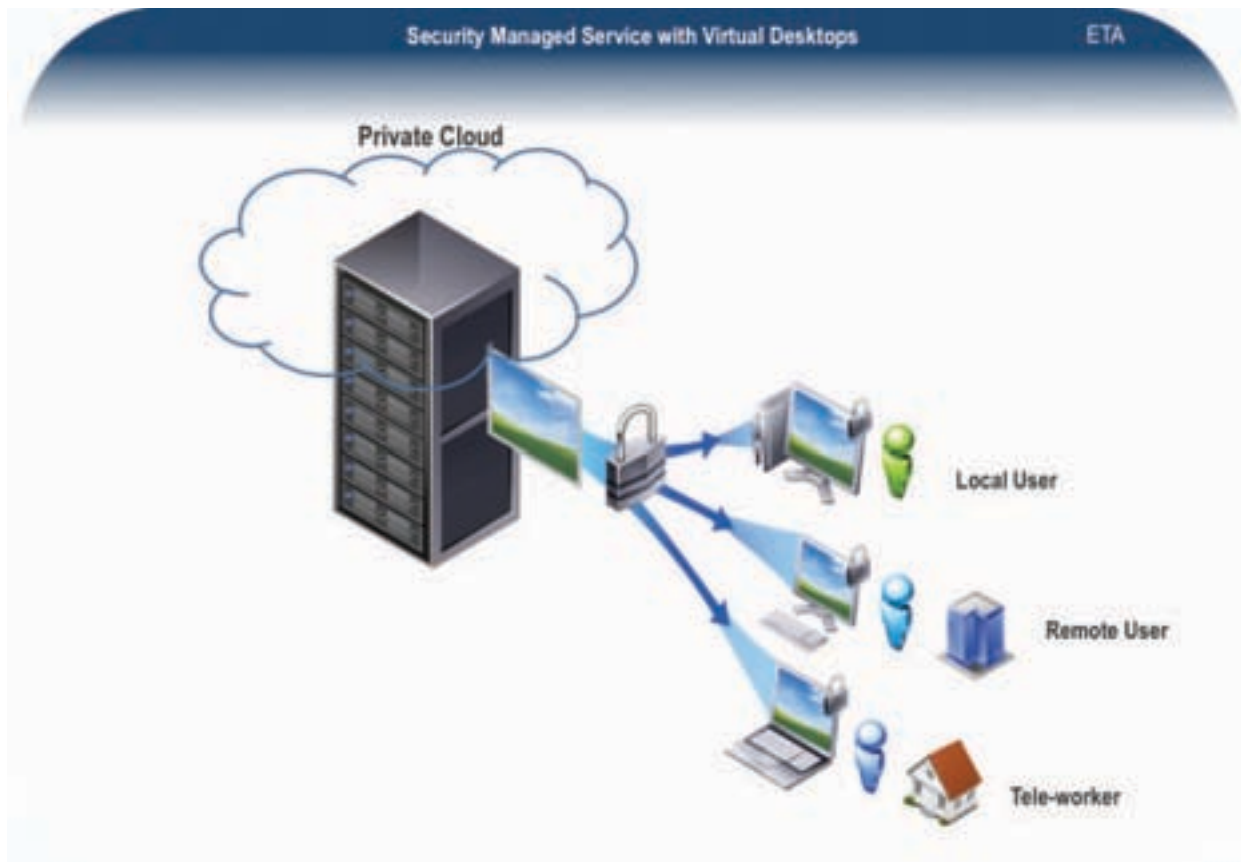


Figure 44: Secure Managed Services with Virtual Desktop

Guiding Principles for End User Computing Domain

1. Technology is viewed as an enabler of productivity; all computing devices support mobile applications and work seamlessly throughout the technical environment.
2. End user devices are kept current with security and Operating System updates and patches.
3. "End-User Empowerment, enhancing traditional user service interaction by facilitating the selection, creation, composition, customization, reuse and sharing of applications in a personalized operating environment.
4. "Seamless Context-Aware User-Service Interaction. New-generation service front-ends should have the capability to detect, represent, manipulate, and use contextual information to adapt seamlessly to each situation, supporting human users in a more effective, personalized and consistent way. Novel engineering tools and methods should be devised in order to support context-aware service front-ends.
5. "End-User Knowledge Exploitation. This principle aims to exploit users' domain knowledge and collective intelligence to improve service front-ends. End users' knowledge can be used to tag resources using

light semantics, assist while interacting with services, enrich contextual information (e.g. by means of automatic user profiling) and infer new candidate processes to be later automated (on the back-end).

6. "Universal Collaborative Business Ecosystems. Enterprise systems should incorporate advanced user-centric, context-aware front-ends to enable their employees and other stakeholders to exploit and share their extensive domain expertise, and their thorough business knowledge. Employees, customers, developers and providers will collaborate to create and improve enterprise applications, sharing, reusing, changing and combining existing context-aware components."*

***End-User Development Success Factors and their Application to Composite Web Development Environments"*

*David Lizcano, Fernando Alonso, Javier Soriano and Genoveva Lopez
ICONS 2011: The Sixth International Conference on Systems*

DESKTOP, LAPTOP, AND MOBILE SUB-DOMAIN

This sub-domain requires standardization of computing hardware to simplify maintenance and offer economies of scale for purchasing hardware. Table 43 describes this sub-domain.

Table 43: Desktop, Laptop, and Mobile Sub-Domain Description

EUC Desktop, Laptop and Mobile Sub-Domain	Sunset Products / Standards	Current Supported Products/ Standards	Preferred Products / Standards	Emerging Trends
Desktop/Workstation			64 bit x86 architecture with multicore CP	64 bit architecture with multi core CPU Thin or Ultra-Thin clients with virtual desktop
Laptop		Need to be at a specification level and not call out vendors on this. Meet need multiple levels based on a short list of types of roles: Entry-level, User, Super-User.	(Example:) WinTel Desktop, 8GB RAM minimum, Windows 7 Professional	Ultrabook with local SSD and cloud storage
Wireless/PDA	RIM Blackberry	RIM Blackberry iOS, Android 4.0, Windows Mobile 8	Latest stable release of iOS, Android, or Windows Mobile	Multi-core processor smartphones with high res touch displays
Tablet		Apple, Android	Tablet with Wi-Fi + 4G-LTE	Tablet computing with cloud storage

USER PRODUCTIVITY SOFTWARE SUB-DOMAIN

This sub-domain includes core applications installed on the majority of computing devices to enable employees to perform work tasks and communicate electronically. This sub-domain is described in Table 44.

Table 44: User Productivity Software Sub-Domain Description

EUC Desktop, Laptop and Mobile Sub-Domain	Sunset Products / Standards	Current Supported Products/ Standards	Preferred Products / Standards	Emerging Trends
Desktop Operating System	Windows 2000, Windows NT, Windows XP SP3	Windows 7, Mac OSX 10.6 or above	64-bit standard; virtual desktops	Windows 8 up Virtualized Desktop Infrastructure, Cloud based OS
Productivity Tools	MS Office 2003, MS Office 2007	MS Office 2010, Adobe Reader X	Virtual productivity tools	MS Office 2012; Hosted solutions Cloud based productivity applications

USER PRESENTATION SUB-DOMAIN

This sub-domain identifies applications and tools used to provide multi-media content to the end users. Table 45 provides additional detail about the User Presentation Sub-Domain.

Table 45: User Presentation Sub-Domain Description

EUC Desktop, Laptop and Mobile Sub-Domain	Sunset Products / Standards	Current Supported Products/ Standards	Preferred Products / Standards	Emerging Trends
Web Browser	IE 6,7	IE 9, Firefox 9, Safari 5	W3C Consortium, http://www.w3.org	IE 10, Firefox 14+, Google Chrome, Opera, HTML 5 compliant WebKit2 based mobile browsers
Video		QuickTime Ver7 (Win) and X (Mac), MPEG-4	Motion JPEG2000 (*.mj2) AVI (*.avi) (uncompressed) Motion JPEG (*.avi, *.mov)	CORBA - Common Object Request Broker Architecture is an architecture and specification for creating, distributing, and managing distributed program objects in a network.
Audio		MP3	AIFF(uncompressed) (*.aif, *.aiff) WAVE (LPCM only) (*.wav)	AIFF(uncompressed) (*.aif, *.aiff) WAVE (LPCM only) (*.wav)
Picture/Image		JPEG, GIF 89a, PNG	JPEG, GIF 89a, PNG	Hardware design of multiple engine compression and decompression

PERIPHERALS SUB-DOMAIN

The Peripheral Sub-Domain includes external devices that provide input and output for computers. Table 46 describes this sub-domain.

Table 46: Peripherals Sub-Domain Description

EUC Desktop, Laptop and Mobile Sub-Domain	Sunset Products / Standards	Current Supported Products / Standards	Preferred Products / Standards	Emerging Trends
Printer	Impact Printers	Laser, Inject Printer	Laser, Inject Printer; ISO/IEC 24711 ISO/IEC 19752	Multi-function devices which incorporate print, copy, fax, scan, email capabilities.
Personal Printer		Laser, Inkjet Printer	Color Laser, Inkjet; ISO/IEC 24711 ISO/IEC 19752	Group printing to Multi-Function device unless business justification is satisfied.
Monitor	CRT	LED, LCD	LED, LCD; ENERGY STAR program requirements for computer monitors	OLED (Organic Light-Emitting Diode) display, QD-LED (Quantum Dot) display
External Hard Drive	Unencrypted attached storage		Encrypted devices; 100 Gigabit Ethernet (100GE) and 40GE capabilities to the Cloud	External media (USB drive, SSD, etc.) with full encryption; intelligent infrastructures ready to support cloud-based environments

ETA TRANSITION AND SEQUENCING PLAN SUMMARY FOR THE END USER COMPUTING DOMAIN

Transition and sequencing is based upon a thorough assessment of the current end user posture, including looking at some of the Centers of Innovation within the State. This transition and sequencing is dependent on decisions to create Virtual Desktops and Network processes within the larger initiative.

The identified initiatives have been created in participation with the End User Planning Working Group to provide a road map and project phasing to address a comprehensive integrated capability.



CREATE VIRTUAL DESKTOP INFRASTRUCTURE

Creating Virtual Desktop Infrastructure (VDI) extends server virtualization to desktop operating systems that are hosted on virtual machines (VMs) running in a secure datacenter. Users' access to virtual desktops is through open Internet

based protocols. Since the desktop VM is maintained in a secure datacenter, there is better containment of State information and more efficient usage of centrally managed, pooled and shared IT resources. Within the VDI infrastructure, desktops can be persisted or be taken offline; therefore, users have the flexibility to customize and access with their desktops from multiple locations.

With more than 41,000 employees in state offices, the State of Hawai'i faces significant challenges from threats that may disrupt efficient operations. Vital to Hawai'i is the dependence on IT services needed to deliver adaptive and secure solutions in the future.

To provide continual growing support for mobile workforces and to diminish disruptions in the workplace caused by natural disasters, pandemics, and security threats, a VDI pilot is included as part of the initiative. This pilot will enable secure and reliable web-based access to virtualized State desktops. Through VDI, desktops and data are centrally managed and contained in a secure datacenter; therefore, safeguarding information and preventing accidental data leakage to unmanaged client physical devices. The EA strategy aligns with industry trends where the rigid enterprise perimeter starts to dissolve and the need to provide a business-ready adaptive infrastructure that supports the endpoint demands between employees, customers, partners, mobile workers and outsourced functions and services is required. The pilot steps are:

- Start using Virtual Desktops as a complement to existing desktop environment, complementary use cases might be desktop users who want to work from home, contractors or suppliers who need access, and building disaster tolerance (fire, flood etc.). Keep this environment as inexpensive and simple as possible. Manage it like a physical environment. A few hundred concurrent users of a product like VDI in a Box are perfect for this. Continue to use roaming profiles. Provide just a core set of common applications installed in the image.
- Start to stream top 10-20% of applications into this environment, making it increasingly useful, while still keeping the environment simple and clean. Keep using roaming profiles or a simple profile management solution that just does a like for like replacement. Once the top 20% of applications are streaming approximately 50% of the users' core needs will be met.
- Monitor event logs for application crashes and hangs to ensure performance and consider making these streamed applications the strategic delivery method for all users and optionally consider piloting virtual desktops for mainstream use, with thin clients. Keep virtualizing remaining applications in batches and 30% of applications are virtualized approximately 70% of users' needs will be fulfilled. Virtualizing the remainder of the applications is harder because these, these are used by less than 10% of the users. [In Hawai'i, this will likely include many of the applications that will be absorbed into ERP].
- Finally, mature the rest of the desktop environment by moving get master data off the physical PCs and onto the network, ensure user entitlements are all defined in AD, begin using a more sophisticated solution for user state virtualization (not roaming profiles). At this point, the State will have one way to deliver applications, data, policy, configuration, user state and applications to virtual and physical desktops."

The VDI test pilot initiative targets a number of users for the initial capability scoped at 1,500 users serving a maximum of 350 users concurrently. This requires the purchase of new server infrastructure and new licenses, as well as training and security enhancements.

The summary required steps include:

- Service Design
- Service transition
 - Test Readiness Review
 - Testing
 - Test Completion Review
 - Production Readiness Review
 - Operational Readiness Review
- Service Operations
- Organization Change Management/ Communications/Training
 - OCM requirements and Analysis
 - Communications
 - Training

⁷VDI Pilot Steps from June 12, 2012 Blog Posting following Apple Working Group Meeting <http://www.whyvdi.com/>

CONDUCT A PILOT TEST OF VDI

The Pilot Test addresses the following commonly required aspects of an enterprise class solution: Standardization, Repeatability, Scalability, Availability, Security, and Integration. The client access device layer for the Pilot Test is comprised of the hardware and software components needed to deliver a PC-like experience. Estimated cost of the Pilot Test is Pending Review.

DEFINE AND IMPLEMENT NEXT STEPS VDI IMPLEMENTATION

This initiative supports the EA and uses common components and a standardized design to reduce the overall cost of implementation and management. The client access device layer is comprised of the hardware and software components needed to deliver a PC-like experience. The process for choosing the appropriate client device varies from deployment to deployment; mixed client environments are not uncommon. In most cases, users are segmented based on their needs and requirements during the planning and design phases, and business requirements and goals are also taken into consideration and mapped to the needs of the user segments. For example, a Department might have personal computers (PC) that are on a staggered depreciation schedule. Depreciated assets can be replaced by thin client devices right away, but assets that have not fully depreciated are often converted into unmanaged end-points, typically by converting them to PXE-booted clients using a Linux-based solution. An alternative to be considered includes the "lock down" of the currently installed Windows OS and then repurposing. Either approach can offer the flexibility to gain the highest return on PC hardware investment. Estimated costs for this planning activity are Pending Review.

Figure 45 represents the roadmap for achieving the future state for end users computing.

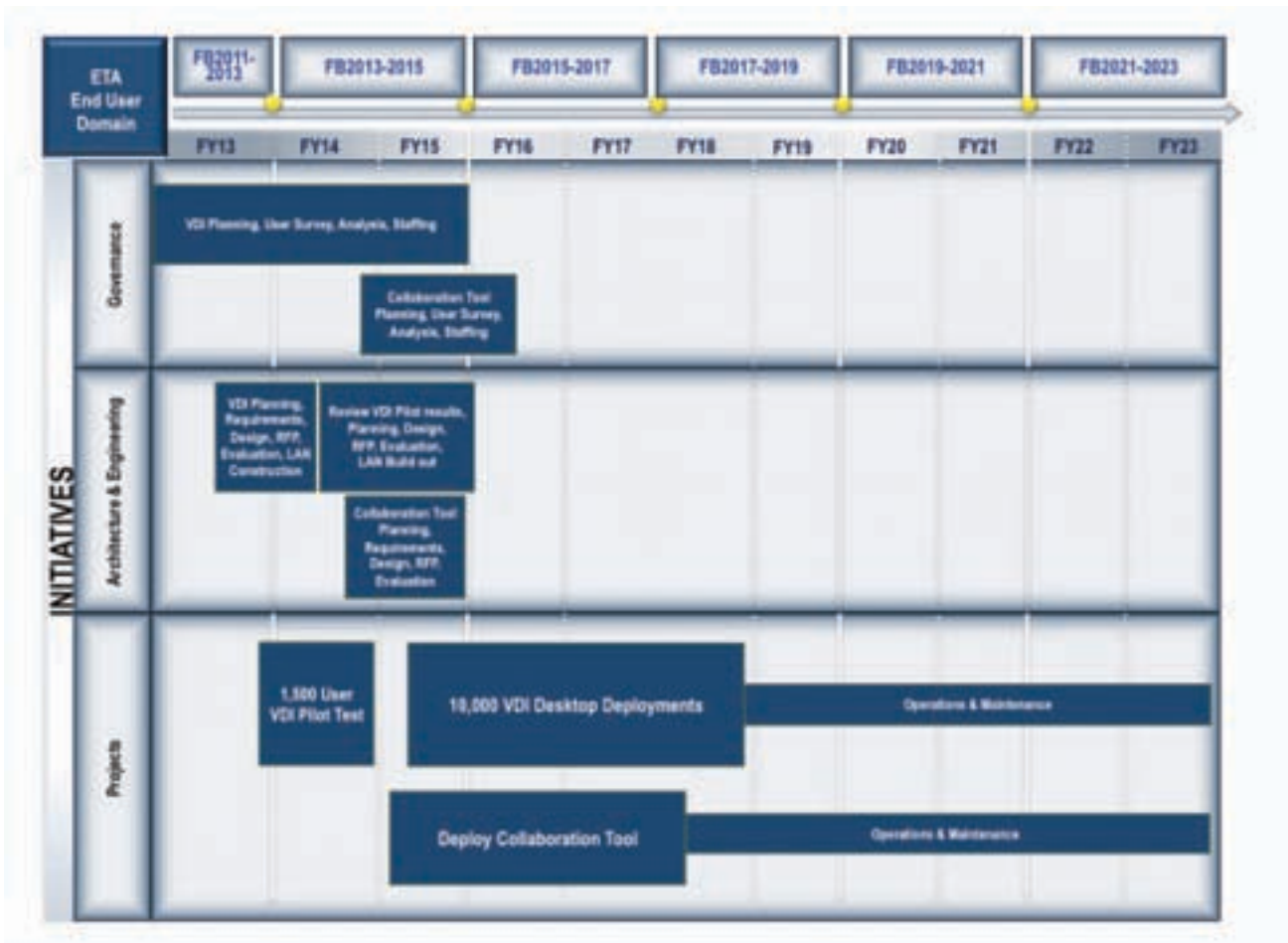


Figure 45: Roadmap for Achieving the Future State of the End User Computing

7.2.3.4 UNIFIED COMMUNICATIONS DOMAIN

According to the International Engineering Consortium, Unified Communications (UC) is an industry term used to describe all forms of call and multimedia/cross-media message-management functions controlled by an individual user for both business and social purposes. This includes any enterprise informational or transactional application process that emulates a human user and uses a single, content-independent personal messaging channel (mailbox) for contact access.

Unified Communications is orchestrated communication and collaboration across locations, time, and medium to accelerate business results. Unified Communications is achieved through the convergence of real-time, near-real-time, and non-real-time business communication applications. These applications include: calling, conferencing, messaging, contacts,

calendar, collaboration, and rich presence with voice, video, text, and visual elements. It is a State of Hawai'i goal to access these capabilities using multiple access methods including voice, data, and speech access through telephones, PCs, and mobile devices.

Components of collaboration/communication technology include:

- **Electronic Mail (Email)** - Email (Electronic mail) is the exchange of computer generated and stored messages by telecommunication. An email can be created manually via messaging applications or dynamically programmatically such as automated response systems.
- **Workflow** - At its simplest is the movement of documents and/or tasks through a work process. More specifically, workflow is the operational aspect of a work procedure: how tasks are structured, who performs them, what their relative order is, how they

are synchronized, how information flows to support the tasks, and how tasks are being tracked. As the dimension of time is considered in Workflow, Workflow considers "throughput" as a distinct measure. Workflow problems can be modeled and analyzed using graph-based formalisms like Petri nets. While the concept of workflow is not specific to information technology, support for workflow is an integral part of document management and imaging software.

- **Facsimile (Fax)** - A fax is the digitized image of text and/or pictures, represented as a series of dots (bit map). Faxes are sent and received through telecommunication channels such as telephone or Internet.

- Fax Server - A fax server is a set of software running on a server computer which is equipped with one or more fax capable modems attached to telephone lines. Its function is to accept documents from users, convert them into faxes, and transmit them, as well as to receive fax calls and either store the incoming documents or pass them on to users. Users may communicate with the server in several ways, through either a local network or the internet. In a big State department with heavy fax traffic, the computer hosting the fax server may be dedicated to that function, in which case the computer itself may also be known as a fax server.

* For outgoing faxes, several methods are available to the user:

- An e-mail message (with optional attachments) can be sent to a special e-mail address; the fax server monitoring that address converts all such messages into fax format and transmits them.
- The user can tell his computer to “print” a document using a “virtual printer” which, instead of producing a paper printout, sends the document to the fax server, which then transmits it. A web interface can be used, allowing files to be uploaded, and transmitted to the fax server for faxing.
- Special client software may be used.
- For incoming faxes, several user interfaces may be available:
 - The user may be sent an e-mail message for each fax received, with the pages included as attachments, typically in either TIFF or PDF format.
 - Incoming faxes may be stored in a dedicated file directory, which the user can monitor.
 - A website may allow users to login and check for received faxes.
 - Special client software may be used.
- Kiosk - A kiosk is a small physical structure (often including a computer and a display screen) that displays information for people walking by. Kiosks are common in public buildings. Kiosks are also used at trade shows and professional conferences .”

CURRENT STATE SWOT FOR THE UNIFIED COMMUNICATIONS DOMAIN

Similar to other technology domains, the Unified Communications Domain is characterized by a lack of collaboration on standard solutions and technologies. Collaboration solutions within this domain have progressed significantly in recent industry history; at the same time that the State has experienced budget constraints and cuts. A few centers of excellence such as DOH and the Hawai`i Public Library System exist as models for lessons learned.

FUTURE STATE VISION FOR THE UNIFIED COMMUNICATIONS DOMAIN

The pattern listed below conveys how any State department may implement a Unified Communications capability using a unified solution. It also shows how specifically the interaction may occur between different department implementations.

- A single State Department Registry made up of a State Directory, LDAP (w/ Integrated Active Directory), and integration into email messaging to support collection of presence information, serves as the foundation for a Unified Communications capability.
 - Active Directory (LDAP) will provide authentication, directory, and other infrastructure security services.
 - State Directory will be enhanced to provide Rich Presence Information and other, as needed, user information.
 - Session Initiation Protocol (SIP) Proxy server will provide the VoIP integration to State Directory and LDAP services.
- State of Hawai`i users will leverage Unified Communications through End Point Devices that comply with State telecommunications and Security standards.
- Once authenticated, presence information will be passed back to allow other users to determine which communication mechanism(s) can be used (Voice, Video or Web Conferencing, Instant Messaging).

- The State of Hawai`i's use of VoIP will make it possible to communicate via telephone over an IP network using Session Initiation Protocol (SIP) instead of using traditional PBX telephony infrastructure.
- The State of Hawai`i Strategic direction requires network traffic to be effectively managed using Quality of Service (QoS) and other network optimization techniques.
- State departments will have the option of selecting from a single vendor solution for a fully integrated UC capability, or leverage a federated model. Federated model requires a connector to interconnect multiple UC solutions, with the ability to translate and offer presence information from the central repository to all end point and UC solutions.
- End Point Devices will require use of Open Standards (e.g., SIP). This will allow multiple vendors, though State of Hawai`i should have a preferred vendor list.

THE FOLLOWING BENEFITS ACCRUE FROM UNIFIED COMMUNICATIONS

- Centralization of a single State Department Registry will support collection of presence information to ensure easier integration with existing Hawai`i Login and integration of presence into Hawai`i's consolidated E-Mail and calendaring. This centralized capability will also ensure that authentication is done once and credentials are passed along to the appropriate UC capability.
- Hawai`i's use of VoIP will make it possible to communicate via telephone over an IP network using Session Initiation Protocol (SIP) instead of traditional PBX telephony infrastructure. Thus avoiding certain call charges and reducing overall calling costs.
- Implementing WAN-Optimization technologies such as QoS will ensure that traffic is managed appropriately so that video and voice traffic can be transferred as required at the State of Hawai`i.

- State departments will have the option of selecting from a single-vendor solution for a fully integrated UC capability, or leverage a federated model. Federated model requires a connector to interconnect multiple UC solutions, with ability to translate and offer presence information from the central repository to all end point and UC solutions.

The following summarizes the impact and implications of State of Hawai'i implementing UC as described in the pattern above. Implications include process changes to accommodate UC, security changes, policy changes, and / or other technology changes to ensure the success of UC in Hawai'i .

- Increased technology support demands
- Additional computing and storage capacity
- Additional network bandwidth needs
- More advanced network management
- Multiple UC solution interconnectivity support
- License management
- New models for usage chargeback and support
- Increased training needs for support personnel
 - Need for improved IT operation's monitoring
 - Need for improvements in metrics management

- * Additional need for end user training and information dissemination as UC capabilities and end-points are deployed

For the purposes of the ETA, focus is on the technical standards that support the policy and enforcement of UC.

Enhances services for citizens and increases efficiency by using technology to improve business processes.

- Provide world-class technology for citizen-centered, integrated, and secure services.
- Information sharing can be achieved when the information is designed to be discoverable, accessible, and reliable.
- Heighten customer-centric research and analysis.

Figure 46 provides a high level view of the current “stove piped” and “siloeed” communications systems using multiple products, various vendors, various releases, various versions, and inadequate capability versus the view on the right of Unified and Integrated Communications as the notional future state.

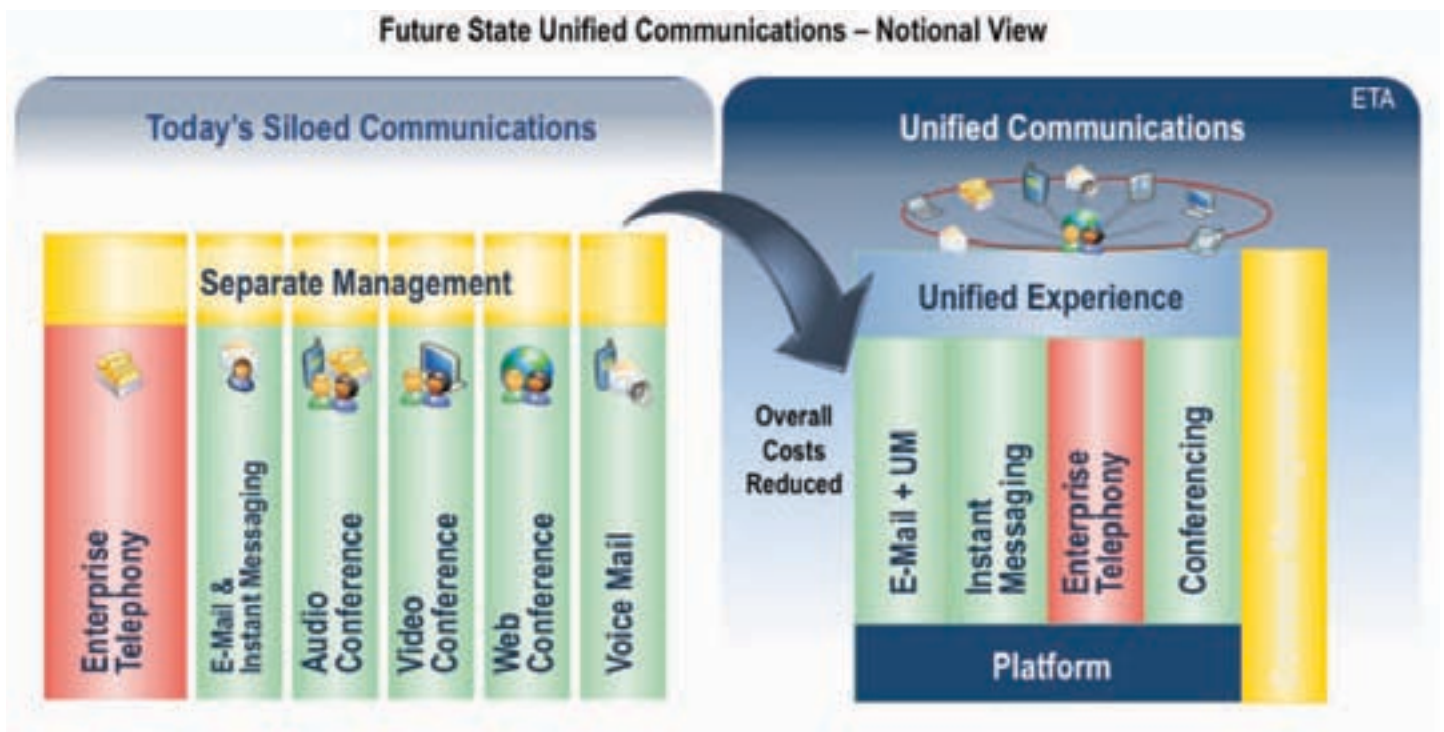


Figure 46: Notional View of the Future State of Communications

Figure 47 depicts the future state view of Collaboration-as-a-Service.

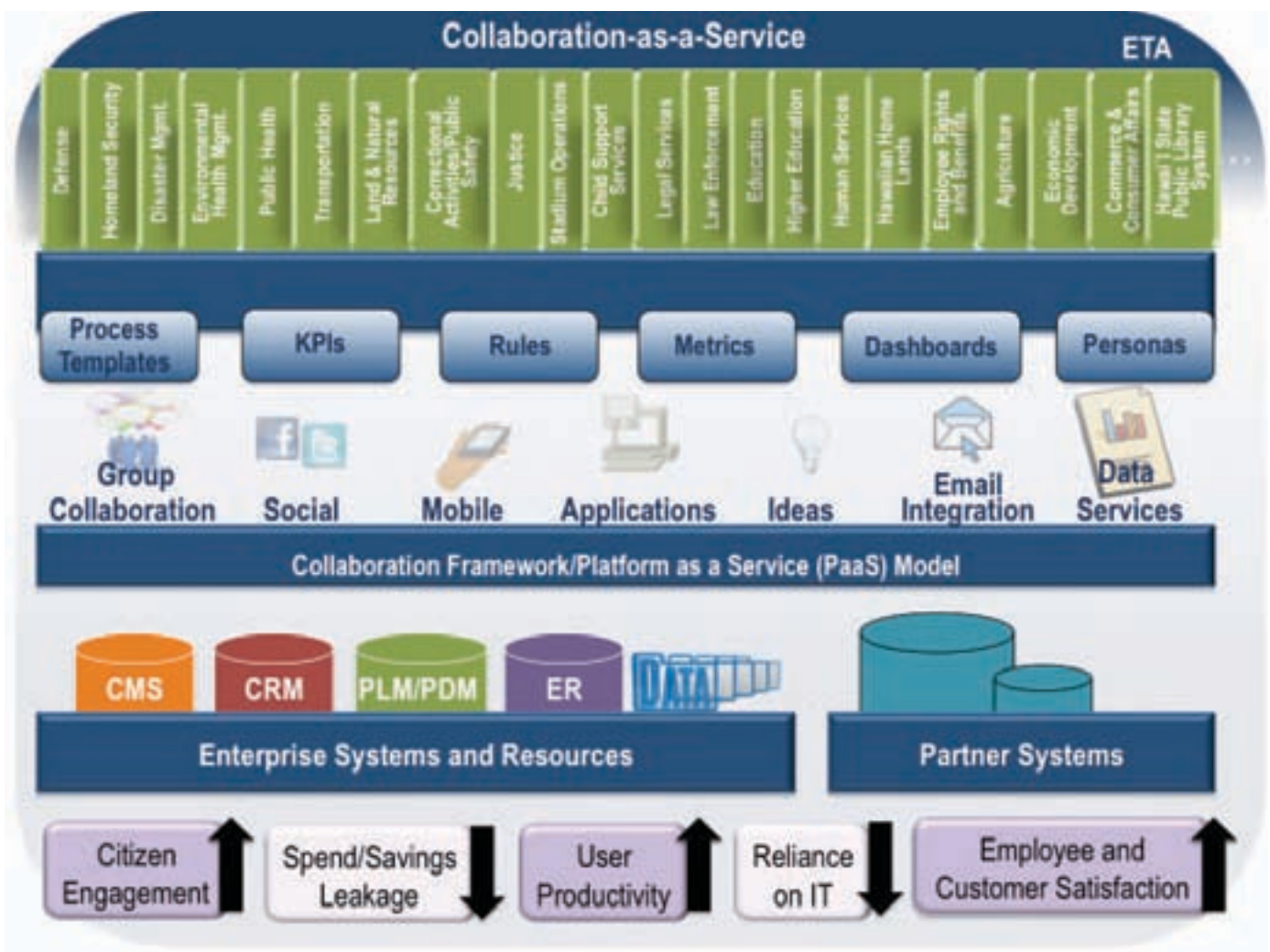


Figure 47: Collaboration-as-a-Service – An Essential Future State Element of ETA

Guiding Principles for Unified Communications Domain

1. Flexible methods of communication to one or many individuals with the State of Hawai'i government.
2. Capabilities to easily communicate with citizens in the manner in that are most productive for both the State and the citizen.

EMAIL AND COLLABORATION SUB-DOMAIN

This sub-domain, described in Table 47, includes all communication functions associated with email and collaboration tools.

Table 47: Email and Collaboration Sub-Domain Description

UC Email And Collaboration Sub-Domain	Sunset Products / Standards	Current Supported Products/ Standards	Preferred Products / Standards	Emerging Trends
Mail Servers		SMTP, POP, IMAP	IMAPS – IMAP over SSL	P-IMAPS or XMPP
Mail User Interface	Thick Client	Browser Based	Mail Application, Browser Based, Mobile Based	Unified inbox via sms, email, or chat where messages are sync'd and received through whatever medium or device that is convenient for the end user
Mail (Proprietary)		Lotus Notes, MS Exchange	Enterprise Messaging System with Global Address Book and Directory Services Integration	Cloud Email with large storage capacity (ex: Google Mail or Microsoft Exchange Online)
Mail (Hosted)			Gartner Magic Quadrant preferred vendor	Google, Microsoft, IBM Cloud based with storage and backup
Workflow			Pending Review	Workflow apps with cloud integration that can extend core ERP applications (ex: RunMyProcess)
Collaboration Environment		MS SharePoint 2010	Gartner Magic Quadrant preferred vendor	Cloud based content and document management system with integrated voice/video/IM/forums/wiki

Table 48: Voice Sub-Domain Description

UC Voice Sub-Domain	Sunset Products / Standards	Current Supported Products/ Standards	Preferred Products / Standards	Emerging Trends
VoIP	Individual department VoIP solutions with no state wide integration	Single vendor platform with integrated voice, data and directory services, G.711	Pending Review	VoIP PBX to mobile device integration, SVoIP – Secure Voice over IP, MoIP (Mobile communications over IP) apps
Landline carrier		Hawai'i Tel	Pending Review	Pending Review
Centrx Provider		Hawai'i Tel	Pending Review	Pending Review
Wireless Provider	Departmental purchase	Central procurement from dual provider with standard contract offering and pricing	Pending Review	Bring your own mobile (BYOM) with monthly employee allocation for service. Virtualization at mobile OS for separation of work/personal data

VIDEO SUB-DOMAIN

The video sub-domain (Table 49) includes communications tools and systems that support and transmit video.

Table 49: Video Sub-Domain Description

UC Video Sub-Domain	Sunset Products / Standards	Current Supported Products/ Standards	Preferred Products / Standards	Emerging Trends
Video teleconference room		<ul style="list-style-type: none"> • Standalone high bandwidth H.323/H.320 with G.711/722 • Multi-point capable 	Pending Review	<ul style="list-style-type: none"> • Tele-presence rooms with High Definition video capability • Centralized VTC monitoring and support
Video teleconference desktop		<ul style="list-style-type: none"> • IP based, multi-point capability • Open standards 	Pending Review	Video integration into desktop collaboration tools

BROADCAST MESSAGING SUB-DOMAIN

The broadcast messaging sub-domain includes the various communications mediums and tools often considered in today's environment as social media. Table 50 provides a description of the sub-domain.

Table 50: Broadcast Messaging Sub-Domain Description

UC Broadcast Messaging Sub-Domain	Sunset Products / Standards	Current Supported Products/ Standards	Preferred Products / Standards	Emerging Trends
Real Time Communication		MS Office Communicator (OCS)	Pending Review	Messaging integration with VoIP and video conferencing
External IM		Google IM	Pending Review	Enterprise level social tool that streams information proactively via a real-time news stream (Ex: Chatter by salesforce.com, Jive, or CiscoQuad)
Social Media		Twitter	Pending Review	Enterprise level social tool that sends information proactively via a real-time news stream (Ex: Chatter by salesforce.com, Jive, or CiscoQuad)
Blog		Blogger	Dynamic web based CMS (Content Management System) solution	Software publishing platform with blogging/content management capability (Ex: Squarespace)
Wiki Services		MediaWiki, WikiSpaces	Pending Review	Public wiki software for external knowledge sharing and enterprise wiki software for internal knowledge sharing
Web content Management	Plume	Pending Review	Pending Review	Cloud WCM (Ex: CrownPeak SaaS WCM, Autonomy, SDL Tridion, Sitecore WCM)

MESSAGING AND SOCIAL MEDIA SUB-DOMAIN

Closely associated with the broadcast messaging sub-domain is the messaging and social media sub-domain described in Table 51. The key characteristic of this sub-domain is the non-broadcasting but more personal one-on-one communication activities.

Table 51: Messaging and Social Media Sub-Domain Description

UC Messaging and Social Media Sub-Domain	Sunset Products / Standards	Current Supported Products/ Standards	Preferred Products / Standards	Emerging Trends
External IM		Google IM	Pending Review	Enterprise level social tool that sends information proactively via a real-time news stream (Ex: Chatter by salesforce.com, Jive, or CiscoQuad)
Social Media		Twitter, Facebook	Pending Review	Enterprise level social tool that sends information proactively via a real-time news stream (Ex: Chatter by salesforce.com, Jive, or CiscoQuad)
Blog		Blogger	Pending Review	Pending Review

CITIZEN COMMUNICATION AND ENGAGEMENT

Citizen communication and engagement sub-domain is intended to attract comments and opinions from the citizens as well as provide significant information in a form and format that is useful. This domain is described in Table 52.

Table 52: Citizen Communication and Engagement Sub-Domain Description

UC Citizen Communication and Engagement Sub-Domain	Sunset Products / Standards	Current Supported Products/ Standards	Preferred Products / Standards	Emerging Trends
External portal		Open government framework	Enterprise Web Portal	Enterprise web portal utilizing WSRP (Web Services for Remote Portlets)
Collaboration		Open government framework	Pending Review	Pending Review
Engagement		Web-based tools (e.g., IdeaScale, Constant Contact, Survey Monkey)	Pending Review	DCM (Digital Communication Management) platform that enables government to maximize direct connections with the public

ETA TRANSITION AND SEQUENCING PLANNING SUMMARY FOR THE UNIFIED COMMUNICATION DOMAIN

The transition and sequencing plan for the Unified Communications Domain is based a thorough assessment of the current product base and decide status and evaluate strategic alignment options.

- Select pilot project (e.g. Voice over IP) to demonstrate near term solutions using cloud based technology that integrates with the new EA.
- Participate with the Messaging and Collaboration planning team to provide a road map and project phasing to address a comprehensive integrated capability.



EVALUATE LEADING TECHNOLOGY PLATFORMS

This investment selects a standard collaboration solution across the State. Project activities include evaluation of leading technology platforms such as Microsoft SharePoint or Lotus Domino Quickr or open source offerings. This effort should be executed in conjunction with the email system initiative. Considerations will be given to solutions on Gartner Magic Quadrant. The scope includes implementation of necessary technical infrastructure and connectivity for cross-departmental workgroup and project collaboration. Estimated costs for this initiative are Pending Review.

PILOT VOIP

The State will initiate a 400-person pilot, based on vendor experience, at an estimated cost of Pending Review.

IMPLEMENT VOIP STATE-WIDE

The VoIP pilot provides the implementation in tiative lessons learned and a solid basis for the actual implementation schedule and costs. As an additional data point, a vendor-provided estimate to the State of Hawai'i to extend VoIP to every State building was estimated to be Pending Review for a "turnkey" engagement for 26,000 end points and as planning progresses the following provides a list of cost considerations:

- Implementation – Typically, companies spend about 20% more in the first two years of their VoIP deployments on the actual implementation than they would have spent in TDM. After they gain expertise, implementation costs are equivalent to TDM rollouts.

Key Points

- Unified communications requires a phased approach, beginning with small steps that target the low-hanging fruit.
- UC projects should start with harnessing existing assets and building from there rather than attempting a one-size-fits-all approach.
- End-user communication is vital for project success.
- Switches – This covers the cost of IP PBXs or the cost to IP enable an existing PBX.
- Handsets/End-Unit Devices or Applications– This includes IP hardphones or softphones.
- Gateways - Often, companies require gateways for TDM to-IP traffic, unless they're using SIP trunking throughout the organization (which is rare still).
- LAN upgrades – VoIP requires Power-Over-Ethernet switches, and most companies provide Uninterrupted Power Supplies to provide for backup. When organizations upgrade their LANs, the costs account for 32% to 47% of an overall VoIP project. Table 53 highlights the typical LAN upgrade costs. These figures include the POE switches, UPS, management tools, and staffing costs, as well as first year of maintenance.

Table 53: Typical LAN Upgrade Costs

IP Telephony Implementations				
Cost per end unit*	Less than 500	501 – 5,000	More than 5,000	All sizes
IPT Hardware	Pending Review	Pending Review	Pending Review	Pending Review
LAN Upgrade	Pending Review	Pending Review	Pending Review	Pending Review
LAN Upgrade Total Average Capital	Pending Review	Pending Review	Pending Review	Pending Review
LAN Upgrade % of Total Capital	45%	41%	32%	42%

**End unit is IP handset, audio bridge, softphone or other end-user device.*

- Management/monitoring tools – Many companies don't budget for management and monitoring tools, which is a mistake. Acquisition costs range from free (with open-source tools) to several million dollars. On average, small and midsize companies spend about Pending Review for each third-party monitoring tool, and large companies spend about Pending Review per tool.
- Training – Many vendors are including training with the sale of equipment. But when they don't, companies spend between Pending Review and Pending Review per IT staff member for training, and they find the most success by training their end users with internal IT staff.

- Equipment licensing and maintenance – Vendors are shifting more to a software model in which the initial acquisition cost is lower, but maintenance and licensing is higher. Whereas vendors once charged about 10% to 14% for maintenance, those fees now are 16% to 22%.
- Ongoing WAN costs – This includes the cost of the converged WAN. Typically, this includes the circuit costs for services such as MPLS, Ethernet, and/or SIP trunking.
- Ongoing operational costs – This includes the cost to manage and maintain the network from a staff perspective. It includes the total compensation of internal staff members devoted to VoIP, plus the cost of any third-party MSPs managing the VoIP system. Also included are power and cooling costs.
- Ongoing network costs – Companies that have not converged voice and data traffic onto a single WAN can save money by eliminating idle capacity and combining access lines. The typical savings is 23%.
 - Staff changes (non-IT) – Some companies are able to reduce staff in other areas because of VoIP. For example, one receptionist can handle multiple locations when he or she can transfer calls and intercom between locations, rather than having to tell a caller to hang up and dial a different number. Or, by using automated attendant, companies have been able to reduce the need for a receptionist at every location, as well. This typically translates into a Pending Review to Pending Review annual savings.
 - Turnover Rates – By allowing employees to work from home, particularly those who work in a contact center, companies are reducing turnover rates. Typical contact-center turnover rates are 35% to 45%, but by giving those employees more flexible work schedules from their home offices, they are dropping turnover rates to 10% to 20%. VoIP allows companies to do this cost-effectively by paying for just a broadband access line (Pending Review to Pending Review per month, depending on service level) and eliminating the Pending Review to Pending Review monthly POTS charge for voice service.
- Savings from SIP trunking – Replacing PRI lines with SIP trunks can save about 40% off the monthly circuit costs.
- Fixed Mobile Convergence – Companies with many mobile employees eliminate costly roaming charges by moving mobile calls to the corporate IP backbone (calling a local number and routing the call from the IP PBX through the corporate WAN).
- IT Cost Considerations
 - Cabling – With IP telephony, there is no longer a need for three to four drops (two Ethernet; two RJ-11) per desktop. Companies typically save about 40% on cabling costs in new buildings (and average spend per drop is about Pending Review).
 - Softphones vs. hardphones – There is a small but growing trend among companies to continue using existing analog or digital handsets with their IP or hybrid switches and move directly to IP softphones. Licenses for softphones range from about Pending Review to Pending Review, compared to a range of Pending Review to Pending Review IP hardphones, so companies can save money with this approach. Among companies using softphones, 53.6% are using them as an adjunct to hardphones, and 35.7% are using them as a replacement to softphones. The balance is in pilot phase.
 - Centralizing servers – By centralizing servers at the data center, organizations report savings in the number of servers they need to buy, along with reduced tools and resources to manage applications such as unified messaging, conferencing, and even the IP PBX itself. By using fewer servers than would be used in a distributed model, companies can save on power and cooling costs, as well.
 - Audio conferencing – By replacing audio-conferencing services with an internal audio-conferencing bridge, companies can eliminate their monthly charge for audio conferencing services. For organizations with limited audio conferences, most vendors offer bridges that are integrated with the IP telephony system (albeit limited to the number of participants).
 - Hosted services – Companies concerned about capital outlay find savings through the use of hosted services. They eliminate the up-front costs of the IP PBXs and handsets because they are included in the monthly service fee. But, the overall service may or may not be less expensive. The point here is that hosted services eliminates the up-front capital cost and depreciation but typically costs more monthly to operate than in-house deployments.
 - Moves, Adds, and Changes – Many companies have justified their entire IP telephony rollout though MAC savings alone. Externally provide MACs cost Pending Review to Pending Review, depending on the city. Internally managed IP telephony MACs cost about Pending Review, based on average telecom salaries.
 - Staff changes (IT) – Though we do not see huge reductions in the staff required to manage VoIP vs. TDM environments, more companies decrease their staff than increase it. Among those who decrease the telecom staff, they lose about 2.8 people on average. Attrition is more common than layoffs; IT staffs frequently reassign their telecom staff to other areas of IT or don't replace retirees. Those who increase their staff do so by one person. (Please see Figure Z: Staff Changes with VoIP).

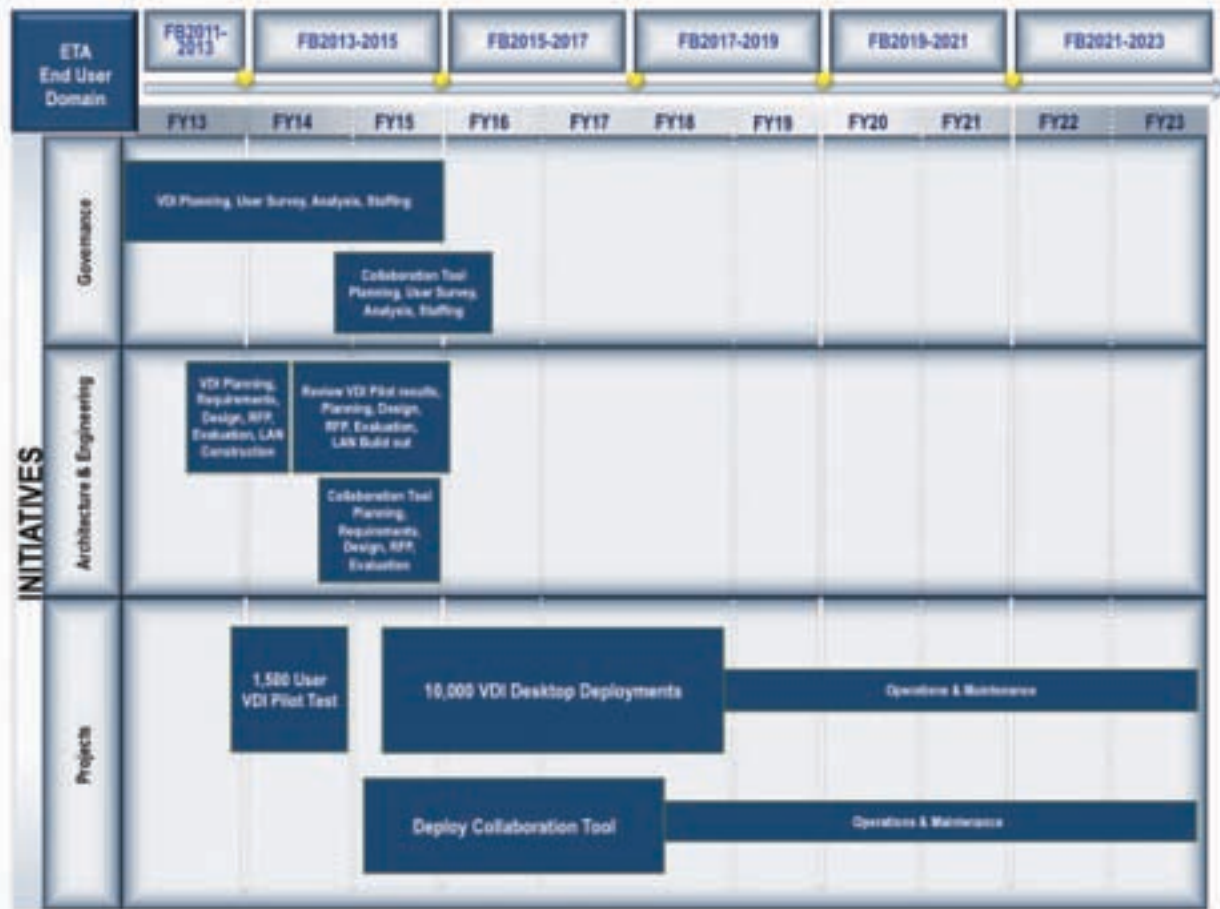


Figure 48: Roadmap to Future State for the End User Domain

7.2.3.5 INFORMATION MANAGEMENT DOMAIN

The goals, objectives, strategies, policies, and principles defined within the EIA and the associated solutions within the ESA are supported by the technology principles, standards, and products defined within the Information Management Domain of the Enterprise Technology Architecture. The information management domain considers relevant technologies related to the scope of data, information, and knowledge assets of the enterprise – both structured and unstructured data as defined within the EIA, and the full life cycle and management discipline of information from creation, to storage and retention, to use, archival, and deletion.

CURRENT STATE SWOT FOR THE INFORMATION MANAGEMENT DOMAIN

The current state of information management practices within the State was discussed above in the EIA. The current state is characterized by a lack of standardization in technologies used in any of the sub-domains below. This area provides a significant opportunity to vault forward with enhanced cultural values in the importance of sound information management, and new processes, practices, and technical solutions.

FUTURE STATE VISION FOR THE INFORMATION MANAGEMENT DOMAIN

The future state vision for Information Management was discussed above in the EBA, EIA, and the ESA outlined the related enterprise service areas of knowledge management, data management, analytics, digital content management, and search. This section highlights additional detail regarding the future state services and technology vision, principles, and standards within the sub-domains.

The summary elements of the future state vision for Information Management include:

- Data Management Services
 - Enterprise and LOB operational databases implemented using relational database management systems technology
 - Enterprise and LOB analytical databases (data warehouses or data marts) implemented using de-normalized relational databases or On-Line Analytical Processing (OLAP) cube technology
 - Enterprise and LOB data management services for create, read, update, and delete (CRUD) of enterprise or LOB data entities

- Digital Content Management Solutions
 - Electronic documents
 - Document management services to store and manage electronic documents including all media types (text, images, video)
 - Document management repositories
 - Document metadata maintained over the life of the document
 - Other content (unstructured data)
 - Content management services to store and manage other unstructured data within defined stores, such as Web page or collaboration content to include all media types
 - Automated content indexing to facilitate search and retrieval
- Records Management
 - Record management services to create and extract digital records and link to and partition within underlying data and information (digital content) stores
 - Records metadata maintained over the life of the record
- Search
 - An enterprise search capability that integrates search across all information management sub-domains discussed here – data, documents, and other digital content
- Business Intelligence and Analytics Solutions
 - Utility services to support the creation of analytics solutions to include analysis and statistics, visualization, graphics, dashboards, drill-downs, ad hoc query, and reporting
- Knowledge Management Solutions
 - The utilization of all capabilities above + collaboration services to build knowledge management solutions for specific problem domains within the enterprise or LOBs.

Guiding Principles for the Information Management Domain

1. The State will continue to have a need to manage official documents and records within its operations. The future direction is for the official authoritative source of all documents or records to be electronic. An enterprise document management solution will address this need, but associated technology standards and products are specified here.
2. Within the operations tier, relational database management systems will be the standard for storing all State data.
3. Analytics and visualization capabilities will integrate geospatial data. Geotagging of data should be evaluated for use in all State database implementations.

DIGITAL CONTENT MANAGEMENT SUB-DOMAIN

The Digital Content Management Sub-Domain is described in Table 54.

Table 54: Digital Content Management Sub-Domain Description

Information Management Document Management Sub-Domain	Sunset Products / Standards	Current Supported Products/ Standards	Preferred Products / Standards	Emerging Trends
Electronic document formats	<ul style="list-style-type: none"> • Microsoft Office • PDF 	<ul style="list-style-type: none"> • Microsoft Office • PDF • XML • HTML5 		HTML5
Electronic document workflow	<ul style="list-style-type: none"> • FileNet • Documentum • Microsoft SharePoint 	<ul style="list-style-type: none"> • FileNet • Documentum • Microsoft SharePoint 		
Document integration with other structured data				

DOCUMENT MANAGEMENT SUB-DOMAIN

The Document Management Sub-Domain is included in Table 55.

Table 55: Document Management Sub-Domain Description

Information Management Document Management Sub-Domain	Sunset Products / Standards	Current Supported Products/ Standards	Preferred Products / Standards	Emerging Trends
Electronic document formats		<ul style="list-style-type: none"> • Microsoft Office • PDF • XML • HTML5 	ISO 19005-1. Document management - Electronic document file format for long-term preservation - Part 1: Use of PDF 1.4 (PDF/A)	HTML5
Electronic document workflow		Microsoft Office 2010	ISO 19005-2:2011 specifies the use of the Portable Document Format (PDF) 1.7, as formalized in ISO 32000-1	
Document integration with other structured data			ISO 19005-2:2011 specifies the use of the Portable Document Format (PDF) 1.7, as formalized in ISO 32000-1	

DOCUMENT MANAGEMENT SUB-DOMAIN

Table 56 described the Data Management Sub-Domain.

Table 56: Data Management Sub-Domain Description

Information Management Document Management Sub-Domain	Sunset Products / Standards	Current Supported Products/ Standards	Preferred Products / Standards	Emerging Trends
Database management	• ISAM	<ul style="list-style-type: none"> • Oracle • SQL Server • DB2 • Adabas • Microsoft Access 	• Relational DBMS	
Data integrity	• Application software	• Relational DBMS integrity rules; web services		
Data modeling		• ER models		• RDF
Metadata management – dictionaries, directories, or repositories		• EA repository		
Data query		• SQL		• SPARQL
Data exchange		• XML		• RDF extractions from Databases, NIEM

ANALYTICS SUB-DOMAIN

Table 57 describes the Analytics Sub-Domain.

Table 57: Analytics Sub-Domain Description

Information Management Analytics Sub-Domain	Sunset Products / Standards	Current Supported Products/ Standards	Preferred Products / Standards	Emerging Trends
Data storage for analytics data or "big data"	• ISAM	• Pending Review		Hadoop
Data extraction, transformation, and loading (ETL) and cleansing,		• Pending Review		
Dimensional data cubes		• Pending Review		
Analysis and visualization		• Pending Review		
Dashboards		• Pending Review		
End user ad hoc data query and reporting		• Pending Review		

GEOGRAPHIC INFORMATION SYSTEM (GIS) SUB-DOMAIN

Table 58 represents the GIS Sub-Domain

Table 58: GIS Sub-Domain Description

Information Management GIS Sub-Domain	Sunset Products / Standards	Current Supported Products/ Standards	Preferred Products / Standards	Emerging Trends
Geospatial data formats and frameworks			OpenGIS© Standards: http://www.opengeospatial.org/standards	ArcGIS Online (in the cloud)
Geospatial data interoperability and transformation			OpenGIS© Standards: http://www.opengeospatial.org/standards	ArcGIS Online (in the cloud)
Geospatial data sets and services			OpenGIS© Standards: http://www.opengeospatial.org/standards	ArcGIS Online (in the cloud)
Geographic information systems	ESRI ArcGIS		OpenGIS© Standards: http://www.opengeospatial.org/standards	ArcGIS Online (in the cloud)

ETA TRANSITION AND SEQUENCING PLANNING SUMMARY FOR THE INFORMATION MANAGEMENT DOMAIN

Transition and sequencing will be based upon a thorough assessment of the current data management and GIS posture. This assessment is a critical input to the development of a sequencing plan that organizes all of the major elements of GIS, Data Management, and Analysis and Visualization as subprojects within the larger initiative

The Information Management Working Group is identifying a roadmap and project phasing to address a comprehensive integrated capability. Additional directional information is provided at the below url.

Information Management Domain Addendum Information

http://idea.hawaii.gov/userimages/accounts/90/907159/panel_upload_18993/SupplementalAddendumDigitalArchives.pdf

7.2.3.6 APPLICATION ENVIRONMENT DOMAIN

The goals, objectives, strategies, policies, and principles defined within the ESA are supported by the technology principles, standards, and products defined within the Application Environment Domain of the Enterprise Technology Architecture. The application environment domain considers relevant technologies related to the environments, platforms, and technology stacks that the enterprise application solutions are built upon. As directed in the ESA, the State will move towards standard enterprise solution patterns that will in turn lead towards an optimum set of standard application environments.

FUTURE STATE VISION FOR THE APPLICATION ENVIRONMENT DOMAIN

To achieve the future state vision for the ESA, the State will require considerable standardization and maturity within the software development and integration service area. The key elements for this service area are depicted in Figure 49 and discussed in more detail below.

CURRENT STATE SWOT FOR THE APPLICATION ENVIRONMENT DOMAIN

The State currently has individual areas of strength in applications development maturity, but the overall environment lacks standardization for process, methodology, skills development, knowledge exchange, or tools and technology.

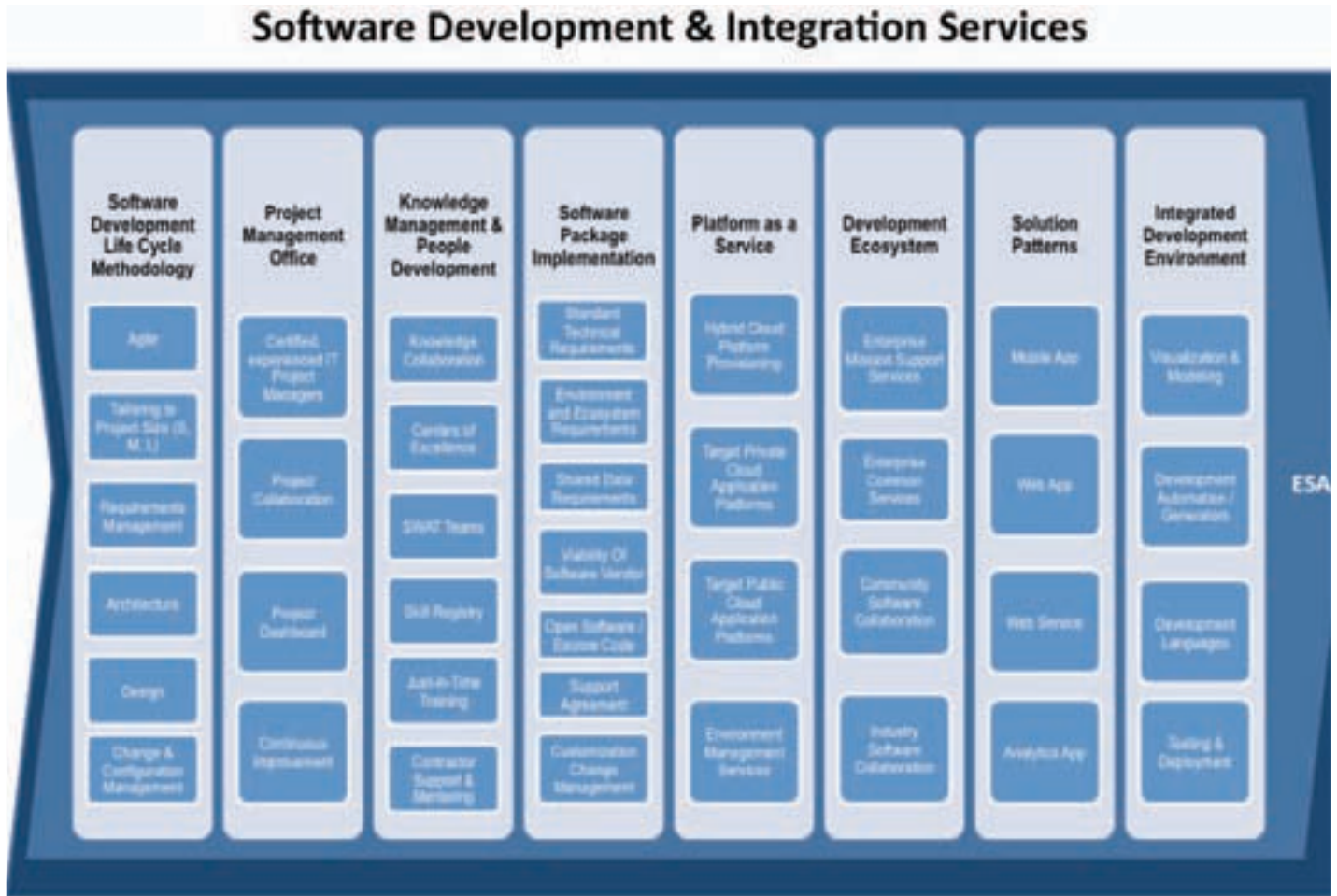


Figure 49: Elements of Future State Software Development Environment

The elements related to achievement of the future state vision are organized within the three major focus areas of Governance, Architecture and Engineering, and Projects.

Governance

Key elements of governance related to the Application Environment Domain include the SDLC, the PMO, and Organization, Culture, and Professional Development.

Software Development Life Cycle (SDLC) Methodology

The vision for the State's new SDLC includes these elements:

- Agility – the most critical aspect is the incorporation of agile methods to facilitate a responsive environment for making rapid decisions, course corrections, and establishment of new directions quickly with system implementation projects within the State.
- Tailorable – the SDLC methodology is organized in such a manner to facilitate tailoring of project activities and deliverables based on project size, e.g. small, medium, or large.
- Software Packages – the methodology addresses both software package implementation and custom software development.
- Usability – the methodology is developed and maintained with helpfulness and usability in mind, and includes process overviews, activity and deliverable instructions and helpful guidelines and suggestions for use, including templates and examples.
- Requirements Focus – a key focus area throughout the SDLC is on developing and managing appropriate measurable requirements for both business and technical perspectives.
- The goal for overall software development maturity within the State is to achieve a CMMI Level 3 maturity within 5 years.

Project Management Office

The vision for the State's new PMO with respect to systems implementation projects includes these elements:

- Experienced Project Managers – the State develops over time a strong PMO with experienced and certified IT project managers. These project managers facilitate the strong execution of the SDLC within their teams. They are engaged early on, and help navigate through requirements development and software package procurement.
- Defined Project Teams – all software development and system implementation projects are managed as a project effort with a defined project team.
- Project Performance Incentives – the successful execution of a project is a critical competency for the State, and project performance is measured and reported, and cultural factors have been enhanced to provide significant incentives for success
- Organizational Change Management – the extent of change for the user community as the new solutions are deployed is significant, and a robust organizational change discipline ensures user involvement, awareness, and education.
- Project Collaboration – collaboration services enable each project to effectively share information, knowledge, and status, and coordinate activities and schedules.
- Project Dashboard – project status is reported through a dashboard for visibility into performance and risk/issues.
- Continuous Improvement – a continuous improvement program surrounds project execution enabling lessons learned, customer and participant feedback, and performance measurement to weave back into improvements of the SDLC methodology, project culture, and tools and technologies.

Knowledge Management and People Development

The vision for the development of people, skills, capabilities, and knowledge for software development as a whole includes these elements:

- Knowledge Collaboration – software development becomes a model discipline for effective knowledge management. The software development community promotes knowledge sharing of environments, platforms, and specific application problem domains. Collaborative wiki style tools are used across the software development community.
- Centers of Excellence – organizations or teams are recognized for expertise in specific application development approaches and patterns, and facilitate project team success through training, knowledge exchange, and mentoring. (Example of AG Justice for J2EE development.)
- SWAT Teams – skilled, experienced teams from the Centers of Excellence support projects with inexperienced staff to facilitate mentoring and project delivery success.
- Skill Registry – a skill registry provides a critical tool for location of expertise within the State for help and assistance.
- Just-in-Time Training – a continuous education program for software development integrates with staff annual performance plans, focusing on development of new skills and enhancement of skills. Various incentives approaches are inculcated into the culture. A variety of educational approaches are used such as mini classes, brown bags, informal sharing and collaboration, social network, wiki's, as well as formal training. The variety enables the project to ensure that education is provided just-in time. Partnering with UH provides new programs tailored to developing skills for State employees.
- Contractor Support and Mentoring – contractors are strategically used to bring in expertise and experience; but project teams incorporate the needed mentoring and knowledge capture activities to transfer the expertise to State team members.

Software Package Implementation

The vision for incorporating packaged software includes these elements:

- Standard Technical Requirements – consistent with the ETA and standard platforms, technical requirements are standardized for reuse in RFPs. These requirements are managed adequately within the evaluation to not stop but steer decisions.
- Environment and Ecosystem Requirements – standard requirements in software RFPs include making sure package or system procurements include life cycle support such as test (QA/QC), staging, production environments, and training environments.
- Integration Requirements – requirements are included for providing data models, compliance with industry standard data such as NIEM, use of Web services or APIs, standard data access (like ODBC), providing reporting capabilities or a data mart/warehouse.
- Viability of Software Vendor – include an evaluation of the viability of the vendor to enhance the probabilities that the vendor will support the package for the life expectancy needed.
- Open Software / Escrow Code – use open software to have access to the source code or require the vendor to put the source code into escrow.
- Support Agreement – include a support agreement in the procurement. Include provisions to bring support in house, or with consultants to keep those options open.
- Customization Change Management – use an Executive Steering Team for guidance and escalation of requirements issues, specifically with respect to minimizing customizations to industry standard software.

Architecture and Engineering

Key elements of architecture and engineering related to the Application Environment Domain include the ESA Common Solutions Framework, Solution Patterns, the Development Ecosystem, the Integrated Development Environment, and Platforms as a Service.

Common Solutions

Framework and Patterns

The vision for a common solutions framework and solution patterns or reference architectures includes these elements:

- Common Solutions Framework – a common solutions framework, including architecture and development approach facilitates software development. The framework incorporates standard enterprise services for a common user interface (my.Hawaii.gov), authentication, role-base authorization, data access, and shared enterprise services.
- Standard Application Patterns – convergence on standard platforms environments and strategic solution patterns with associated technologies such as mobile applications streamline the overall development approach.

Software Development Ecosystem

The vision for a software development ecosystem supporting collaborative development and reuse includes these elements:

- Enterprise Services – inclusion of enterprise services within the development ecosystem for integration into the common solutions framework.
- Community and Industry Software Collaboration – a SourceForge or “Force.com” or “Google App Engine” or “Github” type environment for community development and sharing reuse of trusted, certified source code. Also, a State “apps store” for release of trusted, certified apps to the customer base.
- Legacy Systems Services – specific services to support the wrapping and inclusion of legacy software into the enterprise services, and migration approaches or tools for migrating legacy code into the modernized environment.
- Full Life Cycle Planning – planning for the life expectancy of a software application and building refresh upgrade into the planning. Having metrics on application system “soundness”, to include break fix frequency, difficult to fix/sustain, and down-time.

Integrated Development Environment

The vision for the integrated development environments for software development includes these elements:

- Visualization and Modeling – draw it to code it.
- Development Automation / Generators – automate as much of the SDLC as possible, including code generation and automated testing.
- Development Languages – standardize on technologies used.
- Testing and Deployment – standardize on approaches, tools, and technologies used.

Platform as a Service

The vision for provision of platforms as a service includes these elements:

- Research, Development, Test Environment (RDTE) – provisioning of platforms for the RDTE.
- Hybrid Cloud Platform Provisioning – rapid provisioning of private (or public) virtual environments for system environments.
- Target Private Cloud Application Platforms – standard target application environments (platforms) are provisioned within minutes within the State’s private cloud.
- Target Public Cloud Application Platforms – for specific public or non sensitive uses, standard target application environments (platforms) are provisioned within minutes within secure, trusted public cloud environments such as Amazon Web Services, Windows Azure, or Google App Engine.

Projects

Key project elements related to the Application Environment Domain include the Hawai`i Common Portal and Enterprise Services Implementation, Project Registry and Reporting, and Legacy Systems Migration.

Hawai`i Common Portal

The implementation of the Hawai`i Common Portal, the my.hawaii.gov, includes the following:

- Implement new my.hawaii.gov standards, solution, technologies
 - Develop governance structure over common requirements gathering and management for shared services.
 - Pilot initial implementations; pilot potential future state technologies.
 - Standardize and finalize overall governance and implementation approach, and scale out to broader set of capabilities and implementation stakeholders in an on-going implementation.
- Monitor on-going use and continuous improvement.

Enterprise Services

The implementation of the Enterprise Services within the Common Solutions Framework includes the following:

- See Enterprise Services Section 6 to see the potential scope of the services needed.
- Prioritize the initial set of services for implementation – suggested initial focus includes identity management, role based access, customer management, business management (e.g. organizations), document management, geospatial, and dashboards/drill-down reporting.
- Develop governance structure over common requirements gathering and management for shared services.
- Pilot initial implementations; pilot potential future state technologies – e.g. whether an enterprise services bus needs to be used.
- Standardize and finalize overall governance and implementation approach, and scale out to

broader set of services and implementation stakeholders in an on-going implementation.

- Monitor on-going use and continuous improvement.

Project Registry and Reporting

The implementation of the Project Registry and Reporting approach, standards, and tool set includes the following:

- Implement new IT project registry and reporting approach, standards, solutions, and technologies
 - Develop governance structure over common requirements gathering and management for project oversight and reporting.
 - Scope includes life cycle reporting of IT projects, focused on initial authorization, governance, and reporting through consolidated dashboard capabilities.
 - Pilot initial implementations; pilot potential future state technologies.
 - Standardize and finalize overall governance and implementation approach, and scale out to broader set of capabilities and implementation stakeholders in an on-going implementation.

- Monitor on-going use and continuous improvement.

Legacy Systems Migration

The implementation of a consolidated Legacy Systems Migration project includes the following:

- Goal of Legacy Systems Migration project is to help achieve overall reduction by tenfold of the applications portfolio (reduce 705+ applications).

- The legacy systems portfolio is characterized by numerous small point solutions that often times are intended to address shortcomings of the mission support systems – such as departmental tracking systems in Lotus Domino for procurements, time and attendance, financial transactions, etc.
- Perform Analysis of the overall legacy systems portfolio. Determine future action on current apps, ERP impact, etc. Examples for consideration – Mainframe apps, Lotus Domino apps. Use a graded approach – some need to be redesigned, some need to be killed, some could be ported.
- Re-platform the targeted set of apps – some subset of apps ported off a legacy platform to a modernized platform.

Guiding Principles for the Application Environment Domain

1. Target technology platforms for State application solutions shall be based upon open industry standards and shall avoid being “locked into” specific vendor products, and therefore able to operate on a variety of technology platforms. This standards-based approach allows for vendor independence which promotes cost savings.
2. The target architecture for future applications will be thin client requiring only network access and a web browser for end-user access. Application solutions targeted for thick client, client/server, or the desktop are no longer preferred and should not be developed.
3. XML web services are the preferred future state application integration technology. Business logic and data access should be implemented through XML web services.

APPLICATION DEVELOPMENT AND INTEGRATION SUB-DOMAIN

The Applications Development and Integration Sub-Domain is described in Table 59.

Table 59: Application Development and Integration Sub-Domain Description

Application Environment Application Development and Integration Sub-Domain	Sunset Products / Standards	Current Supported Products/ Standards	Preferred Products / Standards	Emerging Trends
Application Integration		<ul style="list-style-type: none"> • XML Web services • Direct SQL access to Enterprise and LOB Databases 	<ul style="list-style-type: none"> • Relational DBMS 	
Integrated Development Environment				
Visualization and Modeling		<ul style="list-style-type: none"> • UML • ER models • XML transfers 		
Requirements Management		<ul style="list-style-type: none"> • UML • XML transfers 		
Software Configuration Management				

CLIENT SERVER APPLICATIONS SUB-DOMAIN

Table 60 describes the Client Server Applications Sub-Domain.

Table 60: Client Server Applications Sub-Domain Description

Application Environment Client Server Applications Sub-Domain	Sunset Products / Standards	Current Supported Products/ Standards	Preferred Products / Standards	Emerging Trends
Development Environment and Tools		Pending Review		
Quality Assurance and Testing		Pending Review		
Production Platform		Pending Review		

WEB APPLICATIONS SUB-DOMAIN

This sub-domain is described in Table 61.

Table 61: Web Applications Sub-Domain Description

Application Environment Web Applications Sub-Domain	Sunset Products / Standards	Current Supported Products/ Standards	Preferred Products / Standards	Emerging Trends
Development Environment and Tools		<ul style="list-style-type: none"> • IBM WebSphere • MS Visual Studio 		
Quality Assurance and Testing				
Production Platform		<ul style="list-style-type: none"> • Java 2 Enterprise Edition • Microsoft .NET • LAMP 		
User Interface		<ul style="list-style-type: none"> • HTML5 		
Business Logic				
Data Access		<ul style="list-style-type: none"> • SQL 		

MOBILE APPLICATIONS SUB-DOMAIN

Table 62 describes the Mobile Applications Sub-Domain.

Table 62: Mobile Applications Sub-Domain Description

Application Environment Web Applications Sub-Domain	Sunset Products / Standards	Current Supported Products/ Standards	Preferred Products / Standards	Emerging Trends
Development Environment and Tools		Rhodes, RHOStudio		
Quality Assurance and Testing	RHOHub	RHOHub		
Production Platform		RhoConnect		
User Interface		HTML5		
Business Logic		Pending Review		
Data Access		Pending Review		

EMBEDDED SYSTEMS SUB-DOMAIN

Table 63 describes this sub-domain.

Table 62: Mobile Applications Sub-Domain Description

Application Environment Embedded Systems Sub-Domain	Sunset Products / Standards	Current Supported Products/ Standards	Preferred Products / Standards	Emerging Trends
Development Environment and Tools		Pending Review		
Quality Assurance and Testing		Pending Review		
Production Platform		Pending Review		

ETA TRANSITION AND SEQUENCING PLANNING SUMMARY FOR THE APPLICATION ENVIRONMENT DOMAIN

The Development Working Group consists of representation of the software development community across the state and has been active in providing direction in future state visioning and in implementation planning for this area. The work plan enables the continued development and detailing of the elements of the future state vision, in addition to implementation of the vision.



SOFTWARE ENGINEERING IMPROVEMENT

Several identified software engineering improvement initiatives have been identified and detailed separately below and are consolidated together in one initiative within the T&S Plan.

FORMALIZE AN ENTERPRISE SDLC METHODOLOGY

This initiative formalizes the State's new enterprise SDLC methodology and achieves the vision for two key areas defined in the Section 7.2.3.6 – Software Development Life Cycle (SDLC) Methodology and Software Package Implementation. (Refer to the requirements listed there for inclusion in project scope.) The formulation initiative ensures appropriate review and feedback on the draft SDLC developed by OIMT, and will accomplish suitable piloting of the SDLC within initial projects with the goals of further refining the methodology and building teams of experts to accomplish broader adoption in the follow on initiative. Methodology is delivered through Web collaborative environment. The estimate of costs for this initiative is Pending Review.

ADOPT ENTERPRISE SDLC METHODOLOGY

This activity serves as the process to adopt the State's new enterprise SDLC methodology through focused use of new methodology on projects across the departments in an incremental fashion using expertise from mentoring teams and training to equip project teams and staff across the state. This task also includes further refining of the methodology through lessons learned approach. The cost estimate for this project is Pending Review on-going O&M annually.

IMPLEMENT SOFTWARE ENGINEERING PROJECT MANAGEMENT IMPROVEMENT

This initiative has to the goal of improving overall project management approach, expertise, practices, and tools for software engineering projects within the state. Achieves the vision for the Project Management Office defined in Section 7.2.3.6. Focus areas include PM best practice development, training program development and execution, project performance measurement and reporting, and resource development in a collaborative environment. The initiative will be done in close collaboration with Project Registry and Reporting System Implementation. The cost estimate for this project is Pending Review.

IMPLEMENT SOFTWARE ENGINEERING CONTINUOUS IMPROVEMENT PROGRAM

This activity is a one-time implementation of a software engineering continuous improvement program within the State. This initiative includes tasks to establish the organization, staff the organization, and establish the program. Goals of the program include establishing performance service levels and measures, on-going monitoring of progress, administering performance and compliance assessments against industry best practice frameworks and maturity models such as CMMI, and sponsoring desired audits from external organizations. This task also provides guidance and assurance of achieving industry best practices in software engineering for optimized performance in responsive automation of business processes, achieving strategic integration, and interoperability.

The estimated cost for this project is Pending Review.

IMPLEMENT SOFTWARE ENGINEERING MENTORING AND CONSULTING PROGRAM

This initiative establishes a standard mentoring and knowledge transfer approach for the software engineering community and pilot the approach with refinement and adoption for use across the State. Activities include establishing a skills and expertise registry for locating expertise for assistance; and would put in place appropriate acquisition channels for access to external consultants. Project startups with new approaches, tools, or technologies are supported by a formal mentoring process including special mentoring or SWAT teams to assist. See Knowledge Management and People Development in Section 7.2.3.6 for additional information. The estimate for this initiative is Pending Review

DEVELOP SOLUTION PATTERNS

This project expand the SDLC to include guidelines, how-to's, techniques, tools, and training/mentoring to do software engineering in strategic solution patterns: Web, Mobile, Services, and Analytics. Refer to Section 6.2.2.5 Standard Enterprise Solution Patterns and Common Solutions Framework and Patterns in Section 7.2.3.6. The activities for this project optimize effectiveness of software engineering efforts/projects in use and development of skilled resources for overall improvement in responsive automation of business processes, achieving strategic integration and interoperability. The estimated cost is Pending Review.

IMPLEMENT SOFTWARE ENGINEERING CONTINUOUS IMPROVEMENT PROGRAM OPERATIONS

This activity formalizes the on-going administration and operation of software engineering continuous improvement program within the State. It includes on-going emphasis and activities within the following focus areas: on-going training and skill development; compliance to industry best practices and maturity models; and on-going assessments and improvements. It also optimizes effectiveness of software engineering efforts/projects in use and development of skilled resources for overall improvement in responsive automation of business processes, achieving strategic integration and interoperability. The estimated cost is Pending Review

ENTERPRISE DATA AND SERVICES STANDARDIZATION AND SHARING

This investment centers on establishing a program to support the standardization and sharing of enterprise data and services. See EIA Common Information Framework in Section 5.2.2.1 and the ESA Common Solutions Framework in Section 6.2.2. The investment supports the Enterprise Architecture Program, and implements a series of activities and accomplishments to establish

these enterprise-wide data and services management standards and practices. These include:

- Establishing governance standards and practices which include the role of the information stewards and the processes for collaboration, agreement, documentation, and change management of common enterprise or LOB data and services – an area similar to what the industry may refer to as master data management.
- Establishing the common data and services architecture within the EA tool and repository, inventories of enterprise and LOB data and services assets; and the approach and practices for defining shared (or master) data and services standards.
- Establishing the administration standards and practices for creating and maintaining official enterprise and LOB databases and services.

The budgetary estimate for this is Pending Review.

IMPLEMENT SOFTWARE DEVELOPMENT COMMUNITY ECOSYSTEM

This initiative has the goal of implementing tools and an environment to support collaboration and code retention and sharing within the software development community for the State of Hawai`i. It achieves the vision for the software development community ecosystem and integrated development environment (IDE) defined in Section 7.2.3.6; similar to environments such as SourceForge.com; force.com; and Google apps development communities. It also streamlines, standardizes, agile processes and the methodology for developing application software for responsive automation of business processes, achieving strategic integration and interoperability, and maximizing reuse of existing software components. The cost estimate is Pending Review.

IMPLEMENT EA COMMON INFORMATION AND SOLUTIONS ARCHITECTURE / FRAMEWORK ADMINISTRATION

The on-going support of common information and solutions architecture and framework within the State is included in this project. Activities include administration of common architectures to support standardization and sharing across the State; and oversight and maintenance of data and services information within EA repository. Refer to the EIA Common Information Framework in Section 5.2.2.1 and the ESA Common Solutions Framework in Section 6.2.2 for more information on this project. The cost estimate for this work is Pending Review.

CREATE A COMMON PORTAL IMPLEMENTATION

This project include the implementation of the common user interface portal for all end users – state employees, citizens, residents, and other government staff – federal and local, and business partners. The portal is envisioned as a “my.hawaii.gov” implementation – a customized common interface across any end user device platforms – desktop, laptop, tablet, and mobile. This is a critical element of the ESA Common Solutions Framework as defined in Section 6.2.2. Portal implementation has significant standardization issues from a people, culture, and organization perspective as well as from a technology perspective. Suggested implementation approach would generally require working through a phased approach such as:

- Phase 1: Group research, information exchange, and education on what a common portal environment would require organizationally and technically.
- Phase 2: Group deliberation, visioning, establishing governance, and planning towards the common approach.
- Phase 3: Corporate technology decisions and acquisition actions.
- Phase 4: Implementation –piloting and initial linkage; phased roll-out with full application integration.

This project will result in enhanced user productivity and efficiency through portal-driven individual customization for stream-lined access to functionality and self-service applications for employees, customers and partners. Examples include employee benefits, vacation time, loans, procurement, interactive training, expense processing, service desk, access to state services and associated case tracking, etc. The cost estimate for this activity is Pending Review.

IMPLEMENT ENTERPRISE SERVICES

Implementation of the “infrastructure” to support enterprise services within the common services-oriented architecture to be used across the State is included in this set of activities. This is a critical element of the ESA Common Solutions Framework as defined in Section 6.2.2. Similar to the portal implementation above, moving to common enterprise services has significant standardization issues from a people, culture, and organization perspective as well as from a technology perspective. Suggested implementation approach would generally require working through a phased approach such as:

- Phase 1: Group research, information exchange, and education on what a services-oriented environment would require organizationally and technically.
- Phase 2: Group deliberation, visioning, establishing governance, and planning towards the common approach.
- Phase 3: Corporate technology decisions and acquisition actions.
- Phase 4: Implementation –piloting and initial scope implementation; structure for on-going future scope areas such as ERP. Web services would be a primary approach for implementation, but other technological models need to be assessed such as messaging, enterprise service bus, open source versus proprietary, etc.

The cost estimate is Pending Review.

MIGRATE LEGACY SYSTEMS

This investment funds the upgrade of legacy applications to address immediate areas of risk to the State due to the age and condition of the application software and platform, or due to needs to reposition our application software off of legacy platforms in order to enable modernization initiatives to move forward. This initiative will include an analysis of the overall applications portfolio and identify the top risk areas. Projects will be authorized to plan and work through conversions, upgrades, and refreshes to stabilize the applications. Examples of efforts that may already be underway but need to continue to move forward include:

- Continue work underway to implement near-term enhancements to the legacy payroll system to automate EFT to minimize demands for check printing.
- Stabilize the email system versions and enhance overall enterprise capabilities including addressing a global address list and shared calendaring.
- Migrate current Lotus Domino applications to a standard enterprise solution pattern for web applications.

Estimate of costs for this project are Pending Review.

CREATE PROJECT REGISTRY AND REPORTING

This project creates a project registration and reporting system and identifies all required project measures and measurement methods and techniques/tools. Implement project management reporting systems and summary dashboards for OIMT.

Outcomes: Enterprise project management dashboard and reporting capabilities operational. This project depends on enterprise analytics capabilities. The cost estimate is Pending Review.

Figure 50 below identifies and organizes the needed initiatives for establishing the enterprise methodology, processes, and practices for software engineering, the common solutions framework, and the applications environment technologies. As described above, the initiatives are organized within the areas of governance, architecture and engineering, and projects.



Figure 50: Transition & Sequencing Plan to achieve Future State Software Development Environment

7.2.3.7

INFORMATION ASSURANCE AND PRIVACY DOMAIN

The IA domain represents the rules for maintaining information privacy, protecting information soundness, and ensuring information accessibility by mandating that there is accountability for the creation and maintenance of organizational policies, standards, and procedures to match the mandatory regulatory controls and that IT is properly aligned with these policies, standards, and procedures.

CURRENT STATE SWOT FOR THE INFORMATION ASSURANCE AND PRIVACY DOMAIN

Table 63 provides a description of the SWOT for this domain.

Table 63: SWOT for Information Assurance and Privacy Domain

Information and Privacy Domain	
Strengths	Weaknesses
<ul style="list-style-type: none"> • Knowledgeable Current Cyber Security Staff • Information Privacy and Security Council • Vulnerability Scans of ICSD Tier 1 – 2 Systems • Secure Web Gateway • Intrusion Prevention Systems • SEIM • Website App scanning • Virtual Firewalls between Departments • Enterprise SSL Certificate Available • Security Awareness Training (ICSD UH Only) • Spam Filtering for ICSD Lotus Notes • Two-Factor Authentication for Remote Access • Several ICSD IAM Policies • Partnership with MS-ISAC • Albert Project • DNSSEC 	<ul style="list-style-type: none"> • Any known weaknesses have been intentionally omitted for this public domain report
Opportunities	Threats
<ul style="list-style-type: none"> • Security as a Service model. • New skills and opportunities for current and new staff. • Collaborate with Local and Federal IA organizations. • Data Governance, defining the classification of data during the lifecycle. 	<ul style="list-style-type: none"> • Culture • Change • ‘Untrusted’ Insider • Unions Acceptability • BYOD • Compensation does not align with industry standards. • State IA/Cyber PDs

FUTURE STATE VISION FOR THE INFORMATION ASSURANCE AND PRIVACY DOMAIN

Hawai`i's future state vision is to offer world-class technology for citizen-centered, integrated, and secured services. This will be achieved by utilizing the Security as a Service model to provide secure end to end transformation of data for all its employees and citizens. Figure 51 offers a notional view of this future state vision.

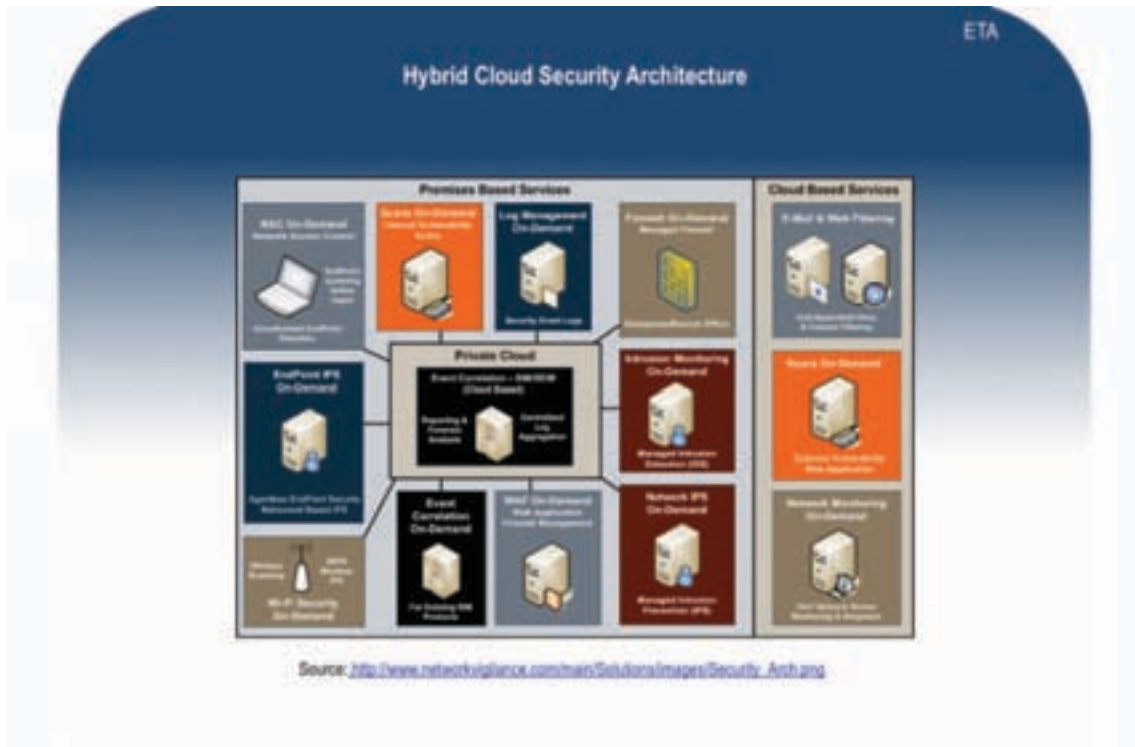


Figure 51: Future State Notional View of the Hybrid Cloud Security Architecture

The future state vision will view Security as a Service and will include the provision of security applications and services via the cloud either to cloud-based infrastructure and software or from the cloud to the customers' on-premise systems. This will enable enterprises to make use of security services in new ways, or in ways that would not be cost effective if provisioned locally.

The following security service categories will be of the most interest to the State of Hawai`i going forward:

- Identity and Access Management (IAM)
- Security Assessments
- Encryption
- Intrusion Management
- Business Continuity and Disaster Recovery
- Security Information and Event Management (SIEM)
- Data Loss Prevention (DLP)
- Network Security
- Web Security
- Email Security

Guiding Principles for the Information Assurance & Privacy Domain

1. Security is the first design consideration for all projects, products or services used by the State of Hawai`i.
2. Employees use a straightforward mechanism for gaining physical access to the work environment while providing electronic authentication to the appropriate electronic work environment.
3. Every device (server, computer, phone, wireless device, etc.), which connects to the States network, is considered a threat until credentials are validated.

Table 64 provides information that is based on “best practices” and “guiding principles” from the Technical Architectures Security Domains of North Carolina, Kansas, Oregon, and includes Security Principles, Security Identification and Authentication Practices, and Security Authorization and Access Control Practices. This information will supplement the OIMT Information Assurance and Cyber Security Strategic Plan (IA and CS) dated July 2012. This IA and CS Plan recommends both a strategic and tactical approach to IT security improvements that address 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 (3-5 year) strategic direction for the overall IA and CS Program.

Table 64: Security Principles for the Future State

Security Principles	
<p>1.1. Implementation of proven security policies, procedures, and controls greatly improves the security posture of an organization.</p> <ul style="list-style-type: none"> • Rationale: <ul style="list-style-type: none"> – Security policies are management directives for directing, governing, and regulating an organization’s security requirements. Security procedures and controls detail the processes required to implement the types and levels of protection necessary. – Successful security efforts depend on management and staff commitment to the protection of resources. – Security is only as strong as its weakest link. A lack of alignment opens opportunities for exploiting differences in commitment to and implementation of security processes and solutions. 	<p>1.4. Focusing on assuring data confidentiality, availability, integrity, and accountability ensures that State’s business objectives and security policies are satisfied. 1NIST Special Publication 800-33 – Underlying Technical Models for Information Security.</p> <ul style="list-style-type: none"> • Rationale: <ul style="list-style-type: none"> – The availability of data is essential in ensuring security. If data is inaccessible by authorized personnel important decisions or processes are delayed. Furthermore, confidence is easily lost when data cannot be accessed. – It is critical to ensure that data or systems have not been altered in an unauthorized manner. Corrupted data jeopardizes all business functions and requires that recovery processes be invoked when discovered. – Data confidentiality is more important than ever. Only authorized entities can be allowed to access data. Agencies must comply with privacy laws; failures in this area could result in fines or the need to notify the citizenry of data exposure
<p>1.2. Security controls for Hawai’i assets must be commensurate with their value and sufficient to contain risks to an acceptable level.</p> <ul style="list-style-type: none"> • Rationale: <ul style="list-style-type: none"> – Security is a business necessity with associated costs. Security expenditures should be a balance between cost and risk. – Qualitative or quantitative analysis techniques can be utilized to determine the proper amount of money to budget to protect assets. – Requirements for security vary depending on the information system, connection to other systems, sensitivity of data, and probability of harm. 	<p>1.5. Classifying information as either Public or Confidential helps to ensure compliance with legal and regulatory requirements and protects the privacy of citizens, businesses, and employees.</p> <ul style="list-style-type: none"> • Rationale: <ul style="list-style-type: none"> – By law, the general public has the right to request access to government information. If the information has been classified as Public, then the information can be made available according to established procedures. Access to Confidential information must be authorized on a strict “need to know” basis, in conformance with legal requirements for allowable access. – Confidentiality is to be determined in accordance with Hawai’i Public Records Law and all other applicable legal and regulatory requirements. – Occurrences of identity theft continue to rise. Public and confidential information must be secured and only revealed to requestors according to approved procedures. – Government has a responsibility to perform its duties as required by law; however these duties must be performed in a manner that ensures privacy.
<p>1.3. Comprehensive security programs are essential. Program operation should occur within a Statewide Security Office.</p> <ul style="list-style-type: none"> • Rationale: <ul style="list-style-type: none"> – Recent policy-based internal security assessments have shown the need to establish a security program or security office. Without a coordinated and on-going security initiative in place, the ability to adequately secure State’s IT assets over time becomes increasingly less possible. – Security programs should focus on accomplishing both the strategic and tactical aspects of security which include identifying and prioritizing security related needs, providing Department CIOs with professional guidance on the best ways to better secure an organization, developing and implementing a security training program for both IT and end users, and performing incident response activities. 	

Table 64: Security Principles for the Future State

Security Principles	
<p>1.6. Security is an integral part of all stages of the Software Development Life Cycle (SDLC). NIST Special Publication 800-27 – Engineering Principles for Information Technology Security.</p> <ul style="list-style-type: none"> • Rationale: <ul style="list-style-type: none"> – Security must be planned from the very beginning of the SDLC (i.e. Initiation Phase); otherwise securing the system is much more costly and inefficient. – Systems already in production (Maintenance Phase) must also be secured. – Even when systems are being retired (Disposal Phase) the proper actions must be taken to ensure the system is decommissioned securely – Designing for security from inception to implementation is significantly less costly than post-implementation attempts to retrofit security into applications. 	<p>1.9. Security risk assessments are effective in identifying vulnerabilities; once identified, actions can be taken to mitigate unacceptable levels of risk.</p> <ul style="list-style-type: none"> • Rationale: <ul style="list-style-type: none"> – A security risk assessment should be performed for all new and ongoing business systems. To determine the appropriate security requirements, departments should assess the value of system assets, risk exposure to those assets, and evaluate the mitigation measures and costs of protecting those systems. – Understanding the value of assets and associated risks is essential to determining the level of security required. – Security requirements should be included when designing or purchasing new applications. – Security requirements should utilize enterprise security resources where available
<p>1.7. Utilizing defense-in-depth and layered security approaches protects State’s information assets. NIST Special Publication 800-27 – Engineering Principles for Information Technology Security.</p> <ul style="list-style-type: none"> • Rationale: <ul style="list-style-type: none"> – The use of layered security controls across all aspects of network and application better protects resources from various security threats and vulnerabilities, thereby reducing the overall risk of a potential security incident. – The use of layered security controls and mechanisms better protects the asset if security controls are circumvented. – Protection of a resource is best accomplished by placing controls as close to the resource as possible. Additional layers of security help to protect the resource in the event that the primary means of protection fails for any reason. – Due to the diverse needs of the Hawai’i, a single security perimeter that protects the entire network and all related systems may not be feasible. A Security Zoning model will be developed, which is consistent with a layered security approach. 	<p>1.10. Security risk assessments are effective in identifying vulnerabilities; once identified, actions can be taken to mitigate unacceptable levels of risk.</p> <ul style="list-style-type: none"> • Rationale: <ul style="list-style-type: none"> – A security risk assessment should be performed for all new and ongoing business systems. To determine the appropriate security requirements, departments should assess the value of system assets, risk exposure to those assets, and evaluate the mitigation measures and costs of protecting those systems. – Understanding the value of assets and associated risks is essential to determining the level of security required. – Security requirements should be included when designing or purchasing new applications. – Security requirements should utilize enterprise security resources where available
<p>1.8. A security architecture that leverages an integrated set of enterprise services permits Hawai’i agencies to focus on the business goals rather than on the implementation of security.</p> <ul style="list-style-type: none"> • Rationale: <ul style="list-style-type: none"> – Utilize State’s infrastructure security services. – Integration of security services will enable interoperability and provide flexibility in conducting electronic business across and beyond the enterprise. – Integration will reduce the costs of protecting State’s resources. – Integration will increase the reliability of security solutions. 	<p>1.11. Maximum effectiveness and usability is ensured when security controls are located in the appropriate communication layer.</p> <ul style="list-style-type: none"> • Rationale: <ul style="list-style-type: none"> – Whenever security is required, the location in a communications protocol will have an impact. The impact may be on performance, reliance on an underlying network protocol, and on developers. Choosing the appropriate OSI layer in a communications protocol will maximize usability and minimize future changes. – Security services can have an impact on performance. The impact is minimized when security services are located at lower layers of a communications protocol. – Security services can have an impact on developers. For example, services provided at the transport layer have less impact on application programmers than services that run above that layer. – Security services can increase reliance on a network protocol. An appropriate choice depends on the communication requirements of the business system.

Table 64: Security Principles for the Future State

Security Principles	
<p>1.12. Formalized trust agreements between Agencies and/or external entities establish the criteria for conducting business securely.</p> <ul style="list-style-type: none"> • Rationale: <ul style="list-style-type: none"> – The security posture of external entities should be carefully evaluated prior to establishing network communications to conduct business-oriented transactions or processes. – Agreed upon minimum security standards must be verified by each entity annually. – Even after trusted communications are allowed, most often these communications occur via a dedicated circuit or VPN into a tightly controlled area of the network, which then relays the information into other portions of the internal network for further processing. 	<p style="text-align: center;">Security Identification and Authentication Practices</p> <p>2.1. Establish and follow industry accepted user-id and password management practices.</p> <ul style="list-style-type: none"> • Rationale: <ul style="list-style-type: none"> – User-ids and passwords are the most common means, but weakest form, of identification and authentication to Hawai'i services. When not managed properly, unauthorized access is possible. – User-ids and passwords must be carefully administered to ensure proper management (selection, aging, retirement, etc.) occurs. – Examples of good management practices include requiring that passwords consist of upper and lower case characters, special characters, and numerics, which are at least 8 characters in length; required password change on a regular basis (e.g. quarterly); required password rotation; disabling user-ids after three to five failed access attempts; not sharing user-ids and passwords with others; and not writing down passwords and hiding them in places that can be easily accessed.
<p>1.13. Systems are resilient to threats, vulnerabilities, and cyber attacks⁴ from both internal and external sources when properly designed and implemented.</p> <ul style="list-style-type: none"> • Rationale: <ul style="list-style-type: none"> – Zero-day vulnerabilities and Distributed Denial of Services attacks can occur at any time. Networks and systems must be designed such that operations can continue at acceptable levels. – Government entities are primary targets for cyber attacks and cyber warfare. – It is critical that the necessary actions are taken to protect information assets from internal as well as external attacks. Attacks or unauthorized access to information by employees can be very damaging, since they are more knowledgeable of the internal workings of an entity. Separation of duties and rotation of responsibilities can be used to protect against these types of attacks. Unannounced external third party reviews by security professionals are also very effective. 	<p>2.2. Use vendor neutral, standards-based, APIs for identification and authentication.</p> <ul style="list-style-type: none"> • Rationale: <ul style="list-style-type: none"> – Avoid proprietary identification and authorization APIs, which promote vendor lock-in. – Examples include NIST 800-63, Office of Budget and Management memoranda M-04-04, and GSA E-Authentication Technical Architecture standards.
<p>1.14. Obtaining superior levels of information assurance within Hawai'i government depends on the use of properly trained security professionals.</p> <ul style="list-style-type: none"> • Rationale: <ul style="list-style-type: none"> – The expertise level of hackers is ever increasing. In addition hacking tools are widely available. Therefore, even novice hackers can cause significant damage to IT resources with very little effort. In many cases these types of attack have tended to be disruptive in nature, however, there is a second generation of hackers emerging that are focused on releasing destructive viruses and worms, or stealing monetary funds from e-commerce systems. – Without the proper expertise and training, security implementations can be faulty and ineffective. 	<p>2.3. Encrypt user-ids and passwords during transmission. In addition, passwords must be stored in an encrypted or one-way hash format.</p> <ul style="list-style-type: none"> • Rationale: <ul style="list-style-type: none"> – User-ids and passwords are the weakest method of identification and authentication. Transmitting or storing this information in the clear places the associated systems or data at great risk of unauthorized access. – User-ids and passwords are easily captured when transmitted over IP networks. – Legacy applications, that transmit passwords in the clear when encapsulated over IP networks, must also be securely transmitted. – Security protocols such as SSL and IPSec and security solutions such as VPNs can be used to protect passwords in transit over networks. <p>2.4. Authenticate users prior to accessing controlled services or data.</p> <ul style="list-style-type: none"> • Rationale: <ul style="list-style-type: none"> – Allowing only authenticated users to access system resources protects those resources from inappropriate access. – Authenticating users is the basis for providing accountability while permitting access.

Table 64: Security Principles for the Future State

Security Principles	
Security Identification and Authentication Practices	
<p>2.5. Perform two-factor authentication when strong authentication is required.</p> <ul style="list-style-type: none"> • Rationale: <ul style="list-style-type: none"> – There are three accepted factors of authentication. The factors are “something you know” (e.g. password, passphrase, or PIN), “something you have” (e.g. token or smart card), and “something you are” (e.g. fingerprint, retina scan, or hand geometry). – The authenticating factors listed above are a means of proving your Hawai’i identity. Strong authentication is accomplished when any two of these factors are provided during the authentication process. 	<p>2.10. Follow PKCS #11 or PC/SC standards to interface smart cards to smart card readers.</p> <ul style="list-style-type: none"> • Rationale: <ul style="list-style-type: none"> – PKCS #11 from RSA is a widely accepted standard for integrating smart cards to applications supported by many vendors. – PC/SC is widely accepted for integration of smart cards on Intel platforms. <p>2.11. Follow the BioAPI when interfacing applications and biometric information other than fingerprint biometrics (e.g. voice, face, iris, etc.).</p> <ul style="list-style-type: none"> • Rationale: <ul style="list-style-type: none"> – A consortium of vendors, technology developers, researchers, VARs, and end-users developed the BioAPI. – The BioAPI offers interoperability over distributed environments with related APIs. – They include SAPI, HA-API, the telecom industry’s S100 (a standard architecture for developing computer-telephony applications), and JavaSpeech (a standard for speech recognition using Java). – Fingerprint biometrics must utilize standards specified by the NC SBI. – Refer to the BioAPI Consortium for specific references to the BioAPI standards.
<p>2.6. Public Key Infrastructure (PKI) initiatives must interoperate with other PKI solutions, utilize a Statewide approach, and conform to any relevant Hawai’i law or Statewide policy.</p> <ul style="list-style-type: none"> • Rationale: <ul style="list-style-type: none"> – The establishment of any PKI infrastructure is complex and must only be pursued after proper analysis and approvals have occurred. Agencies must leverage statewide services if they exist. – Collaboration and co-operation will be required to support security services across the enterprise. – A unified approach to a Public Key infrastructure enables the Hawai’i to respond to changing requirements and conditions. – A fragmented approach to a public key infrastructure will complicate administration and management of security across the enterprise 	<p>2.12. Follow the X.509v3 standard for Public Key Certificates.</p> <ul style="list-style-type: none"> • Rationale: <ul style="list-style-type: none"> – Public Key authentication must be based on Public Key Certificates. – Public Key Certificates must be based on the X.509v3 standard. – Despite the widespread acceptance of this standard, care must be taken when dealing with vendors. Projects should require proof of interoperability with existing or proposed enterprise implementations using X.509v3 certificates. Proprietary extensions to certificates could inhibit interoperability and should be avoided.
<p>2.7. Use industry accepted products for applications requiring digital certificate authentication.</p> <ul style="list-style-type: none"> • Rationale: <ul style="list-style-type: none"> – Certificates for web-based applications are provided by a number of major vendors. This approach is less risky and more cost effective than internal creation of digital certificates. – Use of proprietary certificate extensions must be avoided to ensure interoperability. 	<div style="background-color: #4db6ac; color: white; text-align: center; padding: 2px;">Security Authorization and Access Control Practices</div> <p>3.1. Only authorized users and devices are allowed to access State’s assets.</p> <ul style="list-style-type: none"> • Rationale: <ul style="list-style-type: none"> – Unauthorized access or use of Hawai’i property such as a network, infrastructure device, or service is a violation of OIMT policy. <p>3.2. Authorize users according to the principle of least privilege. Security controls must be established that verify this requirement is satisfied on a regular basis.</p> <ul style="list-style-type: none"> • Rationale: <ul style="list-style-type: none"> – Authorize users to the minimum set of resources appropriate to their role. – Authorizing users on least privilege minimizes the impact of security violations. – Authorizing users to a minimum set of resources necessary to their function makes it easier to establish accountability. – Authorization levels must be checked at least annually. A check on a monthly or quarterly basis is recommended
<p>2.8. Follow ISO/IEC 7816 standards for contact smart cards.</p> <ul style="list-style-type: none"> • Rationale: <ul style="list-style-type: none"> – ISO 7816/1-4 standards define the electrical resistance, positioning of electrical contacts, communication protocol between card and card reader, and command set recognized by smart cards. – They correspond roughly to the OSI layered model. – The command set defined by the ISO 7816-4 standard are included in whole or in part by most smart cards on the market. 	
<p>2.9. Follow ISO/IEC 14443 and 15693 and NIST Government Smart Card Interoperability Specification V2.1 standards for contactless smart cards.</p> <ul style="list-style-type: none"> • Rationale: <ul style="list-style-type: none"> – ISO 14443 standards, such as such as HID’s iCLASS and NXP’s, for contactless smart cards define the characteristics and communication protocols between contactless cards and the card reader. 	

Table 64: Security Principles for the Future State

Security Principles	
Security Authorization and Access Control Practices	
<p>3.3. All portable devices such as laptops, PDAs, smartphones, portable storage devices, other mobile devices, etc. must be scanned and cleaned of any viruses by up-to-date anti-virus software prior to connecting to State’s network.</p> <p>• Rationale:</p> <ul style="list-style-type: none"> – Employees, contractors, consultants, sales representatives, etc. can be exposed to viruses while not behind firewalls or protected by out-of-date anti-virus software. In many cases, this is how viruses are introduced into the internal network. 	<p>3.7. Mitigate security vulnerabilities that exist within various TCP/IP protocols.</p> <p>• Rationale:</p> <ul style="list-style-type: none"> – IP uses various protocols to provide and manage services. Due to the increased security requirements related to using the Internet, many of these protocols have security weaknesses that can negatively impact State’s network, especially when uncontrolled entry into State’s systems and networks is allowed. – Insecure and/or unauthorized network protocols must not be allowed to enter into State’s network. If use of network protocols is required either internally or externally then it must be tightly controlled or proxied from the Transaction Zone. Examples of insecure and unauthorized network protocols include NetBIOS, ICMP, and SNMP. – The use of IPX poses significant risks across State’s WAN. For that reason, routing IPX across State’s network is not acceptable.
<p>3.4. Remote access to the internal network over a public network must occur through a VPN.</p> <p>• Rationale:</p> <ul style="list-style-type: none"> – Accessing application services securely across public networks require encrypted communications. – Mobile workers (users that access the network from unpredictable locations), telecommuters and remote workers (users that routinely or occasionally work from a specific location), contractors, consultants, and vendors can easily expose userids, passwords, sensitive data, etc. over public networks. – VPN technology is not required for web-based applications (e.g. email and calendar) if the communications are secured via SSL. 	<p>3.8. Use encryption technologies to provide information assurance and recoverability.</p> <p>• Rationale:</p> <ul style="list-style-type: none"> – Sensitive information may be susceptible to unauthorized access or viewing unless protected by encryption technologies. – Many applications and operating systems create temporary files, which allow access to encrypted and even unencrypted information. Use of State supported encryption technologies ensure that this type of exposure is avoided. – Organizations must have the means to recover data encrypted by an employee after the employee leaves or when encryption keys are lost or stolen. Many products do not provide data recovery services. Data recovery techniques must be developed whenever data encryption is used.
<p>3.5. Remote access to the internal network must be properly authenticated.</p> <p>• Rationale:</p> <ul style="list-style-type: none"> – Remote access users must be minimally authenticated using proper userid and password management practices. Additionally, strong (i.e. two-factor) authentication can be implemented, using technologies such as tokens or smart cards, to further secure the remote access. – Direct dial-in connections to modems located in desktops provide back door access to the internal network. Agencies must provide secure solutions to mobile workers, telecommuters, remote workers, contractors, consultants, and vendors to avoid this situation. – Applications and file systems must be protected from unauthorized access. 	<p>3.9. Protect desktops, laptops, PDAs, smartphones, other mobile devices, etc. that are used by mobile and remote workers through the use of personal firewalls (hardware and/or software), encryption software, anti-spyware, and anti-virus software.</p> <p>• Rationale:</p> <ul style="list-style-type: none"> – Remote Access and telecommuting are becoming more and more common and therefore the data located on the devices used during remote access must be protected. – Hackers looking for easy targets frequently scan remote users. These hackers may commandeer home systems to launch attacks, to destroy data, or to obtain access to the user’s work network. – Personal firewalls, desktop encryption, virus protection, anti spyware, and anti-virus software are a means of protecting remote users. End-users must be adequately trained in the use of these products. – Use of fully functional purchased software is recommended for this critical function. Shareware products are generally not intended for wide spread use by a Department, and in many cases this may be in violation of the software license agreement. – Centrally configured firewalls and desktop encryption simplify the remote user’s need to manage potentially confusing products. – Some firewall/VPN products provide configuration and administration support for personal firewalls.
<p>3.6. Virtual Private Network (VPM) solutions must utilize either SSL or IPSec technology.</p> <p>• Rationale:</p> <ul style="list-style-type: none"> – VPN solutions must be either SSL or IPSec based. While SSL is an open standard and therefore preferred, there may be times where IPSec would be a better choice based on the function being performed. IPSec, while a more proprietary solution, is also a recognized de facto standard. – IPSec is an extension to the IP communications protocol, designed to provide end-to-end confidentiality for packets traveling over the Internet. – IPSec works with both the IPv4 and the IPv6 protocol 	

Table 64: Security Principles for the Future State

Security Principles	
Security Authorization and Access Control Practices	
<p>3.10. Secure transmission of sensitive data in both wired and wireless environments.</p> <p>• Rationale:</p> <ul style="list-style-type: none"> – Data in transit to and from the enterprise must be protected in compliance with legal requirements for confidentiality and privacy. – Web-enabled applications must protect confidential or critical data from unauthorized access. – Use secure server-to-server communication to protect confidential or critical data transmissions. – Examples of PII and other sensitive data include SSN, Dates of Birth, Credit Card numbers, health related information, etc. – Examples of security protocols include SSL, VPN, Secure FTP, and WiFi Protected Access 2 (WPA2). 	
<p>3.11. Use Secure Sockets Layer (SSL) or Transport Layer Security (TLS) when secure communications between the web client and server is required.</p> <p>• Rationale:</p> <ul style="list-style-type: none"> – SSL/TLS is the most commonly supported protocol for communication between a Web Server and a browser. – SSL/TLS authenticates the Web Server and optionally authenticates the user. – Current implementations allow for client authentication support using the services provided by Certificate Authorities. 	
<p>3.12. Cryptography must be based on open standards and utilize a key of sufficient length to adequately protect data.</p> <p>• Rationale:</p> <ul style="list-style-type: none"> – Cryptosystems and their associated cryptographic algorithms must be publicly reviewed and accepted by the security industry prior to any production usage, otherwise the validity and strength of the cryptosystem cannot be considered as a viable solution. – The key lengths for these algorithms can vary; therefore the selection of an appropriate key size is critical to adequately protect data. In other words, select a key length large enough to ensure that the “work factor” (i.e. time and effort) required to defeat the protection is greater than the value of the “material being protected”. – Cryptography must be based on open standards and utilize a key of sufficient length to adequately protect data. – The Cryptography Categories and Standards Table highlights open, industry accepted, cryptographic standards. 	

Cryptography Categories	Cryptography Algorithm Standards
Symmetric (“Shared” Secret Key)	AES, 3DES, IDEA, RC4, RC5, RC6, Blowfish, Twofish
Asymmetric (Public Key / Private Key)	RSA, ECC, El Gamal, DSA
Hash Functions	MD5, SHA-1, SHA-224, SHA-256, SHA-384, SHA-512

SECURITY DEVICES SUB-DOMAIN

Security defines the methods of protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide integrity, confidentiality and availability.

Software is available and used by a certification authority (CA) to issue digital certificates and ensure secure access to information. The evolution of Public Key Infrastructure (PKI) is based on the verification and authentication of the parties involved in information exchange. Table 65 provides a description of this sub-domain.

Table 65: Security Devices Sub-Domain Description

IA Security Sub-Domain	Sunset Products / Standards	Current Supported Products/ Standards	Preferred Products / Standards	Emerging Trends
Firewalls	Stateful Inspection FW	Cisco Virtual FW Checkpoint NG	Host and network based deep packet inspection application layer firewall	Cloud based web application firewalls, Distributed web application firewalls
Virtual Private Networks (VPN)	Client based VPN	Vendor Specific Checkpoint VPN Cisco VPN	IPSec VPN SSL VPN	mVPN – mobile VPN based on Host Identity Protocol (HIP)
Intrusion Detection System (IDS)	Network based IDS	Cisco	IDPS – Intrusion Detection and Prevention System	Stack based intrusion detection systems
Intrusion Protection System (IPS)		Cisco	IDPS – Intrusion Detection and Prevention System	Integrated Network/Wireless/Host based prevention in network.
Anti-Virus	End user controlled A/V lacking central update capability	Symantec Endpoint	Endpoint protection against zero day threats, antiphishing, antispam, web based protection, and malware removal	Integrated Anti malware/virus for mobile devices. Central A/V deployment and push, Cloud anti-virus
Wireless	Rogue or standalone WiFi deployments	Secure WiFi integration with LAN authentication	WIPS - Wireless Intrusion Prevention System	WiFi intrusion prevention and rogue AP detection
Authentication and Authorization	Departmental authentication systems	Single Active Directory for State, LDAP v3, Kerberos 5	NIST RBAC (Role Based Access Control) model, FIPS 201	Identity Management with single sign on, dual factor authentication and defined privilege classes within enterprise

PRIVACY SUB-DOMAIN

Where security focuses on protection of the network from an outside in perspective, the privacy sub domain is concerned with the protection of information that could compromise an individual, system, or the State as a whole. Personally Identifiable Information (PII) is an example of data that must not be returned in a common query or data set or leaked outside the State. Table 66 provides a description of the Privacy Sub-Domain.

Table 66: Privacy Sub-Domain Description

IA Security Sub-Domain	Sunset Products / Standards	Current Supported Products/ Standards	Preferred Products / Standards	Emerging Trends
Data Loss Prevention (DLP)	N/A	N/A	Network DLP Data in Motion DiM Storage DLP Data at Rest -DaR Endpoint DLP Data in Use - DiU	Content inspection system to prevent transmission of PII or other sensitive data
Encryption	Departmental encryption solutions for data at rest	Encryption of data in transit and at rest. 3DES, AES-128	AES-256 bit encryption	Full Disk Encryption extended to portable media devices. AES-256
IA / Risk Assessment	N/A	Risk IT, CobiT, ISO 27000	COBIT FISMA	3rd party assessment and creation of risk management plan

ETA TRANSITION AND SEQUENCING PLANNING SUMMARY FOR THE INFORMATION ASSURANCE AND PRIVACY (IA&P) DOMAIN

Transition and sequencing is based upon a thorough assessment of the current security posture. This assessment is a critical input to the development of a sequencing plan that organizes all of the major elements of IA&P as sub-projects within the larger initiative.

This list of initiatives and activities was created in conjunction with the Information Assurance and Privacy Working Group to provide a road map and project phasing to address a comprehensive integrated capability.

The OIMT Information Assurance and Cyber Security Strategic Plan (IA and CS) dated July 2012 indicates that “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 proactively remediate vulnerabilities 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, now it is used while valid, during any archival or retention requirements, through 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 access – by authorized users – to the right information, 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, State must deploy secure, reliable, capacious, and diverse access solutions that allow users access to needed information from “anywhere” and at “anytime.”

- 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’ presented 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 4 phases to be completed over the next four years of the current administration.”

IMPLEMENT NETWORK DATA LOSS PREVENTION (NDLP)

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. This investment includes implementing 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. Benefits of this initiative include:

- Prevent network data loss regardless of protocol
- Monitor and inspect all TCP protocols – SMTP, HTTP/S, FTP/S, IM, P2P, and other TCP
- Inline MTA inspects and controls email messages
- ICAP integration controls Webmail, Web 2.0, and FTP, including SSL-enabled sessions
- Policy-based email encryption secures communication and ensures regulatory compliance

The estimate for this investment is Pending Review.

CREATE AND IMPLEMENT IT SECURITY POLICY

This investment supports 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. The estimated cost for this activity Pending Review.

IMPLEMENT DATA AT REST (DAR) ENCRYPTION

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. With the increasing utilization and usage of mobile devices, including

State owned laptops, it is essential that Data at Rest be encrypted. The estimate for this project is Pending Review

INITIATE SERVER CONFIGURATION STABILITY MONITORING

This investment helps identify alterations in operating system, database, applications, and security configurations that result in State’s assets being more susceptible to threats. This includes the ability to examine, evaluate, and report on the level of compliance with security hardening requirements (often referred to as Security Technical Implementation Guides, or STIGs) that are established for equipment and systems across State’s infrastructure. This provides mitigation for exploiting vulnerabilities in devices connected to networks and connecting non-compliant devices to networks without compliance monitoring. The cost estimate for this activity is Pending Review.

INITIATE AUTOMATED SECURITY CONFIGURATION COMPLIANCE MONITORING AND REPORTING

This investment helps identify alterations in security configurations that result in State’s assets being more susceptible to threats. This will provide the ability to examine, evaluate, and report on the level of compliance with security hardening requirements (often referred to as Security Technical Implementation Guides, or STIGs) that are established for equipment and systems across State’s infrastructure. The cost estimate for this is Pending Review.

IMPLEMENT PRIVACY PROGRAM STAFFING AND SENSITIVE INFORMATION PROTECTION IMPROVEMENTS

This investment enables improvements to be made at all levels within State by supporting targeted Privacy Program staffing increases and the development of improved information protection policies and procedures. This investment will be approximately Pending Review.

IMPLEMENT ENTERPRISE SECURITY OPERATIONS CENTER(S)

This investment supports State’s ability to monitor threats presented by data loss from mission critical systems resulting from misconfigurations or unauthorized data transfers initiated by malicious actors. The lack of appropriate tools and personnel to identify hostile traffic, vulnerabilities that can be exploited and non-compliant configurations that expose the State to hostile parties could result in significant disruption of network access and services and of destruction and abuse of sensitive data. The estimate for this set of activities is Pending Review.

IMPLEMENT COMPUTER INCIDENT RESPONSE CENTERS (CIRCS)

This investment improves computer incident detection, reporting, prioritization, response, collaboration, and resolution capabilities throughout the Department. Currently, known incidents take too long to detect, report, respond and collaborate at the State level. Incident reporting arrives too late for appropriate preventative actions to take place. All of this can pose a risk to much higher incident management costs than required; lack of uniform handling of detection, reporting, response, collaboration and resolutions; and, incident-based legal action failing due to inappropriate forensic evidence collection. The cost estimate for this effort is Pending Review.

IMPLEMENT ENTERPRISE PENETRATION TESTING CAPABILITY

This investment defines, documents, and implements 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. These activities total approximately Pending Review.

COMMON STANDARDS FOR PROTECTING PRIVACY AND OTHER SENSITIVE DATA

This investment funds the development and promulgation of common standards for protecting privacy and other sensitive information. This initiative will cost approximately Pending Review.

IMPLEMENT A SECURE APPLICATIONS TESTING PROGRAM

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. Application security should be built-in not added "after market" (much like airbags in cars). Attempting to add security to an application after the requirements have been fulfilled and the application has been developed is rarely successful and typically creates vulnerabilities that cannot be addressed within the application hence incur significant infrastructure costs to remediate. Without a robust application testing regimen, the State is at risk of continuing to deploy applications into the mission-dependent environment that are making the information technology environment less secure rather than more secure and thereby putting the mission data and mission at risk. Further, a lack of uniform testing across all development shops at the State exposes all mission data stores to the vulnerabilities in one insecure deployment. Vulnerabilities could include input validation, cross site scripting, SQL injection, cookie modification, code execution, buffer overflow, URL manipulation, and authentication bypass. The estimate for this initiative is Pending Review.

IMPLEMENT AN ENTERPRISE IDENTITY MANAGEMENT SOLUTION

This investment establishes a standard solution for management of user account identity and authorized roles and access permissions integrated with standard user directory services and enterprise services for authentication. The expectation is that an industry standard commercial-off-the-shelf (COTS) application software package will be selected and procured and implemented. The estimate for this initiative is Pending Review.

IMPLEMENT NETWORK-BASED NETWORK ACCESS CONTROL (NAC)

This investment implements a network-based solution to prevent unauthorized systems from inappropriately accessing State's network(s). A significant risk to all missions dependent on the information technology that supports them is a lack of network-based network access control (NAC). Without network-based NAC, any hostile party can connect any device to the network and attack it and the sensitive and PII data on it and all the devices connected to the network. Selected and deployed adequate network-based NAC solutions will be installed 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. The estimate for this initiative is Pending Review.

IMPLEMENT A SECURE WIRELESS ACCESS SOLUTION

This investment will support the selection, development, implementation, and migration to a standardized State-wide wireless access solution(s) for both remote and local area network access. With the advancement into wireless access solutions to support mission-needed remote and local wireless access to State network assets, servers and data, the State is at risk of having a diversified environment of solutions implemented across the various departments, divisions, branches, and offices leading to costly adaptations for secure configurations across the multitude of products. This initiative will select, develop, implement, and migrate pilot organizations to a State-wide wireless access solution performed incrementally in coordination with all "Remote Access" related initiatives/projects. The estimate for this initiative is Pending Review.

IMPLEMENT NETWORK END-TO-END ENCRYPTION SOLUTION

This investment will support the design and implementation of secure internal network communications between mission critical servers and locations. Information Exposure, Unauthorized Use, Unsecured Operating Environments, Loss of Public Confidence, Exposure to Legal Action an . Data traveling across the State network is available for snooping and capturing by hostile parties that connect locally or remotely to the network. A significantly worse risk lies in the traffic that leaves segments of State’s network to reach field offices or other legitimate parties (e.g. remote teleworkers) that is not encrypted while in transit. This information includes login and password information, sensitive and PII data. Hostile parties can read this unencrypted and abuse the credentials and sensitive information, potentially to embarrass State or to interrupt and destroy its network and data. The estimate for this initiative is Pending Review.

Figure 52 and Figure 53 represent the roadmap for achieving future State vision for the Information Assurance and Privacy Domain.

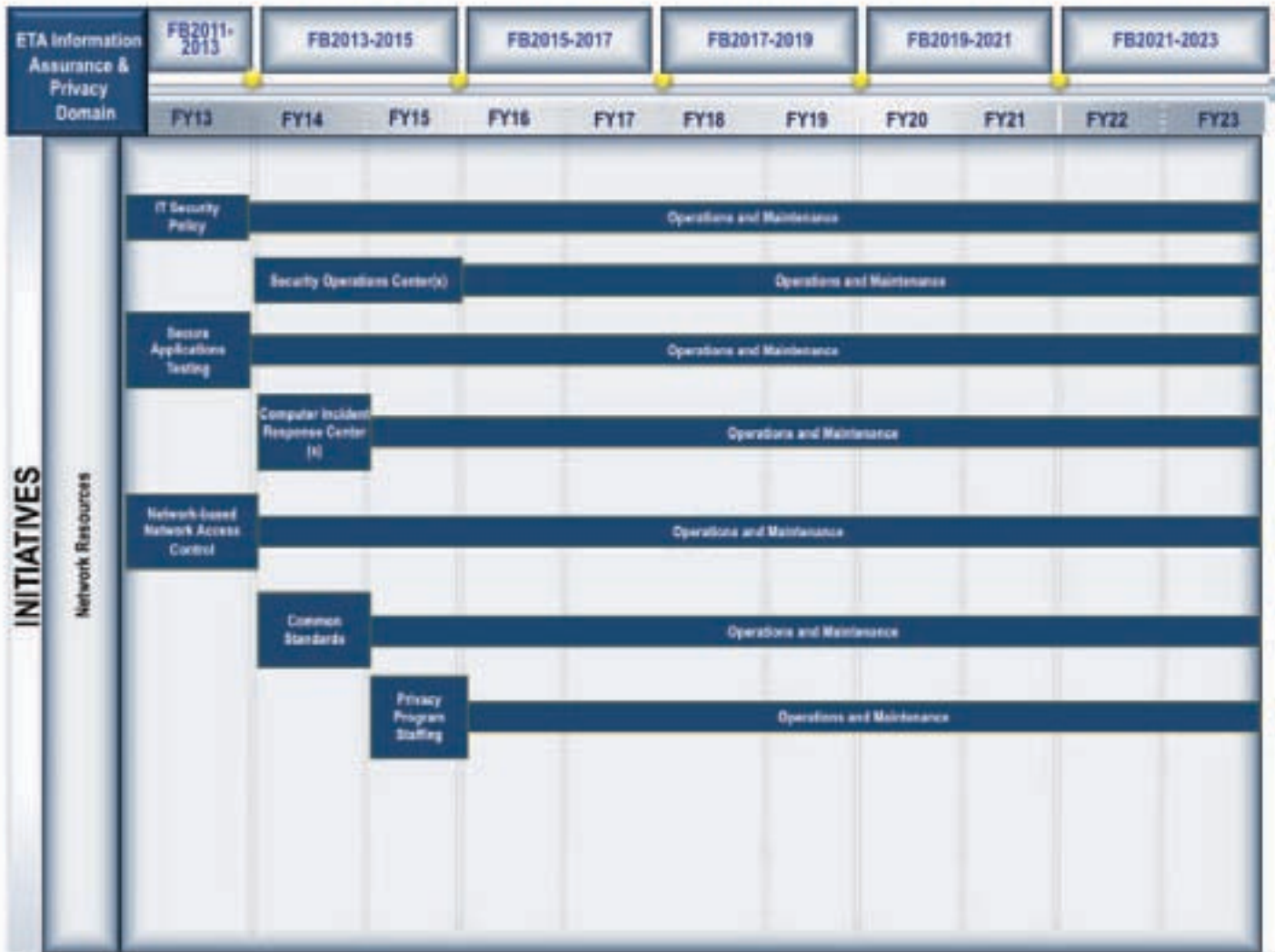


Figure 52: Roadmap for Achieving Future State Vision for the Information Assurance and Privacy Domain (1 of 2)

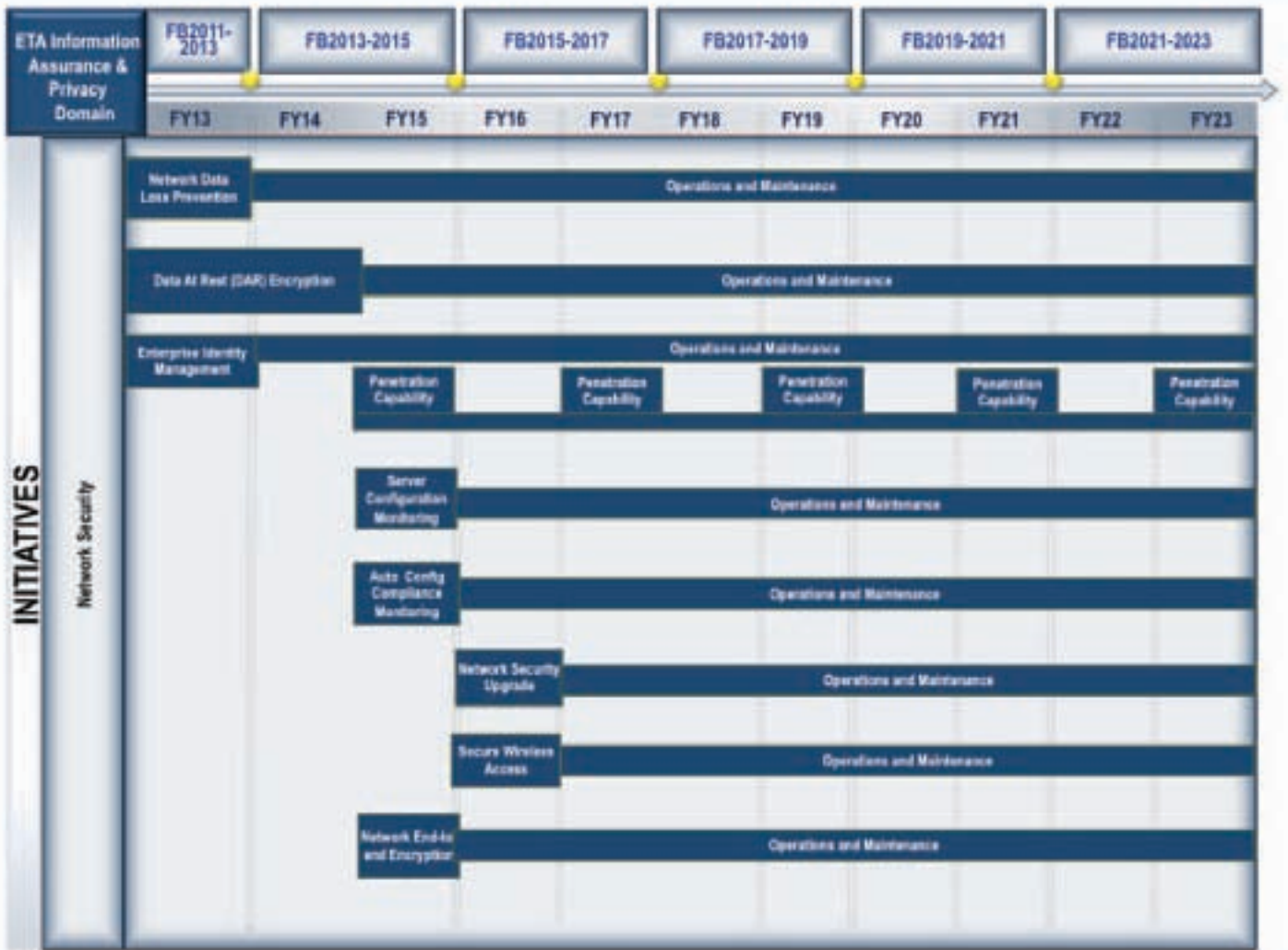


Figure 53: Roadmap for Achieving Future State Vision for the Information Assurance and Privacy Domain (2 of 3)

Information Assurance and Privacy Domain Addendum Information

http://idea.hawaii.gov/userimages/accounts/90/907159/panel_upload_18993/SupplementalAddendumIA.pdf



8.0

**ENTERPRISE LEVEL TRANSITION
AND SEQUENCING PLAN**

8.0 ENTERPRISE LEVEL TRANSITION AND SEQUENCING PLAN

This section provides a high-level view of the transition and sequencing activities for the enterprise while Appendix A provides a detailed view of the transition and sequencing actions from the LOB perspective.

8.1 APPROACH TRANSITION AND SEQUENCING PLANNING

The State's EA characterizes and documents the current state and more importantly defines the standards that will create the desired future state. The T&S Plan is the "how" this transition or transformation occurs in a logical and sequenced or prioritized manner. The T&S process is depicted in Figure 54.

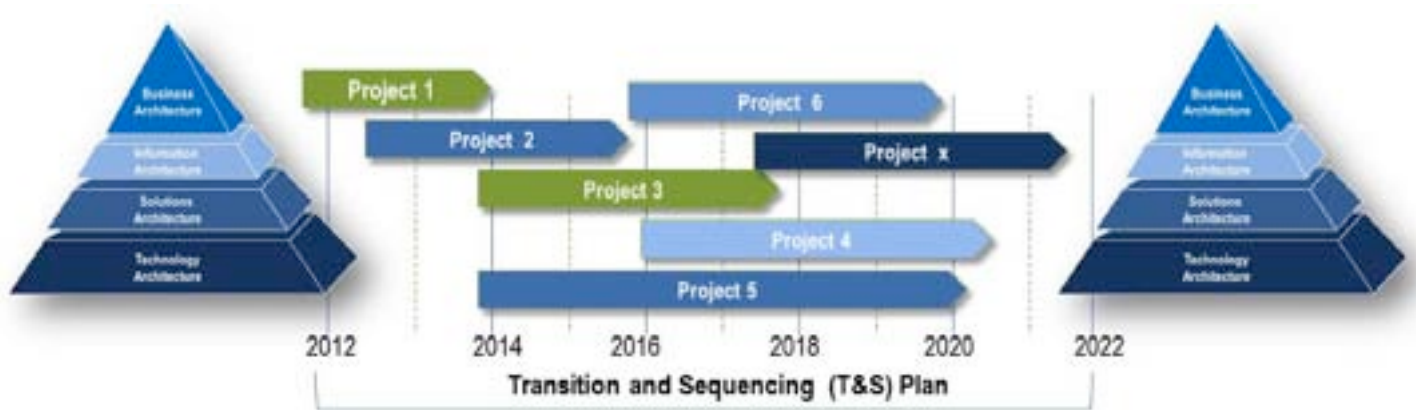


Figure 54: T&S Process

When the T&S Plan is then coupled with the requirements defined in the IT investment Portfolio Management (PfM) Methodology (and its accompanying toolset) along with IT governance and the defined OIMT management practices, the resulting roadmap of activities and projects ensure that IT investments efficiently and cost effectively support the delivery services and programs to all stakeholders (e.g., people of Hawai'i, citizens, business entities, cities, counties, State employees, State government) in a manner they want/need in terms of quality, timeliness, reliability, and transparency. This T&S Plan covers ten years and each year the T&S Plan will be reviewed updated on at least an annual basis.

8.2 ENTERPRISE LEVEL TRANSITION AND SEQUENCING ANALYSIS

The progress of the transition is characterized using a number of perspectives or views. These views summarize the key investments and their resulting projects and activities to ensure alignment with the overarching goals and objectives identified in the future state vision defined in the EA. The details that create these views are maintained in the PfM toolset.

The views also offer perspectives that assist OIMT, CIO, CIOC, and ELC in evaluating new investments to ensure they are aligned with the strategic direction set for IT as part of the Strategic Plan and the EA and in monitoring the progress of the transition to the future state definition. As an evaluation tool, the views should be "refreshed and regenerated" on a regular basis.

The following sections describe a sample of the views that will be used in the evaluation and assessment of IT investments. The actual tables and graphics depicting these views are provided in Appendix C.

8.2.1 STRATEGIC PORTFOLIO VIEWS

This section details the description of the various portfolio views and notional graphic of how the specific views work.

8.2.1.1 INVESTMENT STATUS BY LOB

IT investment dollars are aligned between operations and maintenance (O&M) or Steady State (SS) activities and Development, Enhancement, and Modernization (D/M/E) projects and initiatives by LOB.

This view indicates the portfolio's imbalance in terms of operating and maintaining the more than 700 existing (and often duplicative) systems and their supporting infrastructures. This alignment between O&M or SS and D/M/E indicates that the cost operating and maintaining the current environment is based on technology that is inefficient and ineffective in its application at the enterprise level. Going forward, the funding must be realigned to move more investments to D/M/E (or actively and expeditiously retiring current systems and technology in O&M or SS) especially in the next ten years in order to transform the environment. The OIMT, CIO, CIOC, and ELC should use this view to monitor the investment results.

8.2.1.2 ENTERPRISE SUPPORT SYSTEMS AND ENTERPRISE SERVICES

The EA and specifically the ESA for the State identifies enterprise systems and services that support multiple LOBs (and Departments) due to the shared nature of the activity. As IT investments are identified/architected/ proposed this view supports CIO, CIOC, and/or ELC in making Selection decisions as part of PFM by highlighting the number of LOBs that benefit from the investment, amount of funding, against timeframe that IT solutions are projected to attain economies of scale and cost reduction for the State (based on business case and other provided information in the PFM toolset). This view also supports sequencing decisions.

This view is based on the biannual budget submissions for FY2014. From this view the enterprise investments are substantially more effective in the achievement of the EA future state vision.

8.2.1.3 ESA AND ETA INVESTMENTS

This view provides insight into the distribution of investments between the ESA and ETA.

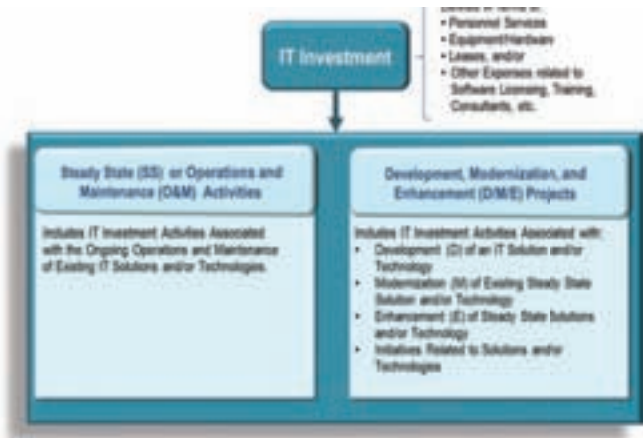


Figure 55: Investment Components

8.2.1.4 EA COMPLIANCE

The enterprise technologies provides the opportunity to make informed decisions on IT activities and investments that are in compliance with the defined technology domains, standards and products outlined in the EA. This understanding of investments and their alignment with the EA help achieve faster deployment with fewer complexities at a lesser cost to the taxpayer.

This view focuses the attention of OIMT, CIO, and CIOC on current investments that should be reviewed as part of the Control/Evaluate Phase for retirement or recommendation regarding D/M/E. This view used in conjunction with the Enterprise Support Systems and Enterprise Services view also supports project sequencing.

8.2.1.5 STRATEGIC VALUE

The strategic value view depicts where IT investment for the State is positioned to achieve the strategic objectives as outlined by the EA (and its alignment to the New Day Plan). This view provides the means for the CIO, ELC, Governor, and Legislature to make informed decisions in moving funding of IT from investment to investment to close business or functionality gaps that are inhibiting fulfillment of goals and objectives.

All investments with low compliance with regard to strategic objectives and minimal enterprise utility are evaluated for retirement while all investments with high enterprise utility and extensive compliance with strategic objectives should be fully funded.

8.3 SPECIFIC PROJECTS AND ACTIVITIES

This view communicates the individual investment initiatives that are required to implement the future state EA. Initiatives are organized within each architectural layer of the EA. A high level Gantt chart depicts all the initiatives and their timing and dependencies by Fiscal Year.



9.0 CONCLUSION

9.0 CONCLUSION

Finally, the EA and the defined projects, initiatives, and activities will serve as a resource and guide for the State's IT practitioners within the LOBs and Departments as they make tactical and strategic decisions about the development, modernization, enhancement, maintenance, retirement of technology. It also provides a basis for the evaluation of technology plans by the Chief Information Officer (CIO), Office of Information Management and Technology (OIMT), Department leadership and IT management, Executive Leadership Council (ELC), and CIO Council (CIOC) and IT Steering Committee who are ultimately responsible for ensuring:

- State government is costeffectively and efficiently managing all resources (e.g., investments, revenues, employees, IT) and delivering services and programs to all stakeholders (e.g., people of Hawai`i, citizens, residents, businesses, cities, counties, State employees, State government, business partners) in a manner they want/need; and
- operating in an aligned, streamlined, and integrated manner so that stakeholders' service expectations and information needs are met in terms of quality, timeliness, reliability, and transparency.

