State of Alaska

Department of Health and Social Services

Enterprise Roadmap Phase II

Contract Number 0610106
Amendment #7

Version 1.4
Date: May 17, 2013

Contents

1.0 EXECUTIVE SUMMARY 1
1.1 VISION 1
1.1.1 ROADMAP PHASE I 1
1.1.2 ROADMAP PHASE II 2
1.2 CREATING THE INFRASTRUCTURE TO MEET EVOLVING BUSINESS NEEDS 3
1.2.1 ALIGNMENT WITH MITA AND CMS SEVEN CONDITIONS AND STANDARDS 3
1.3 SUCCESSFUL PROCESS CHANGE REQUIRES CULTURAL CHANGE 4
1.4 EXPECTED OUTCOMES 4
1.5 EVALUATION AND MEASUREMENT 5
1.6 RECOMMENDATIONS AND LEVERAGING THE ROADMAP 5
1.6.1 ESTABLISH NECESSARY GOVERNANCE AND BLUEPRINT FOR DEPARTMENT ARCHITECTURE 5
1.6.2 MAKE NECESSARY CHANGES TO THE PROCUREMENT PROCESS TO SUPPORT THE MIGRATION TO SHARED SERVICES AND ARCHITECTURE 5
1.6.3 DEVELOP THE TECHNICAL INFRASTRUCTURE TO SUPPORT THE IMPLEMENTATION OF A SERVICE ORIENTED ARCHITECTURE 6
1.6.4 RECOMMENDATIONS FOR SHARED SERVICES IMPLEMENTATION 6
1.6.5 CASE MANAGEMENT AS A SHARED SERVICE 8
1.6.6 ELECTRONIC DOCUMENT MANAGEMENT SYSTEM AS A SHARED SERVICE 8
2.0 REVIEW TEAM AND SOA GOVERNANCE 10
3.0 ENTERPRISE SERVICE BUS 13
3.1 IMPLEMENTING BIZTALK TO PROVIDE FULL ESB FUNCTIONALITY 13
3.1.1 REQUIRED BIZTALK UPGRADES 13
3.2 ESB'S ROLE IN SUPPORTING SHARED FUNCTIONALITY 15
3.3 ESB CONNECTIVITY 16
3.4 SHARED COMPONENTS 17
3.4.1 BUSINESS RULES ENGINE 18
3.4.2 BUSINESS ACTIVITY MONITORING 19
3.4.3 BUSINESS PROCESS WORKFLOW ENGINE 19
3.5 ESB IMPLEMENTATION PLAN 20
3.5.1 ASSUMPTIONS 20
3.5.2 MAJOR IMPLEMENTATION TASKS 20
3.6 POST IMPLEMENTATION MAINTENANCE AND OPERATIONS 22
3.6.1 SERVICES MANAGEMENT 22

3.6.2 SERVICE PERFORMANCE MONITORING 22
4.0 MASTER CLIENT INDEX 24
4.1 ESTABLISHING THE MCI AS THE REPOSITORY OF THE GOLDEN RECORD 24
4.2 MCI'S ROLE IN THE HIE 25
4.2.1 MCI'S ROLE IN MYALASKA AUTHENTICATION AND VALIDATION 26
4.2.2 CONNECTING PUBLIC HEALTH REGISTRIES, MMIS DATA WAREHOUSE, MCI, AND HIE 29
4.3 MCI INTEROPERABILITY IMPLEMENTATION PLAN 30
4.3.1 ASSUMPTIONS 30
4.3.2 MAJOR IMPLEMENTATION TASKS 30
5.0 SHARED FUNCTIONALITY 32
5.1 SHARED FUNCTIONALITY AND MITA 33
5.2 COMMONLY DEPLOYED SHARED FUNCTIONALITY/SHARED SERVICES 34
5.2.1 CASE MANAGEMENT AS A SHARED SERVICE 35
5.2.2 ELECTRONIC DOCUMENT MANAGEMENT SYSTEM AS A SHARED SERVICE 36
5.3 SHARED FUNCTIONALITY/SERVICES HOSTING 37
5.4 SHARED FUNCTIONALITY/SHARED SERVICES ARCHITECTURE 39
5.5 PRIORITY SHARED FUNCTIONALITY/SERVICES 39
5.5.1 PERSON LOOK-UP SERVICE 40
5.5.2 ADDRESS VALIDATION SERVICE 40
5.5.3 ADDRESS LOOK-UP SERVICE 40
5.5.4 PERSON ADD/UPDATE SERVICE 40
5.5.5 ADDITIONAL SHARED FUNCTIONALITY 41
5.6 SHARED FUNCTIONALITY/SHARED SERVICES IMPLEMENTATION PLAN 43
5.6.1 ASSUMPTIONS 43
5.6.2 MAJOR IMPLEMENTATION TASKS 43
6.0 SUCCESSFUL PROCESS CHANGE REQUIRES CULTURAL CHANGE 46
7.0 OUTCOMES 47
8.0 EVALUATION AND METRICS 48
9.0 RECOMMENDATIONS AND LEVERAGING THE ROADMAP 49
9.1 SOA GOVERNANCE 49
9.2 BIZTALK ENTERPRISE SERVICE BUS 49
9.3 ENTERPRISE-LEVEL COMPONENTS 50
9.4 MULTIVUE MCI 50
9.5 SHARED FUNCTIONALITY/SERVICES 51

9.5.1 CASE MANAGEMENT AS A SHARED SERVICE 51
9.5.2 ELECTRONIC DOCUMENT MANAGEMENT SYSTEM AS A SHARED SERVICE 52
9.6 LEVERAGING THE ROADMAP 53
9.6.1 ROADMAP PHASE I 53
9.6.2 ROADMAP PHASE II 53
9.6.3 NEXT STEPS 54

Tables

Table 1: Change Record iii
Table 2: SOA Terms and Definitions 18
Table 3: MITA-based Logical Architecture 33
Table 4: Common Shared Services Required by Recent EIS, HIE, and MMIS Implementation Procurements 38
Table 5: Evaluating the Results of Implementing Roadmap Recommendations 48

Figures

Figure 1: Internal ESB Components 17
Figure 2: SOA – Key Concepts 17
Figure 3: MCI and HIE Integration 26
Figure 4: High-Level Shared Services Architecture 39

Document Control

Table 1: Change Record

Date	Author	Version	Description
3/21/13	Cognosante Team	0.6	Initial draft of shared functionality content
3/29/13	Cognosante Team	0.7	Addition of ESB content
4/26/13	Cognosante Team	1.0	Draft of Complete Roadmap Phase II
5/3/13	Cognosante Team	1.1	Updated based on DHSS feedback
5/10/13	Cognosante Team	1.2	Updated based on DHSS feedback
5/15/13	Cognosante Team	1.3	Updated based on DHSS feedback
5/17/13	Cognosante Team	1.4	Updated based on DHSS feedback

1.0 EXECUTIVE SUMMARY

1.1 Vision

The Department of Health and Social Services (DHSS) is evolving from a traditional model of program-centric administration based on division-level technology needs, to a Department-level, enterprise-wide architecture based on the leveraging of shared technology and business components. The result for DHSS is a modular, flexible Health Information Technology (HIT) architecture, designed to allow the Department to meet current and future business needs, with a focus on lower cost, increased efficiency, and improved service.

In the current model, each Division acts independently to procure, implement, and operate the technology necessary to support day-to-day operations. The unintended results, over time, are multiple siloed systems with redundant technical components, business capabilities, and duplicate data storage. These siloed systems present a barrier to interoperability and efficiency across the Department while increasing redundancy and cost.

The envisioned To Be model for Alaska, as outlined in the Alaska Roadmap Phase I document, is a gradual transition to a Shared Services model, built on an enterprise-level service-oriented architecture (SOA). The initial Roadmap document provides a high-level conceptual architecture of the shared services environment, as well as discussion of the policies and applicable federal and state Information Technology (IT) standards that support the implementation and growth of a shared services model.

To support the implementation of the SOA-based technical infrastructure, Alaska must undergo a corresponding business process and cultural change to support the transition to a modular, shared service environment. Division business and technology leaders will need to embrace sweeping changes, ranging from changes in how technology is procured, to alignment of business processes and process model flows, to testing and change management.

The result for Alaska is the transition from a Division-centric IT approach to one that aligns with the technical and business needs across the Department, supporting the implementation and sharing of common components across Divisions. The full implementation of the Roadmap establishes the following guiding principles and strategies:

- Maximize use of Department HIT expenditures through reuse of shared technology and business services, allowing functionality and services to be exposed for reuse
- Alignment of business needs and business processes across Divisions
- Migration to a DHSS-enterprise, consumer-centric focus, moving away from siloed, program-specific perspectives
- Migration toward an enterprise SOA consistent with Medicaid Information Technology Architecture (MITA) and the Centers for Medicare and Medicaid Services (CMS) Seven Conditions and Standards

1.1.1 Roadmap Phase I

1.1.1.1 Identification of the Current State or As Is

Cognosante completed the Enterprise Roadmap Phase I in September 2012, which documents the Department's current state or As Is model. This analysis also describes DHSS's extensive portfolio of more than 100 health-related applications and registries and more than 40 health projects. These systems are built on a variety of technology platforms, each in response to a specified set of business processes and mission-specific requirements. Each of these systems potentially includes a full set of functionality that, in many cases, is duplicative of the functionality contained in other systems. Examples of this

include data warehouses, case management, document management, and rules engines. Each solution is different, requiring separate technology infrastructure to support these solutions, as well as additional product maintenance staff, license costs, and technical support staff.

Analysis of the ability to exchange data between systems revealed that most of the applications are stand-alone. In fact, about 70 percent of the applications and registries have no integration or interfaces with other systems, which eliminates the ability to share data between systems and users of those systems. Of the 30 percent of systems that include an interface, less than half have more than one interface and many of those are to external systems.

Some of the major systems, including Vital Records; the Women, Infants, and Children (WIC) system; and the legacy Medicaid Management Information System (MMIS) and Eligibility Information System (EIS) are obsolete mainframe-based systems that were implemented in the 1980s and are difficult and expensive to operate and maintain. These systems are either in the process of being replaced or have been targeted for replacement. In addition, there are a number of other systems that are candidates for upgrades or replacement, such as the Resource and Patient Management System (RPMS); Services Tracking Analysis and Reporting System (STARS); Online Resource for the Children of Alaska (ORCA); and Alaska Pioneer Homes medical records program (ACCU-CARE).

1.1.1.2 Identification of the Department's Vision and Goals or the To Be

The envisioned To Be for Alaska, as outlined in the Alaska Roadmap Phase I document, is a gradual transition to a Shared Services model, built on an enterprise-level SOA. The initial Roadmap document provides a high-level, conceptual architecture of the shared services environment, as well as discussion of the policies and applicable federal and state IT standards that support the implementation and growth of shared services model.

The Roadmap Phase II details changes to the current technology infrastructure that are needed to establish the HIT architecture and the transition to an SOA environment. SOA is a general term for a flexible set of design principles used during system design and development to integrate disparate software and system components. Using SOA, components, often referred to as common functions, are exposed as services that can be utilized by multiple applications across the Alaska DHSS Enterprise. Components are then available, as a service, to be utilized and evoked by other programs connected to the network. Thus, a strong SOA is based on common business and technical support components that comprise an integration framework. It is this integration framework that provides the fabric through which functional components interact and gain access to common business and technical support components.

The basis of this integration framework, or the backbone of the technical infrastructure for the SOA architecture, is the implementation of the Enterprise Service Bus (ESB), Business Rules Engine (BRE), and workflow engine, all utilizing a common security infrastructure. The Roadmap Phase II focuses on the necessary changes needed to the current BizTalk environment to support true ESB functionality, which is key to the establishment of the SOA architecture.

In summary, the current DHSS IT environment provides great opportunities for increased efficiency by creating the infrastructure necessary to support shared functionality, transition to use of modular services and components that can be leveraged for reuse, and moving away from siloed systems to enterprise architecture.

1.1.2 Roadmap Phase II

The Enterprise Roadmap Phase II focuses on refining recommendations provided in the following documents including:

- **Interviews with senior DHSS executives in July 2010**
- **A technical assessment conducted in October 2010**
- **The State Medicaid Health Plan (SMHP) containing the Health Information Technology (HIT) Roadmap in November 2010**
- **The Alaska Logical Architecture that noted the State HIT systems connecting to the Health Information Exchange (HIE) in August 2011**
- **The MITA Self-Assessment (SS-A) gap analysis and Eligibility Information System (EIS) analysis conducted during 2012**
- **DHSS Enterprise Roadmap Phase I completed in September 2012**
- **Master Client Index (MCI) Architectural Review completed in March 2013**

The recommendations in this Roadmap capitalize on the prior efforts listed above and suggest additional steps and initiatives for continuing the transformation over the next 5 to 6 years. Additional topics include:

- Creating the Infrastructure
  - BizTalk ESB
  - MultiVue Master Client Index (MCI)
  - Shared Services
- Cultural and process changes
- Expected outcomes
- Evaluating results
- Recommendations for next steps and leveraging the Roadmap

1.2 Creating the Infrastructure to Meet Evolving Business Needs

The traditional approach included creating separate projects, procurements, and products to meet the similar business needs of individual Divisions and programs. Implementing an enterprise-level, MITA- and SOA-compliant infrastructure will enable DHSS to coordinate HIT spending across Divisions to reduce redundancy, encourage reuse, and leverage components and services to meet evolving business needs efficiently. By analyzing the business needs of each Division, the Project and Portfolio Management Review (PPMR) team will identify the need for enterprise-wide solutions.

1.2.1 Alignment with MITA and CMS Seven Conditions and Standards

The CMS Seven Conditions and Standards and Medicaid Information Technology Architecture (MITA) support the Roadmap recommendations to move forward with the implementation of an enterprise architecture based on SOA and increasing modularity.

Additionally, CMS has made it clear that MITA, while developed specifically for the Medicaid enterprise, contains the vision for SOA-based interoperability and the blueprint for modularity. As such, the

principles of MITA are applied to the development of enterprise architectures and the integration of modular components using a common process and conformance to MITA and national standards.

These standards include developing systems, applications, and services using smaller, modular components. By breaking functionality into smaller components, common functionality can be shared or reused in different Divisions or Sections of the Department. This reusability allows DHSS to procure a service once, rather than including that functionality in every Request for Proposal (RFP). This reduces costs and redundancy and allows new functionality to be available for use sooner.

Section 1561 of the Affordable Care Act (ACA) supports the separation of Business Rules from Business logic within the application architecture. To support this architecture, the BRE is accessed via an ESB through common services or customized Web Services interfaces.

1.3 Successful Process Change Requires Cultural Change

The traditional, program-centric approach, as well as the inflexibility of legacy applications, required resource-intensive processes tailored to meet the specific needs of individual programs. Business processes and procedures had to be designed within the constraints of existing technologies. As the Department moves toward enterprise architecture consistent with MITA and SOA, changes to business processes, procedures, and paradigms will be as significant as the changes in technology. Mental models for determining when a project is needed will shift from analysis of program or Division business needs, resources, and funding, to analysis and alignment of business services across the Department.

Cultural change to align with the Department's vision includes developing RFPs that require vendors to reuse existing services rather than procuring redundant functionality as part of each new system or application. RFPs will need to be reviewed to ensure they require vendors to address and comply with licensing considerations, interface control definitions, and enterprise-wide standards.

The level of effort traditionally required to share information and coordinate services across Divisions has made the resulting return on investment (ROI) minimal. The benefits of improved access to information about client participation across Department programs are not always readily apparent. It will take effort to think differently and recognize the advantages this new, more collaborative model provides. The value resulting from sharing services, functionality, and information will produce an ROI that outweighs the discomfort that accompanies change.

1.4 Expected Outcomes

Given the complexity and volume of federal mandates, budget constraints, and anticipation of future uncertainty because of the ACA, states need to have IT architectures that are more responsive, flexible, and adaptable to change.

For Alaska DHSS, the Roadmap represents an opportunity for change that will modernize the State's technology infrastructure, standardize business processes, streamline functions, and reduce or eliminate redundancy. This will allow DHSS to meet evolving business needs, respond to increasing demand for services, and comply with federal mandates through use of a modular, agile, and flexible infrastructure.

Implementation of the recommendations above will provide the following benefits:

- Strong oversight and governance of IT acquisition projects
- Improved IT service model
- Strengthened security oversight and measures
- Standardized business services, available and accessible through shared services
- Consolidation of systems

- Elimination of duplicate storage and unnecessary collection of data
- Creation of a statewide master shared services and data management strategy
- Standardized technology platform, available and accessible through multiple access channels
- Greater access by citizens and providers to health care information and services
- Higher level of shared knowledge
- Lower overall system acquisition and maintenance costs
- Ability to leverage enhanced Medicaid funding

1.5 Evaluation and Measurement

The success of implementing the Roadmap can be measured in terms of the savings in systems implementations. As a result of leveraging shared services and functions, as described in this document, DHSS should align and standardize business processes across Divisions. The level of success DHSS attains in achieving the HIT vision and goals can be measured by evaluating the reuse of services within the architecture.

It should be noted that some of these measurements and processes are already being put into practice by the PPMR team. As part of the new procurement process, Divisions must complete the IT Alignment Framework Template and define business needs prior to moving forward.

The key metrics for evaluation include:

- Count of shared services and functions with the Department
- Count of Divisions leveraging a specific service or functions
- Implementation costs per service (costs should decrease with repeated implementations of a shared service due to reuse of code, testing processes, and procedures)
- Reduced procurement costs

1.6 Recommendations and Leveraging the Roadmap

1.6.1 Establish Necessary Governance and Blueprint for Department Architecture

- Include SOA Governance as a responsibility of PPMR
- Create a SOA Governance Plan
- Develop a blueprint for the Department's overall architecture
- Develop conceptual, logical, and technical models of the To Be architecture
- Develop and maintain a list of shared services and components
- Require Interface Control Documents for each shared service

1.6.2 Make Necessary Changes to the Procurement Process to Support the Migration to Shared Services and Architecture

- Require that each new RFP enforce the use of Shared Services
  - Use the IT Framework Alignment process to identify shared services
  - Ensure all new procurements utilize existing or planned share services
  - Publish Interface Control Documents for shared services that are expected to be leveraged within a procurement as an RFP Appendix
  - Require vendors to leverage existing shared services and documented interfaces
  - Ensure that vendors are not including licenses, products, or hardware costs for existing shared services

1.6.3 Develop the Technical Infrastructure to Support the Implementation of a Service Oriented Architecture

- Update/upgrade the current hosting infrastructure for BizTalk
- Enable and implement all required components for the BizTalk ESB
- Prioritize recommended shared functionality/services implementation
- Identify hosting, life cycles, and required parameters for each existing and priority service
- Create measurable success criteria for all new applications and shared services
- Utilize the ESB to expose existing and future shared functionality/services
- Ensure all future applications and services are strictly following SOA standards
- Evaluate the proficiency and knowledge of DHSS IT staff for the BizTalk ESB and MultiVue MCI and determine if additional training is needed
- Determine if additional DHSS IT staff should be hired, or a vendor secured to implement and maintain enhanced functionality within BizTalk ESB and MultiVue MCI

1.6.4 Recommendations for Shared Services Implementation

Cognosante researched shared services commonly deployed by health and human services agencies to increase efficiency and productivity, while reducing costs. Cognosante identified areas of focus that the Department may want to consider when determining the highest priorities for shared functionality/services. Factors considered included:

- The number of DHSS Divisions or applications that would benefit from the shared service
- How well implementation of the service supports DHSS next steps for the BizTalk ESB and MultiVue MCI
- The potential of each service to provide a “quick win” for the Department
- The level of increased efficiency, time and cost savings
- Ability of the service to increase productivity
- Potential reduction in manual tasks

As existing systems are prioritized for replacement and system maintenance contracts renegotiated, there may be additional shared services that DHSS should consider implementing. The following services are not exhaustive but describe services that have been successfully implemented in other health and human services agencies that may provide opportunities as DHSS continues to move forward with a shared services model.

1.6.4.1 Person Look-Up Service

A Person Look-Up Service consists of person demographic information that provides a high degree of accuracy when querying MCI data and identifying matching records. These data elements are typically included when creating the golden record.

1.6.4.2 Address Validation Service

An Address Validation Service checks the address the user enters against a national database of valid addresses such as the United States Postal Service (USPS).

1.6.4.3 Address Look-Up Service

An Address Look-Up Service checks the address the user enters against the existing address information for that individual in a database, such as the MCI. It is also used to validate address information against golden record data.

1.6.4.4 Person Add/Update Service

A Person Add/Update Service can add new person records and update existing client demographic data.

1.6.4.5 Person Record Locator Service

This service identifies where records are located based on client demographic data, allows the appropriate staff to update record location information, and includes the following functionality:

- Retrieves record locations with information associated with a specific person
- Locates context-sensitive information based on data matching requirements
- Provides information about the types of information or topics stored in a given location
- Identifies the topics that will message a given location
- Determines requirements for storing person data and record locations

1.6.4.6 Identity Management Service

Automates security related maintenance tasks such as creating unique user identification (ID), complex password, and resetting user passwords when needed. Because a large percentage of help-desk calls are password-related, a service that allows users to reset their own passwords can save significant IT resource time and expense.

1.6.4.7 Provider Directory Service

Provider directories not only store a listing of providers, but they include associated provider information such as the National Provider Identifier (NPI) and medical specialty.

1.6.4.8 Identity Proofing Service

This service verifies that the individual creating a user account is the same person whose identifying information is being provided. In addition to demographic information, life history events or financial transaction data available from public and private data sources is used to validate the identity of the person attempting to create a user account.

1.6.4.9 Payment Processing Service

Payment Processing Services allow funds to be received from an individual's credit card or checking account, process payments, and deposit funds into the appropriate state account.

1.6.4.10 Hardcopy Notice Sending Service

The Hardcopy Notice Sending Service can be used by any agency or Division that is required to send paper notices to clients. To use this service, each Division submits their notice jobs and provides all necessary information to the Shared Service. That information is sent to a centralized unit or vendor that prints, processes, and mails the notices.

1.6.4.11 Softcopy Correspondence Generation Service

The Softcopy Correspondence Generation Service is used to send correspondence via email, text message, or Interactive Voice Response (IVR). Because the ACA encourages use of these additional communication methods, many health and human services agencies are exploring Softcopy Correspondence Generation Services. By implementing this functionality as a Shared Service, costs and redundancy can be reduced. However, Softcopy Correspondence Generation Services often require a large number of technical resources to maintain. Because of the relatively small number of DHSS clients, this service may provide a lower return on investment than in larger states.

1.6.5 Case Management as a Shared Service

DHSS has already procured some of these services which can be exposed for reuse. Additional services should be prioritized for implementation. Multiple DHSS systems contain case management functionality. By separating case management into smaller, more modular capabilities, the Department could leverage common functionalities as shared services.

For example, DHSS may want to consider leveraging services such as:

- Grievance and appeals service
- Fraud, waste, and abuse tracking service
- Incident tracking

By leveraging these case management functionalities as shared services, the Department could increase consistency, improve data quality and transparency, and reduce the amount of time required for staff to complete case management tasks. This would reduce costs and allow current staffing levels to meet increasing service demands.

1.6.6 Electronic Document Management System as a Shared Service

Each Division within the Department is required to collect, process, manage, store, retrieve, maintain, and provide search capability for documents as an integral part of day-to-day operations.. Documents for a given individual are stored in separate repositories, requiring different access technologies, separate storage, maintenance, and product licensing costs, as well as different business processes, retrieval, and search procedures. The end result for DHSS is duplicate costs across Divisions, lack of standardization of business processes, and difficulty in sharing or retrieving documents for the same individual across different systems.

Differences in each Division's business processes and storage needs make this one of the more challenging functions to implement as a shared service. Challenges include differences in the business processes, document types, workflow, storage requirements, and access needs of each Division.

Implementing EDMS as a shared service will require more than selecting the right technology component. Each Division's requirements will need to be documented in order to develop EDMS as a shared service and to ensure understanding of the current documentation needs. However, the evolution of EDMS to a shared function offers the following potential benefits to Alaska:

- Total lower cost of ownership: elimination of multiple technology and consolidation of current document storage reduces product license and maintenance costs, and allows DHSS to leverage economy of scale for storage of larger documents
- Reduced Duplication of Documents: a single repository also minimizes the potential duplication of documents across different Division level repositories
- Improved Access: leveraging shared services standardizes storage and access routines across the Department, allowing multiple Divisions the capability to securely search for and access documents appropriately
- Standardized Business Processes: document workflow and processes can be automated and standardized across the Department, improving the ability of different Divisions to access documentation. Workflow can be automated across Divisions for documentation notification, eliminating the need to electronically or physically pass documentation from one Division to another. Alerts and notifications can be automated as part of the centralized workflow
- Centralized Security: with a shared repository, document security is centralized, which reduces the security risks incurred with multiple repository environments

Cognosante recommends DHSS proceed with establishing EDMS as a shared service. Work will be required to identify common storage and retrieval requirements across Divisions and implement these as the initial services for the EDMS shared service. The Department will also need to gather statistics for current and future data storage requirements to accurately price the solution and procure the necessary storage.

2.0 REVIEW TEAM AND SOA GOVERNANCE

As a best practice, health and human services agencies often create a Service Oriented Architecture (SOA) Governance Body that is responsible for coordinating all of the activities required to create and maintain shared services within the agency. One role of the SOA Governance Body is to ensure development teams follow documentation standards so that consistency and continuity is provided, regardless of staff turnover.

The Department of Health and Social Services (DHSS) could incorporate SOA Governance within or reporting to the Project and Portfolio Management Review Team (PPMR) to provide oversight and ensure all future Requests for Proposals (RFPs) identify shared functionality needs and require key modules and capabilities to be sharable. Once shared functionality is established, DHSS should consider requiring vendors to interface with those functions and use pre-established Web Service Definition Language (WSDL) definitions. PPMR could provide oversight to ensure uniformity and standardization of WSDLs, as well as transparency. One of the key requirements is that each WSDL be defined by an interface control document. PPMR could assume responsibility for establishing and enforcing the use of shared functionality and ensuring reusability across the enterprise, including interface control document review and deciding which functions should be shared. Once approved by this group, DHSS Information Technology (IT) could publish the web service, the associated interface control document, and make it available for appropriate, secure usage.

The success of implementing SOA in any organization depends on defining and enforcing SOA guidelines for all applications and services. The Department should consider establishing an Enterprise-wide standard that would require newly acquired services and applications to be SOA-compliant out of the box. Vendors often use terms such as “SOA-ready” which can be misleading because they suggest that the software is built on a SOA-compliant framework. However, major code changes may be required for an SOA-ready application to be fully SOA-compliant.

DHSS may want to consider designating a small team of senior developers, analysts, and other staff who would be responsible for developing and maintaining:

- BizTalk Enterprise Service Bus (ESB)
- Business Rules Engine (BRE)
- Master Client Index (MCI)
- Shared functionality/services
- Business processes, workflows, and service testing using Business Process Execution Language (BPEL)
- Business Process Model and Notation (BPMN)
- Defining, establishing, and governance of the interfaces for each module (accomplished through the use of the Interface Control Document)

This team would work with the appropriate application developers to create required business rules, business processes, and workflows. This coordination and oversight would also be necessary to complete other ESB-related tasks such as creating and maintaining WSDL files and creating documentation for connecting to, using, or consuming each shared service thorough connection to the BizTalk ESB.

Modern commercial off-the-shelf (COTS) applications built to SOA standards make exposing services easier for development teams. However, it can be difficult to share functionality contained in older legacy applications not based on SOA. The approach for implementing shared functionality/services may be

different for services that are already included as part of a larger application, than for new services. A dedicated team would help ensure consistency and standardization.

Optimally, the team members would be familiar with their application's code, as well as Application Programming Interfaces (APIs), SOA, and BizTalk. Creation of a dedicated team ensures programming required to create or expose shared functionality/services within each Division's systems meet standards, is documented, and follows business processes. PPMR could also have responsibility for decisions regarding product licensing and Service Level Agreements (SLAs).

For example, if DHSS decides certain functionalities from the new Eligibility Information System Replacement (EIS-R) are modular and can be exposed as shared services, PPMR and the EIS-R DHSS technical team would be responsible for identification, development, and documentation of the details and parameters of the service being exposed.

Vendors may also provide shared functionality/services for the Department. In these situations, the PPMR should require vendors to provide an interface control document for review. This will ensure that interfaces become publically available and that PPMR has control over the methods used in shared functionality/services implementations. When vendors propose proprietary interfaces, DHSS could require that these be made public, where practical and warranted.

DHSS should also track the interfaces of existing components. By making these available to vendors during the RFP process, DHSS could require that vendors connect to existing services. This would also enforce reuse of components, lower costs, and provide the Department with a growing library of shared functionality/services and components.

For each shared functionality/service, PPMR would determine:

- The name of the service
- Shared functionality/service life cycle
- Which data fields to include
- Capabilities such as "add and/or update" or "read-only"
- Roles and permissions
- Security
- How the service will be called
- How the service will be used
- Input/output parameters
- Documentation of the returned values and their interpretation
- Review and approve submitted interface control documents

PPMR, in coordination with the dedicated IT team, may decide on a case-by-case basis which current or replacement Department system should contain the shared functionality/service and the best methods for implementing or installing each shared functionality/service. The approach may be different for services that are already included as part of a larger application than when new services are implemented outside of a new system implementation project.

Cognosante recommends DHSS consider creating a SOA Governance Plan. The SOA Governance Plan could be published to the DHSS IT intranet and should include:

- Information about how shared functionality/services are identified
- Requirement that the RFP process must require vendors to integrate with the available shared functionality/services

- Requirement that vendors must supply interface control documents for modules that are identified in the RFP process as common services that can be reused by one or more Divisions
- List of supported shared functionality/services
- Information about requesting access to the ESB
- Instructions for connecting a shared service to the ESB
- Data interchange instructions
- Documentation for interpreting the data provided by each shared functionality/service
- Shared functionality/services data parameters,
- Contact information of DHSS IT resources supporting the ESB
- Confidentiality, privacy, and security standards and requirements

Additionally, an electronic form could be used to standardize requests for new shared functionality/services that would connect to the ESB.

3.0 Enterprise Service Bus

The Enterprise Service Bus (ESB) is a component of a modular, Service Oriented Architecture (SOA) that promotes reusability and the use of shared services. The ESB acts as a universal translation program or a gateway for non-homogenous applications to share and consume services. An ESB enables communication between different Department systems and supports compliance with the Centers for Medicare and Medicaid Services (CMS) Seven Conditions and Standards by aligning with Medicaid Information Technology Architecture (MITA) and promoting re-use of services.

When there is an overflow of data requests, the ESB automatically creates a queue and serves each customer accordingly. The BizTalk ESB uses internal algorithms to prioritize tasks and ensure critical actions are completed first. The ESB can also be a valuable component of Alaska's Master Data Management (MDM) system as the key mediation tool for data conversion. The Department of Health and Social Services (DHSS) Information Technology (IT) should consider dedicating staff resources with specific ESB experience to BizTalk system development and maintenance. These staff could also be responsible for coordinating with business users to ensure decisions regarding the ESB meet business needs.

3.1 Implementing BizTalk to Provide Full ESB Functionality

The Master Client Index (MCI) Architectural Review recommended implementing BizTalk's full ESB capabilities. This action would further the DHSS IT goal of moving toward an enterprise framework, implementing near real-time connectivity between the MCI and Division applications, and implementing shared functionality or shared services.

Additionally, the Roadmap Phase I and the MCI Architectural Review recommended moving forward with an SOA initiative and implementation of structures to allow shared functionality. Organizing and managing services and delivery processes would maximize responsiveness, efficiency, and effectiveness. The next step in this process, which also supports the DHSS IT goal of moving toward the use of shared functionality/services, is to implement the full ESB capabilities of BizTalk.

The current implementation of BizTalk may not be configured in a way that supports full ESB functionality. DHSS IT will need to make some configuration changes for BizTalk to provide enterprise-level support and be leveraged by multiple Divisions for continual production use. As DHSS IT prepares for BizTalk ESB implementation, some system administration work may be needed to enable features that are currently unavailable and address any bugs that may be identified.

During the BizTalk ESB implementation, it may be helpful to arrange for VisionWare, BizTalk representatives to be onsite. The representatives would provide support, address any issues that arise, and ensure a smooth implementation process.

3.1.1 Required BizTalk Upgrades

In the Enterprise Roadmap Phase I and MCI Architectural Review deliverables, Cognosante recommended DHSS review and upgrade the current BizTalk infrastructure architecture. In order for BizTalk to provide essential functionality in the DHSS environment, such as providing information in near real-time to many critical applications and services, DHSS IT should host BizTalk on an infrastructure that will ensure maximum availability with minimal downtime. This will ensure DHSS IT is able to maintain system availability during routine maintenance or during a natural or human-caused disaster, based on the Department's Disaster Recovery Plans.

3.1.1.1 Distributed Architecture and Virtualization

Cognosante met with DHSS IT representatives to discuss the current architecture of the BizTalk ESB. During those conversations, DHSS IT provided information that suggested BizTalk is currently running on non-virtualized, non-fault tolerant, non-high availability hardware and network architecture. This means that the system has a lower ability to handle peak loads that could occur with increased usage of ESB services. If a component should fail, there is currently no duplicate component that would automatically take over. Additionally, BizTalk currently provides a shared messaging layer that has the ability to handle a limited number of specific messages but does not provide the ability to share services.

Cognosante recommends using a hardware architecture and internal connectivity that are highly available, redundant, and failsafe, based on the latest distributed architecture. By deploying two identical hardware components, DHSS IT can efficiently distribute load. Redundancy allows the duplicate component to continue to provide the required functionality and eliminate the impact of unexpected hardware failure. This will allow DHSS IT to prevent system downtime and service delivery disruptions while replacing failed hardware.

DHSS IT will need to purchase additional BizTalk licenses if BizTalk is implemented on two or more parallel servers. Whenever existing hardware is upgraded, it is important to ensure the current network has the ability to support the new hardware. Depending on the technology being deployed, additional training may be required to ensure DHSS IT resources can effectively manage the new hardware.

Cognosante also recommends using virtualized environments to deploy Microsoft BizTalk. Because DHSS IT is currently using virtualization for some systems, IT resource with the current knowledge base to complete this task may be available. Virtual machines provide an elastic operating system that allocates and re-allocates resources from a shared pool as needed. This means the virtualized systems can automatically allocate memory or disk space from a shared pool, as needed. When the additional resources are no longer needed, the virtual machine re-allocates the shared resources back to the pool.

By sharing resources in this manner, system administrators can ensure resource availability for the highest priority systems. The approach also reduces the possibility that system administrators will need to logon or go into the Data Center outside of normal business hours to add a hard disk drive or manually start, stop, or restart processes to free up memory needed to complete large jobs.

The virtualization operating system constantly monitors its applications, including the ESB. If BizTalk were to experience a failure, the virtualization operating system would promptly spawn a new instance of BizTalk to continue processing information held in the queue.

3.1.1.2 Test and Production Environment

Often, system administrators deploy a less-robust architecture for their ESB test environment that uses less powerful hardware. This allows design of the ESB production environment using the organization's highest quality hardware platform. Another option is to run both test and production environments from shared hardware and architecture. When system administrators use this method, they also establish the business processes and procedures that ensure test environment activities do not slow down the production environment. With enhanced implementation of the BizTalk ESB, Cognosante recommends DHSS IT use a dedicated and robust test environment.

3.1.1.3 BizTalk Enterprise Licensing

The current BizTalk implementation provides a shared messaging layer for the enterprise, but can only handle certain types of messages. Microsoft sells BizTalk in many different editions or packages. Cognosante's research indicates that DHSS IT installed the Enterprise edition of BizTalk's license, which

supports full ESB capabilities. However, the Department should review current BizTalk licensing details to ensure no adjustments are needed.

When BizTalk is upgraded to provide full ESB functionality, DHSS IT may need to deploy additional Central Processing Units (CPUs) in a virtualized, highly available, failsafe, and redundant hosting environment for BizTalk. Cognosante researched BizTalk licensing costs and found that Microsoft offers per-processor-based BizTalk licensing. Microsoft's BizTalk website listed the per CPU license cost of $44,228 for the Enterprise edition on March 20, 2013. Only the Enterprise addition, which DHSS purchased, allows an unlimited number of shared functionality/services and applications to connect to the BizTalk ESB.

3.2 ESB's Role in Supporting Shared Functionality

The BizTalk ESB works as the universal translation program for applications and services that connect through the ESB. Connections and interfaces through the ESB are considered loosely coupled because they can be deployed and deleted easily. Adding or deleting a loosely coupled connection does not affect other services or connections. Any shared functionality/service can be replaced at any time, as long as the replacement service precisely follows the criteria for data interchange. System administrators can install new services transparently, without affecting other applications, services, or interfaces connected to the ESB.

All communications through an ESB are considered "near real-time" because translating and transforming data cause ESB communications to be slightly slower than traditional direct data interfaces. However, because small amounts of data are usually being exchanged, end-users receive the data instantaneously just as when a point-to-point interface is used.

Hardware and software are not always compatible due to variables such as:

- Programming language
- Operating system
- Version number and installed patches
- Software and hardware platforms

IT departments implement ESBs to make connecting components easier. One role of a system administrator is to ensure each component's requirements are satisfied and the resulting system provides the desired functionality. Without an ESB, IT resources would need to connect each component to every other component directly, using the native Application Programming Interfaces (APIs) and the unique databases of each. These point-to-point interfaces would not provide reusability; therefore IT resources would need to complete hundreds of tasks before multiple components could be successfully connected and exchange data. Any change in the configuration of one component would cause broken connections and a loss of functionality.

ESBs based on SOA make it easy for IT resources to complete the connection and data interchange processes among non-homogeneous applications and services. Developers only need to meet a few requirements to enable communication between the ESB and shared functionality/services. Upon request, the ESB can provide developers with service definitions and connection instructions as well as a description of how to use any specific service the ESB is capable of running.

For example, Application A was developed in C++ programming language and has a maximum field length of 30 characters for the first name field. Shared Service B was developed in Visual Basic .NET, and uses a "variable characters" field with up to 4,000 bytes for the first name field. If first name field data was interchanged using a direct connection or point-to-point interface between Application A and

Shared Services B, data type mismatch and field length mismatch errors would likely occur. However, by using an ESB, IT resources can easily create this type of data interchange transparent to the application, shared service, and end user.

3.3 ESB Connectivity

In order to make the BizTalk ESB data connections and data interchange processes easier, DHSS may want to use a helper application, like the BizTalk ESB Toolkit that is included in the Department's current BizTalk enterprise license. DHSS IT resources could install this toolkit on the same server as the BizTalk ESB. It provides a collection of tools and libraries that extend the capabilities of the BizTalk ESB and support a loosely coupled, dynamic message-based SOA. The toolkit functions as a middleware application that provides mediation tools for shared service providers and service consumers. The BizTalk ESB toolkit simplifies loosely coupled composition of service endpoints and management of service interactions for developers.

The BizTalk enterprise license has the following internal components, modules, and engines that DHSS will need to install, configure, and run in order to use BizTalk as an ESB. Please note equivalent external engines also exist that could be used in place of the following BizTalk components:

- Transformation Engine
- Business Rule Engine (BRE)
- Orchestration Engine
- Publish and Subscribe Engine
- Data Adapters Module
- Dynamic Ports Module
- Business Activity Monitoring (BAM) Module
- Universal Description Discovery and Integration (UDDI) Module
- Host Environment Monitoring Module
- BizTalk Administration Console

In order for BizTalk to function as an ESB, DHSS IT will need to implement files that extend the base functionality of BizTalk. Once installed, these files, called extensions, would work with internal BizTalk components to provide the desired functionality. DHSS should consider implementing the following BizTalk extensions:

- Business Activity Monitoring (BAM)
- Service Level Agreement (SLA) Monitoring and Management
- Business Process Execution Language (BPEL) and Business Process Support
- Dynamic Service provisioning
- BizTalk ESB Toolkit

Because this functionality currently exists within the BizTalk ESB, this process is straightforward and does not require installation of new software. Figure 1 depicts the internal components of an ESB.

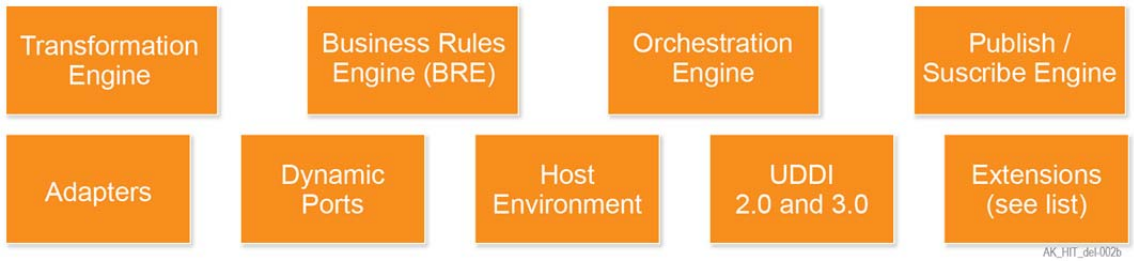


Figure 1: Internal ESB Components

3.4 Shared Components

DHSS IT will need to implement and properly configure shared components in order for BizTalk to function as a Department-wide ESB.

The objective of an SOA is to provide an architecture that uses the concept of "Service" as the underlying business IT strategy. In addition, SOA is a vision of how heterogeneous applications should be developed and integrated. SOA is the way to shift away from stovepipe applications to a set of reusable services that can be integrated to build applications.

The key concepts surrounding SOA are Service Provider, Service Consumer, and Service Registry as shown in Figure 2.

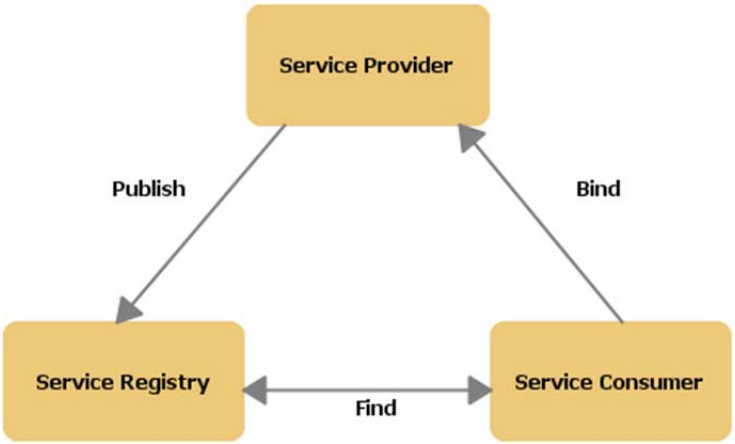


Figure 2: SOA – Key Concepts

Table 2: SOA Terms and Definitions

SOA Terms and Definitions	
Term	Definition
Service	Encapsulates business domain specific logic and is exposed through an open standards based interface
Service Contract	Stipulates the terms and conditions under which a service is provided
Service Consumer	Consumes a service or an assembly of services to deliver a particular business process
Service Provider	Provides services based on a pre-defined service contract that guarantees a minimum service level which may include performance, reliability, and usage cost
Service Registry	Holds the descriptions and contracts associated with the services available for consumption

3.4.1 Business Rules Engine

The BRE can be utilized two ways within the BizTalk environment. First, as a shared service or functionality, the BRE can act as the central repository of rules for the Department. Secondly, the Rules Engine within BizTalk can be utilized as part of the Orchestration Engine, to enable and prioritize simple to complex processes within the BizTalk environment. DHSS may want to consider including the requirement that vendors utilize the IBM WebSphere ILOG JRules BRE utilized by the Eligibility Information System (EIS) for any future replacement system Request for Proposals (RFPs). The WebSphere ILOG JRules BRE could also be leveraged over time to become the central repository for DHSS business rules.

3.4.1.1 Business Rules Engine as a Shared Service

The BRE is an example of common functionality that could be shared by one or many applications. Additionally, MITA, CMS Seven Conditions and Standards, and Section 1561 of the Affordable Care Act (ACA) require that business logic be separated from business rules, allowing the BRE to be external to the application. Following this standard, application business rules can be consolidated within a common rules engine and accessed thru BizTalk by the applications connecting to the ESB. While the criteria for selecting a BRE is not included in the scope of this document, leveraging a centralized BRE provides several benefits to Alaska:

- Allows the business rules to be stored in a common repository
- Creates a centralized knowledge bank of business rules
- Eliminates the costs associated with duplicate rules engine licenses and instances
- Allows applications across the enterprise to access shared functionality through application specific or shared services
- Provides the ability for DHSS business analysts to learn to create and maintain rules in a common rules engine, saving training costs

3.4.1.2 Business Rules to Support Orchestration Processes

Part of the power of BizTalk is its ability to orchestrate processes. An orchestration is the executable code used to run a workflow supporting a business process. Orchestration interacts with outside entities by

using APIs, Web Service Definition Language (WSDL) definitions, and ports. Together, these create a powerful tool to perform process automation.

An orchestration describes a logical and chronological set of activities in order to achieve a business goal. In order to interact with systems and applications outside the boundaries of the orchestration, DHSS IT can use, send, and receive data between applications connected to the ESB through ports using WSDLs. Orchestration allows business processes to be modeled visually and is the primary mechanism used to automate processes within a solution. Business process models are created in Visual Studio and compiled into .NET assemblies that are deployed in the global assembly cache and registered in the BizTalk management database.

The tool used to define the orchestration is BizTalk Orchestration Designer, which presents a visual development environment for specifying the process flow separately from the implementation of the individual activities in the process.

Orchestrations are executed by the BizTalk orchestration engine, which is the maestro and runtime environment that manages the life cycle of orchestrations such as instantiation, execution, termination, and migration across host instances. The orchestration engine also schedules and monitors the interaction with external entities and the capability to invoke the BRE to perform processes and make policy or data decisions within the orchestration process.

3.4.2 Business Activity Monitoring

DHSS IT should also enable BAM functionality available within BizTalk. BAM would provide tools that a dedicated team of developers could use to monitor and analyze data from business process information sources in real time. Additionally, the BAM API enables developers to expose data that is processed by BizTalk for viewing. BAM provides critical data regarding:

- Length of time required to complete a process using the current business rules
- Length of time required to complete individual tasks within a process
- Number of process cycles completed in the last week, month, or year

DHSS IT can use this data to improve the SLA, identify process bottlenecks, and enable fine-tuning of the application and overall service performance.

3.4.3 Business Process Workflow Engine

BizTalk also includes a business process workflow engine that DHSS IT resources will need to implement to provide ESB functionality. BizTalk's business process workflow engine is compatible with BPEL, Business Process Model and Notation (BPMN), WSDL, UDDI, and Web Services.

A business processes workflow engine is a core component of every ESB. An ESB can have an internal or an external business process workflow engine. This component describes the steps in the process and the order in which they are executed to achieve business goals. A business process workflow engine uses a flow chart similar to the popular modeling tool, Visio®. A business process workflow engine improves the visibility and agility of the business logics, resulting in higher-level and domain-specific representations that can be understood by non-technical business users. Within BizTalk, this engine is simply referred as the Workflow Engine, which works with the Orchestration Designer.

The business processes workflow engine is a critical component, and one that is commonly needed by many agency divisions. DHSS will want to consider the availability of IT resources to support and maintain the engine as well as business needs when determining if the BizTalk engine or an external engine is the best fit. The BRE and the business process workflow engine work very closely to define and

process the data that are coming into the ESB and going out of the ESB. Every shared service that is supported by the ESB uses one or more business rules and business process workflows to interchange data. Therefore, the BRE the Department selects as the enterprise BRE will affect whether BizTalk's internal business process workflow engine or an external version should be selected for enterprise-wide use.

Additionally, BizTalk needs to be configured to perform the following tasks:

- Shared Services mediation and virtualization
- Transformation of incoming and outgoing data
- Content-based routing and delivery to end-point
- Validation of messages, ensuring that they are well-formed
- Event management
- Quality of Service (QOS) that provides security and prioritization of shared functionality/services
- Internal and integrated security and privacy features
- Hosting services capability
- Shared service orchestration, which is the automatic, logical arrangement of shared services to ensure faster processing speeds
- Comprehensive error handling
- Asynchronous and synchronous service support
- Support and conversion of common protocols and accelerators such as:
  - Health Level Seven (HL7), which provides health related confidential data transfer
  - Hypertext Transfer Protocol Secure (HTTPS) for data encryption
  - Health Insurance Portability and Affordability Act (HIPAA) and ACA security standards
  - Secure File Transfer Protocol (SFTP)

- Advanced functionalities and extensions that DHSS IT can easily add or remove as needed:
  - SLA Monitoring and Management
  - BPEL and Business Process Management
  - Business Activity Monitoring
  - Dynamic Service Provisioning

3.5 ESB Implementation Plan

This implementation plan describes the major tasks associated with implementing BizTalk to provide full ESB functionality.

3.5.1 Assumptions

The following assumptions were used in the development of this implementation plan:

- MCI Architectural Review recommendations will be implemented
- BizTalk deployment will include all peripherals recommended in this document
- DHSS will move forward with creating a BizTalk adapter for the MCI

3.5.2 Major Implementation Tasks

DHSS requires an ESB that provides mediation, security policies, management, and routing for shared services. The major tasks that DHSS IT will complete to implement BizTalk as an ESB are discussed in Sections 3.5.2.1 through 3.5.2.9.

3.5.2.1 Project Management

Project management and planning help ensure all of the tasks necessary for a successful implementation are identified, tracked, and managed. The Project Manager is responsible for implementation planning and coordination. This includes working with sponsors and other stakeholders to determine implementation dates and schedules. Development of project management plans, including communication, risk, and issue management plans provide a basis for tracking communication, identifying risks, and planning for issues that may arise during execution of the ESB implementation. Project Management ensures all tasks are completed and implementation proceeds smoothly.

3.5.2.2 Implementation Team and Stakeholder Identification

DHSS IT should consider identifying the Project Manager and other staff who will comprise the implementation team. Key implementation roles include:

- Development and maintenance team
- Quality Assurance team
- Database Administrator (DBA)
- Security Management team

3.5.2.3 Determine Maintenance Location and Team

Before implementation activities can begin, DHSS IT will need to determine where the system will be maintained and identify the staff responsible for maintenance and operations. Location will be a factor in determining detailed implementation tasks and staff available in the location to complete the work. It will also identify accommodations needed for staff participating in implementation activities remotely.

3.5.2.4 Security

The implementation team will need to configure BizTalk's authentication, authorization, encryption, and other security settings. The easiest way to address security concerns is to document and implement user access through security roles. Access to the ESB, as well as to shared services and the applications in which they are contained, should be limited based on business need. It is also possible to administer security and manage access to shared services based on parameters such as date and time, service invocation count, and other constraints.

3.5.2.5 Complete System Documentation

System documentation provides information about the application's features, functionality, configuration, and installation that can be referenced during maintenance and operations activities.

3.5.2.6 Establish Acceptance Criteria

Acceptance criteria describe the standards and requirements that must be met before code can be promoted from one environment to another. The acceptance criteria for implementation are met when all technical, functional, and User Acceptance Testing (UAT) is complete and all tests have passed.

3.5.2.7 Technical and Functional Testing

Before BizTalk can be implemented, DHSS IT will need to conduct technical testing to ensure each component has been installed correctly and is providing the required functionality. Cognosante recommends creating test plans to guide the testing effort, document any defects, and track their resolution. Thorough testing will provide confidence when it is time to make the go/no-go decision

As recommended by MITA, most services can be separated into two major categories, technical services, and business services. Each type of service must go through rigorous technical and functional testing before promoted to the production environment.

All shared services test cases should pass, and established entrance, exit, and acceptance criteria met before a shared service is ready to be rolled out from the test environment to the production environment.

3.5.2.8 User Acceptance Testing

UAT must be performed before moving new shared applications or services to the production environment. Once all UAT scripts and test scenarios have been executed and the system has been verified as meeting business needs, the shared application or service can be implemented into the production environment.

A rollback plan should be prepared so that if a major issue is discovered during implementation, the system can be restored to the previous state. The rollback plan provides step-by-step instructions for restoring the production system to the pre-implementation state.

3.5.2.9 Production Implementation

Once technical, functional, and UAT is successfully completed, DHSS IT will be ready to implement the shared functionality/service or application to the production environment so that it can begin providing the required functionality and meeting the related business needs.

The Department has already established several checkpoints and readiness verification processes and procedures. DHSS IT will need to ensure all exit and entrance criteria are met before code can be migrated from the test environment to production.

After completion of the ESB production release, DHSS IT should conduct thorough system oversight for the first 72 hours after implementation.

3.6 Post Implementation Maintenance and Operations

After ESB functionality has been implemented in BizTalk, tasks required to maintain and operate BizTalk to support day-to-day operations begins.

3.6.1 Services Management

BizTalk offers a web-based management console that controls user access based on system administration permissions. Cognosante recommends DHSS IT manage the BizTalk environment/system using configuration files. These Extensible Markup Language (XML) files or scripts allow administrators to perform automatic migration from one environment to another, e.g., a test environment is used to test shared services before moving them to the production environment. Once a service has been successfully tested, the XML scripts can be easily modified and re-used to promote the service to the production environment. This process provides more consistency during the code migration process than configuring parameters via the web console.

3.6.2 Service Performance Monitoring

DHSS should consider implementing detailed application monitoring within BizTalk to safeguard against system failures and instability issues. There are several products in the market that can provide BizTalk Service Monitoring. One example is Hewlett-Packard's OpenView Service Monitoring product.

Software application and service monitoring could be included as part of the overall DHSS IT system monitoring activities. However, there are special monitoring requirements for an ESB, such as monitoring

for any potential problem with one of the peripherals on the connected applications or services. Because these issues can easily be propagated from the connected applications to the ESB layer, which is the heart of the SOA, they can disrupt communication. For this reason, Cognosante recommends DHSS IT consider implementing detailed BizTalk performance monitoring in addition to other performance monitoring activities.

DHSS IT will need to monitor ESB performance metrics, such as the service invocation count and each message size. By monitoring statistical metrics, such as the count of services invoked by users, services called by other services, and the number of connections, DHSS IT can ensure the system is reliable and provides the functionality required to meet business needs.

4.0 MASTER CLIENT INDEX

The Department of Health and Social Services (DHSS) implemented the MultiVue Master Client Index (MCI) to provide improved access to client participation data and increase coordination of services throughout the Department. The MCI Architectural Review found that the hardware and architecture of the MCI supports the Department's vision for the MCI. This includes integration to provide near real-time interoperability to comply with Affordable Care Act (ACA) requirements for interoperability with the Federally Facilitated Exchange (FFE), improve data quality, increase data matching accuracy, and reduce duplicate client data.

DHSS is moving forward with procurement and implementation of Prism and Chroma, which will provide improvement in the percentage of accurate MCI matches and help DHSS Information Technology (IT), automate, monitor, and resolve near-match conditions.

Refining the implementation of the MCI would provide an index of Department client records exposed through the BizTalk Enterprise Service Bus (ESB), with data available for consumption in near-real time. Because the ESB exposes functionality or services for consumption by various applications using the same methods, lessons learned and experience gained from further refinement and implementations of the MCI and BizTalk could be leveraged in the development of shared services.

4.1 Establishing the MCI as the Repository of the Golden Record

DHSS should consider establishing the MCI as the repository of the golden record by standardizing business processes across DHSS Divisions and systems interacting with the MCI. Merging records from several Division systems for a single client and eliminating duplicate client records would be more efficient if source system data were consistently formatted.

Another step in establishing the MCI as the repository of the golden record includes requirements gathering and documentation of the MCI Cross-functional Views. These requirements were documented by Cognosante in April 2013 and define permissions by user role to view or update MCI client data. Permissions are based on the need to coordinate service delivery across the Department or prevent creation of duplicate clients during day-to-day business activities. By defining access to MCI data, DHSS is positioned to create standards and business processes for client record management.

Establishing the MCI as the golden record repository will reduce the creation of duplicate records by ensuring that data changed in one of the systems connected to the MCI results in data for the same client being changed in each of the connected system and the MCI.

As an example, the Online Resource for the Children of Alaska (ORCA) system may have a client's maiden name and related demographics information from when she received foster care services as a teenager. Today, when she applies for Supplemental Nutrition Assistance Program (SNAP) benefits as an adult using her married name, staff may inadvertently create a new client record for her. Using the MCI as the single golden record source of demographic data will reduce these issues. The MCI has built-in algorithms and safeguards that constantly comb the database and reconcile person records that may be duplicative.

The technical configuration of the MCI system should be used as the standard for all demographic data. The data provided from the systems connected to the MCI should be formatted to be consistent with the MCI database, whenever possible. One example would be to format data from the connected systems so that data from the name fields conform to the MCI standard for field length and character type. The benefit of this approach is that the ESB requires fewer resources to translate, transform, or mediate the

data from Division systems to the MCI. This can significantly impact data flow speed and ESB performance.

Documentation is required to ensure consistency and standardization. Documentation should include the technical characteristics of all data fields and the business processes each shared functionality/service is intended to support. Documentation should also describe the step-by-step processes for sharing data based on interoperability between the MCI and other Department applications. Documentation should address viewing, adding, and updating data within the MCI database. This includes creation of a data dictionary or data definition document for the MCI.

4.2 MCI's Role in the HIE

AS 18.23.300, Article 4 directed the Department to create a statewide Health Information Exchange (HIE) to accomplish the following objectives:

- Ensure the confidentiality of Protected Health Information (PHI)
- Improve health care quality and efficiency
- Promote wellness and disease prevention, by increasing the availability and transparency of health information
- Ensure information needed to make medical decisions is available at the time medical services are provided
- Reduce health care costs resulting from inefficiency, medical errors, and inappropriate care
- Promote a more effective marketplace with increased choice and improved outcomes
- Improve coordination of information and provision of health care services through an effective infrastructure for the secure exchange of health care information

Within the HIE environment, the role of an MCI is to help facilitate the creation of a consolidated view of an individual's healthcare history, tests, procedures, and acute incidents. Alaska citizens may have a number of different records, ranging from laboratory results, immunizations, medications, medical procedures, and hospitalizations from a wide range of facilities.

MCIs serve two primary functions within the HIE. The first is to enable the unique identification of an individual. The second is to allow the association of all medical and clinical information from across the federated data sources within the HIE with the correct individual. The combination of these capabilities allows the MCI to be used within the HIE to verify patient identity and provide the record locators or pointers to a patient's data. Once the identity of the patient has been correctly matched and verified using the MCI, the HIE is then responsible for data retrieval from the federated sources using the pointers created in the MCI, such as a Record Locator Service.

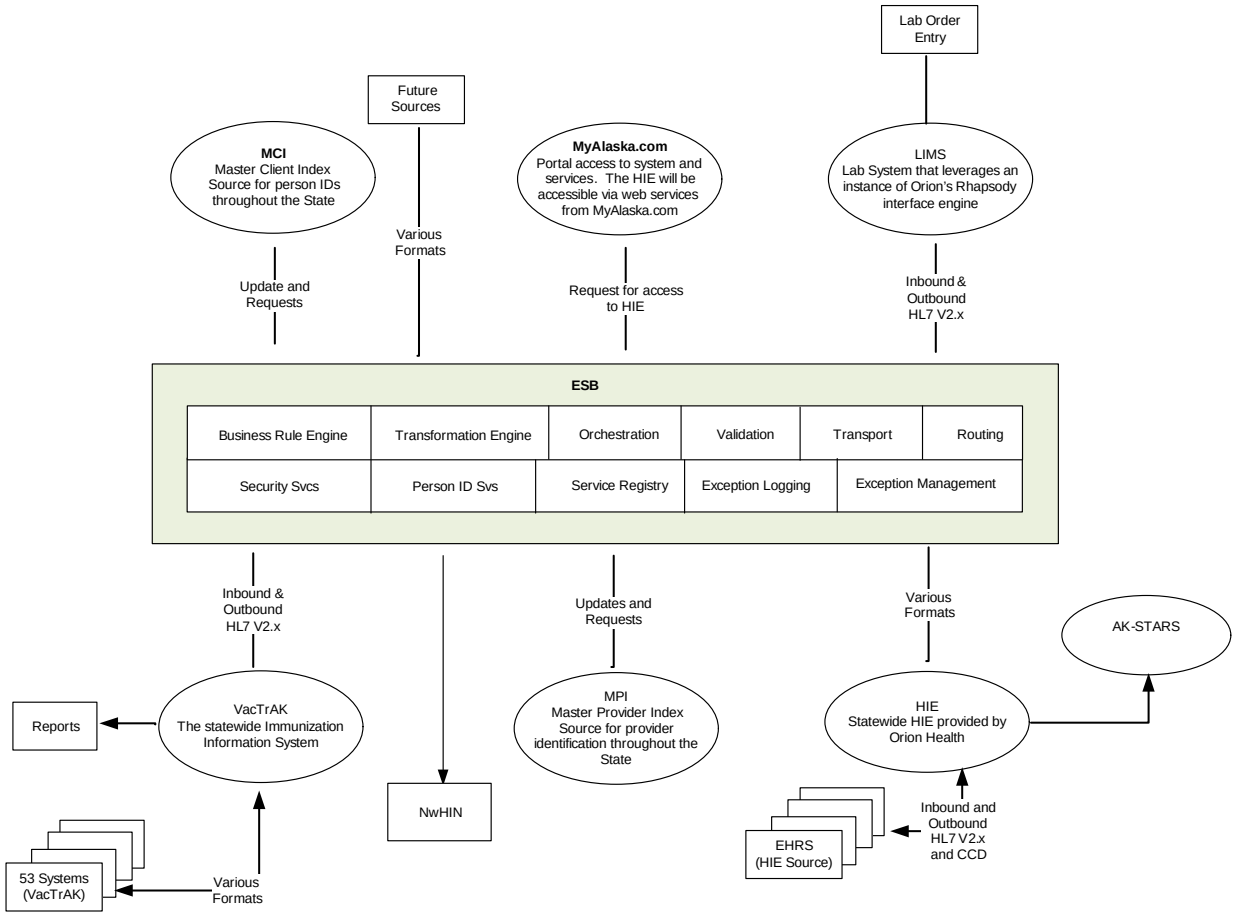
In order to keep a single source of truth for person demographics data, it is important to use only one application or shared service and its databases to store, update, and serve that data. If DHSS decides to use MultiVue's MCI as the single source of truth for demographics data, meaning it would be the Department's single repository of golden records, it will be important for DHSS to designate the MultiVue MCI as the Department-wide standard for storing, updating, and serving that data. This means all other MCIs that are currently in use in DHSS must either be reconciled using the MultiVue's MCI data or taken offline and replaced with MultiVue's MCI database.

Having more than one MCI within the Department is not recommended because it introduces unnecessary complication into the system. However, DHSS may need to interact and exchange data with MCIs external to the Department. DHSS will need to develop business policies and processes regarding the

demographics data received from external MCIs that will determine if data from each source can be trusted and used, or if it should be overwritten by DHSS's own demographics data for further processing.

Cognosante analyzed the MultiVue MCI to determine its current and potential role in facilitating access to the Public Health Record (PHR) through the myAlaska portal and its role in creating interconnectivity between the MMIS data warehouse and HIE repositories. Figure 3 depicts how the potential integration of the MCI and HIE might be configured.

Figure 3: MCI and HIE Integration



4.2.1 MCI's Role in myAlaska Authentication and Validation

The myAlaska portal offers secure Single Sign-On (SSO) and provides an electronic signature system, allowing Alaska citizens to interact with multiple State of Alaska services through one convenient portal. The myAlaska portal includes many layers of validation, such as User Interface validation, Business Logic validation, and Data Access validation, that are utilized during the account creation process.

Users provide their legal names, Social Security Number (SSN), Date of Birth (DOB), and tax information after creating their myAlaska account in order to apply for the permanent dividend fund, unemployment benefits, and other services available through the myAlaska portal.

The information entered at the time of account creation is used by myAlaska to validate identity through real-time authentication with various systems, such as the Department of Motor Vehicles (DMV), that contain verified demographic data for Alaskan citizens. Lightweight Directory Access Protocol (LDAP) is used to create the user account, which requires unique user identification (ID), a complex password, and an industry standard authentication process. The identity management process works using authentication tokens, cookies or "magic strings," e-signatures, confirmation codes, and validation codes for myAlaska portal's authentication. This methodology can easily be shared and adopted by other applications to obtain pass-along authentication, thus creating an SSO authentication system that can be used to consume services provided by the ESB.

The following services are currently accessible by individuals through their myAlaska account:

- Alaska donor registry
- Alaska Performance Scholarship and Alaska Educational Grant Information
- Alaska State Government public notice access
- Alaska Youth Court information
- Apply for the Permanent Fund Dividend (PFD) or check PFD application status
- Apply for Unemployment Insurance online
- Access Child Support financial statements
- Report a motor vehicle collision

Additional services for State of Alaska employees and public officials accessible through myAlaska include:

- Disclosure forms for public officials, legislative staff, and campaign activity
- Emergency Medical Services (EMS) certification and training information
- Lobbyist reporting
- Online application for Violent Crime Compensation Board expense reimbursement
- Online training resources
- Pay Food Worker Card fee online
- Retirement and benefits services for State employees

The myAlaska portal allows adults to create an account to access available services. Children cannot create their own myAlaska account. However, parents can apply for the PFD for their children through the parent's myAlaska account. The same method could be used to allow parental access to children's PHR whenever the parent is associated with the child in HIE repositories or DHSS databases.

Cognosante's research indicates that DHSS currently validates the myAlaska portal demographics data entered by users who applied to obtain social services through the DMV and PFD databases. DHSS utilizes a dedicated interface to the DMV and performs a six points of data check to validate information and establish identity. This sort of external data check, based on a point-to-point data interface, written using DMV's Application Programming Interface (API) is not recommended.

Cognosante recommends DHSS use its own MultiVue MCI to validate the information. This method will require the MultiVue MCI to exchange updated data several times throughout the day with the DMV and other databases as separate processes, while maintaining the MultiVue MCI's own internal database for user identity verification when users apply for social services using the myAlaska portal.

This method will decrease real-time dependency on external systems and will make the identity verification process work faster, through use of the internal MCI database, and will eliminate delays

introduced by backed up or failed interfaces. The current MCI database is already populated with the golden records of most Alaska residents. Cognosante recommends DHSS consider using it for demographics data verification. The data quality of the MCI needs to improve and will be discussed in more detail later in this section.

DHSS currently manages the MultiVue MCI and could leverage the myAlaska portal as the shared functionality for social services and PHR access. This functionality should be implemented using Service Oriented Architecture (SOA) to provide the ability to use the MCI database to validate user demographics as new applications for social services are submitted. To support HIE integration with the MultiVue MCI, DHSS should consider standardization of the data submission process or application intake process, which will reduce the on-boarding time required to integrate DHSS Division systems with the MCI.

Although the MCI is connected to the BizTalk ESB, it is not currently connected to myAlaska through an interface. Additionally, Cognosante's research indicates that myAlaska is not using BizTalk to publish or subscribe to any web services at this time. A Person Look-Up Service would need to be implemented to allow myAlaska to query client data contained in the MultiVue MCI for user validation when applying for services like PFD.

Although the MCI is connected to the BizTalk ESB, it is not currently connected to myAlaska through a point-to-point interface. Additionally, Cognosante's research indicates that myAlaska is not using BizTalk to publish or subscribe to any web services at this time. A Person Look-Up Service would need to be implemented to allow myAlaska to query client data contained in the MultiVue MCI for user validation.

The MCI was originally seeded with data from the PFD system, which includes demographic data covering 98 percent of all Alaskans and is loaded and manually updated annually. Subsequently, the following DHSS systems have been connected to the MCI using BizTalk:

- Alaska's Automated Information Management System (AKAIMS)
- Data System 3 (DS3)
- Eligibility Information System (EIS)
- Juvenile Offender Management Information System (JOMIS)
- Medicaid Management Information System (MMIS)
- Online Resource for the Children of Alaska (ORCA)

Cognosante met with representatives of DHSS IT and discussed whether the MCI data represented the golden record for client data. Feedback from DHSS IT indicated that although the MCI is a logical repository for the golden record, MCI data does not currently represent the highest quality standard or the one source of truth for golden record data. If the State of Alaska were to leverage the MCI as a validation source for myAlaska authentication, the MCI would need to be established as the repository of the golden record.

Development of standards and business processes would help DHSS IT staff responsible for maintaining MCI data improve data quality. Additionally, as DHSS implements Prism and Chroma, manual processes currently involved with data maintenance will be reduced, saving staff time.

The first step in establishing the MCI as the repository of the golden record is to standardize business processes across DHSS Divisions and systems interacting with the MCI. Merging records from several Division systems for a single client and eliminating duplicate client records in the MCI would be more efficient if source system data were consistently formatted when transmitted to the MCI.

Another step in establishing the MCI as the repository of the golden record includes requirements documentation of the MCI cross-functional views, completed in April 2013. These requirements define staff access to view or update MCI data based on user roles and business needs. Defining access to MCI data will position DHSS to create standards and business processes for client record management.

4.2.2 Connecting Public Health Registries, MMIS Data Warehouse, MCI, and HIE

In order to create access to PHR data through the myAlaska portal, confidential Public Health Registries, MMIS Data Warehouse, the MCI, and the HIE must be accessible by the myAlaska portal. This requires development of interfaces as well as reviewing and addressing any security concerns. The Health Insurance Accountability and Portability Act (HIPAA) and Affordable Care Act (ACA) require that PHI data must be stored in a password-protected database with the PHI fields encrypted with 128-bit encryption or higher. It also requires similar protection and encryption for the PHI data while in transmission in between the user's computer and the DHSS databases, so that the data packets cannot be captured and protected information cannot be stolen. The myAlaska portal must use 128 bit or higher encryption using Hypertext Transfer Protocol Secure (HTTPS), Secure Sockets Layer (SSL) for PHI data transmission and user authentication. The whole computing infrastructure related to the myAlaska portal, Public Health Registries, MMIS Data Warehouse, the MultiVue MCI, and the HIE, including all servers and databases that store, cache, or relay PHI, must also go through verification that they meet the minimum security requirements set by law.

4.2.2.1 Interfaces

Interfaces are used to transfer data from one system to another. In the absence of an ESB, interfaces tend to be point-to-point, transferring data only between two specific systems. Point-to-point interfaces are common between older legacy systems. To promote reusability and comply with CMS Seven Conditions and Standards and ACA requirements, DHSS could use the BizTalk ESB to create interoperability between the MCI, myAlaska, and the DHSS systems currently connected to the MCI, for demographics related data verification, validating identity, and sharing and updating PHI data.

However, developing interfaces between the MCI, myAlaska, the MMIS Data Warehouse, and HIE repositories would be a complex project because it would require planning, stakeholder input, coordination with multiple agencies, requirements gathering, security compliance, and near real-time interoperability between each of the applications involved. The Department may want to consider development of a Request for Proposal (RFP) to secure a vendor to manage the implementation of an interoperable, near real-time interface between the MCI, myAlaska, and the DHSS systems currently connected to the MCI, interchanging data using the ESB.

The ESB is one component that could support access to PHR through the myAlaska portal. Other components include the HIE Repositories, Laboratory Information Management System (LIMS), Electronic Laboratory Record (ELR) files, the MMIS Data Warehouse, and the MultiVue MCI. Additionally, the ESB must be fully implemented, as described in this document, to allow near real-time interoperability with each of its associated systems before it can support PHR access through myAlaska.

4.2.2.2 Sharing LIMS Electronic Laboratory Records through myAlaska

Currently, the LIMS is delivering Electronic Laboratory Records (ELR) using Direct Secure Messaging (DSM). This is accomplished using Health Information Service Provider (HISP) services and the Alaska electronic Health Network (AeHN) HIE. The DSM messages include lab results in both PDF and Health Level 7 (HL7) file formats. DSM messages are handled by Orion Rhapsody interface engines using the DIRECT protocol as the primary transport mechanism. This LIMS interface does not currently utilize the enhanced functionalities that the BizTalk ESB can provide.

However, security concerns will need to be addressed to ensure compliance with HIPAA and ACA requirements for the sharing of ELR, regardless of whether or not the ESB is used to expose the PHR through the myAlaska portal. DHSS should conduct detailed, technical analysis of the current security architecture before the BizTalk ESB is used to share PHR data through myAlaska. The results of this analysis would expose any vulnerability DHSS would need to address during interface development.

To provide access to ELR data through the myAlaska portal, DHSS can develop web service interfaces using the BizTalk ESB, which will provide integration between the LIMS and the PHR.

The ACA and HIPAA regulations require encryption of PHI while stored and during transmission. If myAlaska is used to view or exchange PHR data, HTTPS, with Secure Sockets Layer (SSL), with 128 bit or higher encryption must be used to transmit all PHI data.

Caution must be exercised when a mix of unencrypted Hypertext Transfer Protocol (HTTP) and encrypted HTTPS protocol is used. Rigorous testing is required to ensure compliance with all security regulations and standards. Any database physical or virtual backup files, delta files, redo files, redo logs, and flat files containing PHI data must also be encrypted and password-protected.

4.3 MCI Interoperability Implementation Plan

The MCI interoperability implementation plan is an enterprise level plan that requires all applications and shared services connected through the ESB to use the MCI when validating and updating personal demographic data. Identity validation using the MCI is different than the functionality provided by an Identity Management Service, described in Section 5.5.5.

This MCI interoperability implementation plan describes the major tasks associated with implementing near real-time connectivity between the MCI and its associated systems.

4.3.1 Assumptions

The following assumptions were used in the development of the high-level MCI interoperability implementation plan included in this section:

- DHSS IT will create a data dictionary or data definitions for the MCI
- DHSS IT will ensure data interoperability complies with requirements for PHI

4.3.2 Major Implementation Tasks

In order to implement near real-time interoperability between the MCI and its associated systems, DHSS will need to complete the following tasks discussed in the ESB Implementation Plan Section 3.5.2 and its subsections including:

- Project Management
- Implementation team and stakeholder identification
- Determine maintenance location and team
- Security
- Complete system documentation
- Establish Acceptance Criteria
- Technical and Functional Testing for Technical Services and Business Services
- User Acceptance Testing (UAT)
- Production roll-out

In addition to these tasks that are common to most system implementations, DHSS IT will need to complete the following tasks specific to the implementation of MCI interoperability.

4.3.2.1 Complete Implementation of Prism and Chroma Tools

The Enterprise Roadmap Phase I recommended completion of an MCI Architectural review to determine if changes were needed to the current implementation of the MultiVue MCI. Cognosante completed the MCI Architectural Review in March 2013 and based on those recommendations, DHSS is moving forward with the use of the data quality and governance tools Prism and Chroma. Prism provides the ability to create data views, improves data matching, and makes it easier to generate reports from the MCI database. Chroma manages updates to the golden record and reduces the need for manual intervention when resolving duplicate data. Implementation of these tools should be completed prior to beginning MCI interoperability implementation.

4.3.2.2 Implement MCI Architectural Review Recommendations

To achieve near real-time interoperability between the MCI and the currently connected Division applications, DHSS IT will need to implement the recommendations documented in the MCI Architectural Review including:

- Utilize the integration engine capabilities of BizTalk to transform data requests to standard formats for submission to the MultiVue MCI for match processing
- Standardize the data submission process to decrease the time required to integrate DHSS Division systems
- Implement a shared Web Service with the BizTalk ESB to support real-time access to the MultiVue tool
- Determine the transaction volumes anticipated during the ACA Medicaid open enrollment period, which begins on October 1, 2013, and perform volume stress tests to ensure sufficient capacity to handle the expected number of applicants
- Review BizTalk hardware to determine fault-tolerance, high-availability capability, and processing capacity

4.3.2.3 Create an MCI Data Dictionary

A data dictionary is a repository used by system administrators and developers to maintain system documentation regarding the architecture, configuration, and maintenance of system hardware and software. DHSS IT should consider creating a data dictionary for the MCI. Without a proper data dictionary or a data definition document it will be more difficult to utilize the MCI at an enterprise level and maintain standards and consistency.

4.3.2.4 Validate the Unique MCI Client Identifier

A unique client identifier is different than a system generated record number that is created automatically within the MCI. DHSS IT may want to validate that the unique MCI client identifier field has at least eight digits to ensure it will accommodate a virtually unlimited number of unique clients and eliminate the possibility that the number of clients will exceed the available identifiers. An incremental algorithm can be used to give an accurate count of the number of individual clients within the MCI. This provides an accurate count of the number of MCI clients without having to run a report. More information on the virtues of using a unique identifier, rather than using an SSN to identify a person can be found later in this document.

5.0 SHARED FUNCTIONALITY

Shared functionalities, also referred to as shared services, consolidate business operations used in multiple areas of an organization to promote efficiency, reduce costs, decrease redundancy, and promote consistency across an organization.

When implementing shared functionality/services, systems can be broken into component parts or modules. The modules that represent a common functionality used in more than one part of the organization can be shared by all agency divisions. Divisions can create extensions to configure a shared service to meet their specific needs. When implemented using a shared services model, the baseline functionality of an application or a service can be updated without affecting the functionality of the other associated applications or services.

Using a shared services model decreases duplication of functionality and reduces the costs of implementing those functionalities throughout the Department. A shared services model also makes it easier to deploy subsequent customizations or upgrades without breaking custom functionality. Common services can also be leveraged across lines of business (LOB), reducing redundancy and lowering the total cost of ownership (TCO). Standardizing services also enforces uniform data definitions across LOB and divisions, allowing for consolidation of data storage and access routines. Master Data Management (MDM) is improved by storing data on common repositories, breaking down traditional LOB or Division-level data silos.

An Enterprise Service Bus (ESB) like BizTalk is required to share services because it provides a common gateway and translation mechanism for all kinds of applications written in different programming languages, using different versions and types of Application Programming Interfaces (APIs), running on different software Operating Systems (OS) and hardware platforms. An ESB allows efficient, near real-time communication between systems by following a set of common rules and communicating via a simple interface.

An example of a shared service for public consumption is a public-facing web interface to the State of Alaska employee directory where Alaskans can search employee contact information by entering the employee's name and agency. Therefore, instead of keeping a list of state employees and their contact information on that website's local database, and maintaining that information as people join or leave State employment, a simple shared service with about five read-only data fields from the State's Human Resources Department's database can provide fast, accurate, and up-to-the-minute information.

A shared functionality/service for an internal consumption could be a simple messaging interface that adds or updates client information in the MCI database when users with the appropriate role and permissions enter updated information. Standards and business processes for acceptable verification would ensure only verified information resulted in an update to MCI client data. Birth certificates, marriage certificates, and other legal documents are examples of verification sources that business processes could require before updating MCI client data. Prior to implementing each shared service, the Department of Health and Social Services (DHSS) will want to define the data that each shared functionality receives and makes available for consumption through the ESB.

Business analysts, programmer analysts, project managers, and others work together to create shared functionality/services. DHSS Information Technology (IT) staff responsible for exposing the shared functionality/service also need to work closely with those developing and maintaining applications and services and those maintaining the BizTalk ESB, Business Rules Engine (BRE), and business process workflows. Cognosante recommends establishing a team dedicated to development of these functionalities.

5.1 Shared Functionality and MITA

Consistent with Medicaid Information Technology Architecture (MITA) and the Centers for Medicare and Medicaid Services (CMS) Seven Conditions and Standards, shared functionality increases efficiency by promoting reuse and reducing duplication across the Health Information Technology (HIT) architecture. Rather than creating a particular functionality in each system, an ESB is used to expose an application or functionality for consumption by multiple systems. The result is effective use of HIT funding both within Divisions and across DHSS, as well as standardization of services, data formats, and data utilization. Use of standardized functions enforces MDM throughout the Department.

When implementing shared functionality, it is helpful to understand the full architecture of the solution. MITA provides the definition of the architecture and helps define the role of components in the system. MITA encourages the automation of common business processes using web services. Web services encompass standards that enable applications to communicate and exchange data over the internet (or intranet) across many sites and organizations. Developing common data and information standards enables interoperability across different platforms. Integration of applications and modular programming enables the incremental introduction of change and leverages existing information assets.

Developing (or procuring) and implementing shared functionality modules requires definition of the business, information, and technical architectural layers of the system. This MITA-based approach results in creating a logical architecture for the enterprise architecture. This comprehensive logical architecture includes business, information, and technical architectural layers.

Table 3: MITA-based Logical Architecture

MITA-based Logical Architecture	
Architecture	**Description**
Business Architecture	The Business Architecture summarizes vision and objectives required to operate the Exchange and define all of the Business processes into functional areas (groupings of business functions). Functional areas are comprised of one-to-many modules or components. Each component contains a discrete set of business processes needed for a specific purpose or task.
Information Architecture	Information Architecture aligns data and information needs with business requirements. Business processes and capabilities from the Business Architecture are mapped to a conceptual data model and a logical data model. The interface requirements of each module are matched in this process to ensure that correct data elements are identified and built into the interface definition.
Technical Architecture	Technical Architecture compiles models and approaches to support the business and information needs of the Alaska HIT architecture.

The resulting architecture includes business and data access services, modular application architecture, and interface definition. Collectively, these elements create a set of business services, interoperability, connectivity, and data standards that define the business framework of the enterprise architecture.

By implementing MITA and adhering to its guidelines and principles, DHSS can create well-defined business, interface, and technical architectures. The design provides the flexibility to allow Alaska to select and replace individual modules within the architecture.

5.1.1.1 Identification of Reusable Services

Reusable services can include new shared services and sharing functionality that currently exists in Department applications. An example of a new shared service in a Service Oriented Architecture (SOA) based application might be a security service. SOA-compliant applications have a code base that is

modular and exposed for sharing. In a legacy system, class libraries linked into new applications could be identified as a service with the potential to be reused and shared. However, modifications may be needed to enable legacy systems to expose functionality for consumption by other applications.

5.1.1.2 Enabling Shared Application Services in Legacy Systems

DHSS IT will need to make changes to the coding of the existing legacy applications in order for them to expose services for consumption and become SOA-compliant. Enabling services includes many variables, such as the development environment used, the existing system architecture, the type of code each application uses, and the associated APIs. SOA-compliant applications are designed to work with an ESB to expose services for consumption by other applications. However, legacy applications can also be modified to work within an SOA framework, and utilize ESB connectivity. The shared functionality/services implementation plan in Section 5.6 will provide more information about enabling shared functionality/services.

There are several ways to enable or expose services within legacy applications. Three of those methods are briefly discussed below.

5.1.1.2.1 Direct Code Changes to the Legacy Application

Applications that are developed in-house can be modified and restructured to create independent blocks of code. Developers create a wrapper so that a block of code can be used as a function of a service. Applications that are developed by third-party vendors or commercial off-the-shelf (COTS) products may require vendor coding to create the ability for a block of code to be exposed and used as a shared functionality/service. Some license agreements may restrict the ability to modify application coding.

5.1.1.2.2 Use a Third-Party Product

There are several third-party commercial products available that help service-enable legacy applications. Many of these products specialize in enabling legacy mainframe applications to support shared services. One example of this type of third-party product is IBM's WebSphere Information Integrator Classic Federation for z/OS.

5.1.1.2.3 Application Re-Hosting

Some legacy applications are written in such a way that it may be easier to re-write the application from scratch than trying to change the code to make it SOA-compliant or service-enabled. This can be due to constraints imposed by the hardware or the software architecture that is used to host the legacy application. Although complex, one method that can be used is to port the application from its legacy environment to a modern Linux or Windows-based virtual environment or to virtual ports. This methodology is usually used as a last resort due to the level of complexity. There are several products like VMware and Ubuntu Linux that can be used to automatically re-host an application from one system to another. For example, an application could be re-hosted from a mainframe system to UNIX or from UNIX to Windows, without changing any of the application’s native code.

5.2 Commonly Deployed Shared Functionality/Shared Services

There are several types of shared services commonly implemented by health and human services agencies, including shared services and functionalities for public consumption and shared services for internal applications. Any shared service, regardless of intended audience, needs to meet all State of Alaska and DHSS security requirements and comply with Health Insurance Portability and Accountability Act (HIPAA), the Health Information Technology for Economic and Clinical Health (HITECH) Act, and the Affordable Care Act (ACA).

5.2.1 Case Management as a Shared Service

Many of the Department's health-related applications include some level of case management functionality. Because of the potential for eliminating redundancy and improving efficiency, Cognosante evaluated the risks and benefits of implementing case management functionality as a Department-wide shared service.

The DHSS systems containing case management functionality also support a variety of services to distinct client populations, each with specific program requirements, business processes, workflows, and funding streams. While there are several COTS products on the market that support case management activities, to implement case management as a service, functionality needs to be separated into smaller, more modular capabilities.

For example, many of the programs DHSS administers include grievance and appeals processes. Clients may appeal a Department decision regarding their benefits and services or raise an issue with the level of customer service provided. Staff from each program document appeal requests, gather data about Department decisions and customer service, track steps in the appeals process, and document findings. Rather than implementing this functionality in each case management system, DHSS may want to consider implementing one grievance and appeals shared service that each Division application or program could leverage.

Another example of case management functionality that could be shared across programs and Divisions is fraud, waste, and abuse tracking. Virtually every program requires fraud detection, tracking, and management. Some agencies consolidate these activities into one unit with a specific fraud case management system. This approach requires staff from every program to pass fraud-related data to the consolidated unit. While there are some benefits to this approach, there is also a risk that information will be lost or that staff outside the fraud unit will have a reduced focus on fraud detection and reporting. Another approach is to implement fraud, waste, and abuse functionality as a shared service. This would allow staff in each Division to continue to detect, report, and document fraudulent activities and allow fraud investigation staff to utilize the same shared service to track and monitor individual cases throughout the process.

Incident tracking is another example of a case management functionality that can be utilized as a shared service. Multiple programs document, report, and track incidents that occur during service delivery. By leveraging a shared service, the Department could increase consistency and improve data quality. Implementing incident tracking as a shared service would also improve the ability to view this data across programs and provide an enterprise-level view.

The MultiVue Master Client Index (MCI) is an example of a client demographics shared service that can interact with major Department applications that include case management functionality. Enhanced interoperability between the MCI and the Divisions' systems will provide data needed for improved coordination of services and improve the quality of DHSS client data.

The Department may want to consider leveraging these shared services as well as shared components such as a BRE and business process workflow engine to improve case management system efficiency while reducing redundancy, costs, and staff time.

The Department should also explore opportunities to align and create consistency in case management business processes and workflows across the Divisions. Increasing standardization creates additional opportunities to leverage shared services and minimize the scope of customized functionality in the case management applications.

5.2.2 Electronic Document Management System as a Shared Service

Electronic Document Management System (EDMS) is a candidate for shared services. Each Division within the Department is required to collect, process, manage, store, retrieve, maintain, and provide search capability for documents as an integral part of day-to-day operations. Supporting these processes requires each Division to have an array of document management capabilities and technologies. Documents for a given individual are stored in separate repositories, requiring different access technologies, separate storage, maintenance, and product licensing costs, as well as different business processes, retrieval, and search procedures. The end result for DHSS is duplicate costs across Divisions, lack of standardization of business processes, and difficulty in sharing or retrieving documents for the same individual across different systems.

Differences in each Division's business processes and storage needs make this one of the more challenging functions to implement as a shared service. However, the evolution of EDMS to a shared function offers the following potential benefits to Alaska:

- Total lower cost of ownership: elimination of multiple technology and consolidation of current document storage reduces product license and maintenance costs, and allows DHSS to leverage economy of scale for storage of larger documents
- Reduced Duplication of Documents: a single repository also minimizes the potential duplication of documents across different Division level repositories
- Improved Access: leveraging shared services standardizes storage and access routines across the Department, allowing multiple Divisions the capability to securely search for and access documents appropriately
- Standardized Business Processes: document workflow and processes can be automated and standardized across the Department, improving the ability of different Divisions to access documentation. Workflow can be automated across Divisions for documentation notification, eliminating the need to electronically or physically pass documentation from one Division to another. Alerts and notifications can be automated as part of the centralized workflow
- Centralized Security: with a shared repository, document security is centralized, which reduces the security risks incurred with multiple repository environments

Implementing this solution is challenging due to differences in the business processes, document types, workflow, storage requirements, and access needs of each Division. Implementing EDMS as a shared service will require more than selecting the right technology component. Each Division's requirements will need to be documented in order to develop EDMS as a shared service and to ensure understanding of the current documentation needs. The following requirements will need to be documented:

- Current document storage and access needs
- Current physical storage requirements and projected growth rates
- Types of documents currently stored and anticipated future document types
- Division business requirements and processes
- Identify common storage, access, and retrieval needs to standardize business processes across Divisions
- EDMS solutions require multiple supporting capabilities and technologies including imaging (generally scanning), form creation, form workflow processing, and enterprise report access.
- Identify and evaluate tools that provide capabilities to link capabilities and technologies into an integrated solution
- Plan integration of the EDMS with the MultiVue solution

Cognosante recommends DHSS proceed with establishing EDMS as a shared service. Work will be required to identify common storage and retrieval requirements across Divisions and implement these as the initial services for the EDMS shared service. The Department will also need to gather statistics for current and future data storage requirements to accurately price the solution and procure the necessary storage.

5.3 Shared Functionality/Services Hosting

The term hosting in this section refers to the system in which the shared functionality would be supported. For example, if a shared functionality were implemented as part of the Master Client Index (MCI), we would refer to the MCI as hosting the shared functionality.

Cognosante's research found that Eligibility Information Systems (EIS) and Medicaid Management Information Systems (MMIS):

- Often contain the majority of an agency's clients
- Send a large volume of paper notifications to clients and providers
- Receive a large volume of mail returned due to incorrect address
- Eligibility Systems must interoperate seamlessly and in real-time with the Federally Facilitated Exchange (FFE)
- Eligibility systems must include the ability to apply for health coverage online

Therefore, as agencies replace their MMIS and EIS, Systems Integration Request for Proposals (RFPs) are requiring vendors to include many of these shared functionalities/services. For example, the *State of Iowa, Department of Human Services, Iowa Integrated Eligibility System (IIEP) RFP* required the replacement system to provide the following services:

- Address Validation Service to validate addresses with the United States Postal Service (USPS)
- Person Look-Up Service to locate existing clients and prevent addition of duplicates
- Person Add/Update Service to allow users to view and update data based upon the user's role
- Softcopy Correspondence Generation Notification Service to provide/distribute the applicable notices, pamphlets, communications and forms via email

The Alaska Eligibility Information System-Replacement (EIS-R) RFP included the following functionality in the replacement system. Cognosante has included the related shared functionality/service that could meet the EIS-R requirement.

- Person Look-Up Service – "The system must perform a broad person search to determine if the person is already known to a system in the State, in a way that is transparent to the user."
- Address Validation Service – "The system must be able to validate the mailing address" and "The system must contain an address validation function that will automatically populate the additional four digits of a Zone Improvement Plan (ZIP) code and alert the Eligibility Technician (ET) if the address entered is not valid."
- Address Look-Up Service – "The system must alert the ET if an address is the current address on another open case."
- Person Add/Update Service – "The system must allow an ET to change a client name" and "The system must allow an ET to add a client alias."
- Softcopy Correspondence Generation Notification Service – "The system must contain email functionality for client contact." Cognosante assumes email content would include softcopy notices.

- Hardcopy Notice Sending Service – The EIS-R RFP contains detailed requirements that include batch jobs for centralized notice printing, stuffing, and mailing, including the ability to print USPS bar codes on envelopes for bulk mailing.

Health Information Exchange (HIE) system RFPs, such as the *State of Oklahoma, American Recovery and Reinvestment Act (ARRA) HIE/Electronic Health Record (EHR) Design, Development, and Implementation (DDI) Enhancement Project RFP*, often include the following shared functionalities/services:

- Person Look-Up Service
- Person Add/Update Service
- Person Record Locator Service
- Provider Directory

The *Arkansas MMIS AME Core Systems and Services RFP* includes the following shared functionalities/services:

- Person Look-Up Service (Members)
- Address Validation Service
- Address Look-Up Service
- Person Add/Update Service
- Provider Directory
- Payment Processing Service
- Hardcopy Notice Sending Service
- Softcopy Correspondence Generation Notification Service

Table 4 summarizes the information above and identifies which shared services vendors were required to provide as part of recent EIS, HIE, and MMIS implementation RFPs.

Table 4: Common Shared Services Required by Recent EIS, HIE, and MMIS Implementation Procurements

Common Shared Services Required by Recent EIS, HIE, and MMIS Implementation Procurements	
Shared Functionality/Service	**Type of System Replacement RFP Requiring Each Shared Service**
Person Look-Up Service	EIS, HIE, or MMIS
Address Validation Service	EIS, HIE, or MMIS
Address Look-Up Service	EIS or MMIS
Person Add/Update Service	EIS, HIE, or MMIS
Person Record Locator Service	HIE
Identity Management Service	EIS or HIE
Provider Directory	HIE or MMIS
Identity Proofing	EIS (Online Application for Health Coverage)
Payment Processing Service	MMIS
Hardcopy Notice Sending Service	EIS or MMIS
Softcopy Correspondence Generation Notification Service	EIS or MMIS

5.4 Shared Functionality/Shared Services Architecture

The ESB provides the functionality that is essential for sharing services at an enterprise level. The BizTalk architecture DHSS IT deploys will significantly influence ESB speed and performance for service brokering, asynchronous queuing, processes event-driven messaging, and performing dynamic service composition and/or service orchestration.

Health and human services agencies are moving towards the use of automatic validation through JavaScript, .NET, PERL, or Java-supported Graphical User Interfaces (GUIs). As an example, Person Look-Up Services can be configured to query MCI data as information is entered into each demographic field, rather than pending the query until all fields have been completed. DHSS should plan to define the data that is received and made available for consumption through each Shared Functionality/Service.

Cognosante created the following high-level shared services architecture to illustrate potential architecture of the BizTalk ESB, MultiVue MCI, and shared services. The figure below includes shared services that are independent of DHSS applications as well as shared functionality included in a DHSS current (or future replacement) application that could be exposed and shared by the ESB for consumption by other DHSS applications.

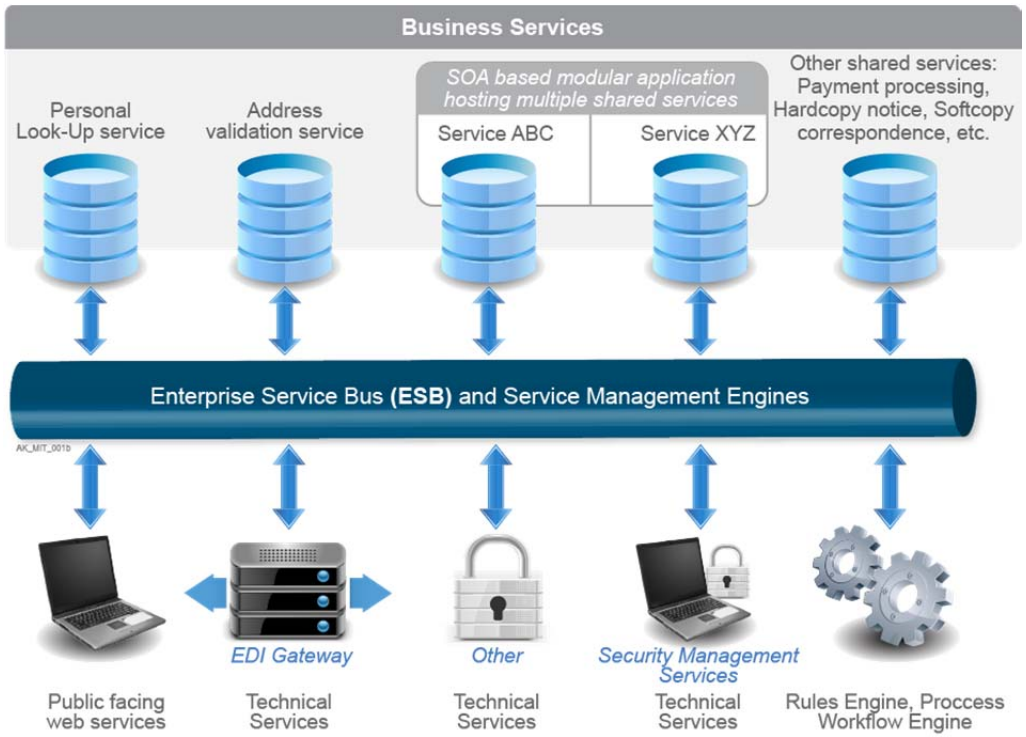


Figure 4: High-Level Shared Services Architecture

5.5 Priority Shared Functionality/Services

Cognosante researched shared services commonly deployed by health and human services agencies to increase efficiency and productivity, while reducing costs. Cognosante identified areas of focus that the Department may want to consider when determining the highest priorities for shared functionality/services. Factors considered included:

- The number of DHSS Divisions or applications that would benefit from the shared service

- How well implementation of the service supports DHSS next steps for the BizTalk ESB and MultiVue MCI
- The potential of each service to provide a "quick win" for the Department
- The level of increased efficiency, time and cost savings
- Ability of the service to increase productivity
- Potential reduction in manual tasks

As existing systems are prioritized for replacement and system maintenance contracts renegotiated, there may be additional shared services that DHSS should consider implementing. The services described in detail in Sections 5.5.1 through 5.5.4 are suggested as potential priorities for DHSS. These recommendations are not exhaustive but describe services that have been successfully implemented in other health and human services agencies that may provide opportunities as DHSS continues to move forward with a shared services model.

5.5.1 Person Look-Up Service

One of the most common shared services health and human services agencies deploy is Person Look-Up. A Person Look-Up Service consists of person demographic information such as first name, middle name, last name, suffix (title), Date of Birth (DOB), Social Security Number (SSN), and gender. Additional fields can be included as required, but these data elements provide a high degree of accuracy when querying MCI data and identifying matching records. These data elements are typically included when creating the golden record.

5.5.2 Address Validation Service

An Address Validation Service checks the address the user enters against a national database of valid addresses such as the USPS or Google address that supports geo-coding, ZIP code, and other verification. For example, when a user enters a client address with only the five-digit ZIP code, the Address Validation Service may return the same address with the "plus four" ZIP code extension for the user to select. If the user has entered a house number that does not exist, the Address Validation Service may return the closest valid address to the one entered for the user to verify and select. If the original entry was correct, the user has the ability to add the non-standard address, based on business processes and organizational standards. For example, legal restrictions may require an agency to use the address entered by an applicant or tax filer, even if the address is inconsistent with USPS known addresses.

5.5.3 Address Look-Up Service

An Address Look-Up Service checks the address the user enters against the existing address information for that individual in a database, such as the MCI. It is also used to validate address information against the golden record data. The golden record address information is only updated when information is received from a trusted source of verified data such as state tax records, Permanent Fund Dividend (PFD) applications, or EIS data verified during the benefit application process.

5.5.4 Person Add/Update Service

Another common shared functionality health and human services agencies deploy is the Person Add/Update Service. This is different from a Person Look-Up Service. While a Person Look-Up Service provides downstream, read-only data from the MCI for verification purposes, it does not perform data updates. However, a Person Add/Update Service can add new person records as well as providing the ability to update existing records.

Cognosante recommends DHSS separate the Person Look-Up and Add/Update services. This is a best practice because it adds an extra layer of protection by separating the ability to query from the ability to

update. However, if DHSS prefers, both services can be combined to create a Person Service. The advantage to the combined service is reduced complexity and easier development of the service.

Security for accessing the Person Add/Update Service should be limited to the appropriate DHSS staff. If the Person Add/Update Service were shared with multiple Department systems, security roles and permissions should be defined. The Person Add/Update Service that would update the MCI data should only be available to users with the proper level of security access to update the golden record. If a user without the proper security access tries to update MCI data, the Person Add/Update Service should return a default error code and notify the ESB for incident logging. These security standards maintain data quality and minimize data errors and corruption.

5.5.5 Additional Shared Functionality

In addition to the priority shared functionality previously described, health and human services agencies often implement the shared functionalities mentioned in Sections 5.5.5.1 through 5.5.5.7. DHSS may also consider implementing these services based on Department priorities.

5.5.5.1 Person Record Locator Service

A Person Record Locator Service identifies where records are located based on client data such as name, SSN, DOB, etc. This service also allows the appropriate staff to update record location information. Data can be returned based on simple criteria, such as client data or based on detailed criteria, depending on the business need. A Person Record Locator Service typically includes the following functionality:

- Retrieves record locations with information associated with a specific person
- Locates context-sensitive information based on data matching requirements
- Provides information about the types of information or topics stored in a given location
- Identifies the topics that will message a given location
- Determines requirements for storing person data and record locations

5.5.5.2 Identity Management Service

An Identity Management Service is used to automate security related maintenance tasks such as creating unique user identification (ID), complex password, and resetting user passwords when needed. Because a large percentage of help-desk calls are password-related, a service that allows users to reset their own passwords can save significant IT resource time and expense. A Single Sign-On (SSO) service, like that provided by myAlaska, allows access to multiple applications with a single password. Health and human services agencies often use identity management to increase security and productivity, while decreasing cost and reducing redundancy.

5.5.5.3 Provider Directory Service

Provider directories not only store a listing of providers, but they include associated provider information such as the National Provider Identifier (NPI), Unique Physician Identification Number (UPIN), Medicaid Provider Number (MPI), Drug Enforcement Agency (DEA) number, state licenses, credentialing, practice name, practice location, contact information, and medical specialty. One benefit of Provider Directories is that they allow consumers to access information about providers to increase choice and transparency. Health and human services agencies use Provider Directories for Medicaid claim processing or when establishing a medical home for a Medicaid client. Provider Directories are also an important component in HIE architecture, where they reliably discover and confidently identify provider participants. These can be both individual providers as well as provider organizations.

5.5.5.4 Identity Proofing Service

An Identity Proofing Service verifies that an individual creating a user account is the same person whose identifying information is being provided. This service is used prior to a user account being created. In addition to personally identifying information such as name, SSN, and DOB, life history events or financial transaction data available from public and private data sources is used to validate the identity of the person attempting to create a user account. In addition to account creation, the Identity Proofing Service is used to authorize transactions that access sensitive or confidential information such as Protected Health Information (PHI).

5.5.5.5 Payment Processing Service

Payment Processing Services are often divided into two separate services for convenience:

1. Credit/Debit/Automated Teller Machine (ATM) card processing
2. Electronic Check Processing

Both services receive funds from the payer's account, process payments, and deposit the funds in a state account or to the account of an authorized service provider. These services typically do not process refunds or credits that return funds to an individual's credit card or bank account. To process refunds or returns, an Outgoing Payment Processing Service would be used.

Medicaid agencies often collect premiums from higher income clients. Long-term Care (LTC) services agencies often require patients to participate in the cost of their care or pay a share of cost. Child support agencies collect support from non-custodial parents when children receive Temporary Assistance for Needy Families (TANF) benefits or for distribution to the custodial parent. Recovery units are often used to collect overpaid Supplemental Nutrition Assistance Program (SNAP) and TANF benefits resulting from inadvertent household errors, agency errors, and fraud. Because many Department applications may use a Payment Processing Service, it is often implemented in a central location as a shared service.

5.5.5.6 Hardcopy Notice Sending Service

The Hardcopy Notice Sending Service can be used by any agency or Division that is required to send paper notices to clients. Historically, agencies have achieved efficiency by contracting with a vendor to accept electronic notices and handle printing, stuffing, postage metering, and mailing tasks in a consolidated facility or business unit.

The Hardcopy Notice Sending Service is frequently being implemented as a shared service that may or may not have a web interface. To use this service, each Division submits their notice jobs and provides all necessary information in a pre-defined Extensible Markup Language (XML) format to the Shared Service. That information is sent to a unit or vendor or centralized unit that prints, processes, and mails the notices. When regulations allow, notices can be sent to third-party vendors that offer Hardcopy Notice Creation and Mailing Services directly from a mail processing center using the XML feed created by the ESB. These shared printing and mailing facilities offer services that are more cost-effective than if each Division printed and mailed its own notices.

5.5.5.7 Softcopy Correspondence Generation Service

The Softcopy Correspondence Generation Service is used to send correspondence via email, text messages, or Interactive Voice Response (IVR). Because the ACA encourages use of these additional communication methods, many health and human services agencies are exploring Softcopy Correspondence Generation Services. By implementing this functionality as a Shared Service, costs and redundancy can be reduced.

However, Softcopy Correspondence Generation Services often require a large number of technical resources to maintain the correspondence generation Simple Mail Transfer Protocol (SMTP) gateways, Short Message Service (SMS) gateways, and IVR servers. Efficiency can be gained by consolidating smaller groups that maintain each of these services into one unit. Existing DHSS IT staff may also need training to maintain this service, if DHSS decides to implement it. Because of the relatively small number of DHSS clients, this service may provide a lower return on investment than in larger states.

5.6 Shared Functionality/Shared Services Implementation Plan

Using services not only reduces the amount of deployed code, but it also reduces the management, maintenance, and support burden by centralizing the deployed code and managing access to it.

5.6.1 Assumptions

Cognosante developed this high-level shared functionality/services implementation plan using the following assumptions. DHSS IT will:

- Build and maintain business rules using BizTalk's internal or other enterprise BRE
- Build and maintain business processes and/or workflows
- Define process maps using Business Process Modeling Notation (BPMN)
- Define and manage all message related requirements for the ESB
- Define all data interchange, Electronic Data Interchange (EDI) gateway, and data mediation requirements for the ESB
- Define and manage legally required logging infrastructure
- Define new processes, test, and implement using Business Process Execution Language (BPEL)

5.6.2 Major Implementation Tasks

In order to implement shared functionality/services, DHSS will need to complete the following tasks discussed in the ESB Implementation Plan Section 3.5.2 and its subsections including:

- Project Management
- Implementation team and stakeholder identification
- Determine Maintenance Location and Team
- Security
- Complete system documentation
- Establish Acceptance Criteria
- Technical and Functional Testing
- User Acceptance Testing (UAT)
- Production roll-out

In addition to these tasks which are common to most system implementations, DHSS IT will need to complete the following tasks specific to shared functionality/services.

5.6.2.1 Granularity of Shared Services

Shared Services may be implemented with different levels of granularity. Granularity describes the level of functionality covered by one interface or service. In order to support maximum reusability, shared functionality/services should be implemented to provide small sets of functionality. This approach will enable DHSS IT to build combined and complex services composed of several more granular services.

This approach would allow DHSS IT to implement new services whenever a business need is identified, because developing the new services would require minimal work. DHSS will need to decide the level of granularity for each shared service.

5.6.2.2 Installing Shared Services Using BizTalk ESB

Cognosante recommends utilizing BizTalk's ESB functionality to implement shared functionalities/services. However, it is also possible to directly communicate with the Shared Service Provider bypassing the ESB. Increased data interchange speed is one of the most common reasons for doing so. This method is risky and creates a bottle neck for other services. Special care must be taken if this method is used. Only systems that have the same software and hardware architecture can take advantage of this methodology. Even then, systems cannot always communicate directly and an ESB is needed to complete mediation tasks.

5.6.2.3 Define the Runtime Topology of the BizTalk ESB

When IT Departments share services using an ESB as part of an SOA- and MITA-compliant architecture, system administrators need information about the interaction between available services. System maintenance is easier and more efficient when system administrators know which services are interacting with each other and specifically when the interactions are occurring. This is referred to as Runtime Topology and the resulting data will provide DHSS IT with a better understanding of ESB system composition. DHSS IT can use Runtime Topology data to develop an ESB maintenance plan and determine when to install service upgrades.

By defining the Runtime Topology, DHSS IT can use BizTalk's administration module to manage the nodes and services running within the ESB. Having a well-defined Runtime Topology is also very important when testing the test environment version of BizTalk. In order for BizTalk to be production-ready, it must go through proper testing and UAT. The entrance, exit, and acceptance Criteria for BizTalk to be promoted from the test environment to the production environment depends on many variables, including meeting the Service Level Agreement (SLA) for each service.

DHSS IT can review the SLA and Service Policy compliance in real-time, using BizTalk's administration module. For example, the Runtime Topology may require the Address Lookup Service to have an average response time SLA of 100 milliseconds or less in order to be compliant. By constantly monitoring the SLAs, BizTalk's administration module can provide DHSS IT with information needed to ensure a high-quality service that is fast enough and acceptable to those using it. If the system fails to maintain the SLAs, the BizTalk administration module allows DHSS IT to view the performance metrics of each data field. This provides IT staff with enhanced ability to troubleshoot issues. Graphic charts and data are also included that provide a visual comparison between the target and the actual data for each service. These graphs and charts are useful tools to verify the overall health of the production system.

BizTalk allows management, viewing, and maintenance of each node and node group. It also allows real-time viewing of the resources used by servers, shared services, dynamic services, and clusters, as well as the modules under each node. Although the BizTalk Administration Console is a valuable tool for viewing resource consumption in real time, it consumes a large percentage of the available system resources. DHSS IT may want to consider restricting the use of the BizTalk Administration Console to a small number of IT staff, in order to manage system resources.

5.6.2.4 Implement Recommended Software and Hardware Updates

DHSS should review the hardware and software components that will be used to share services and implement any recommended updates. This includes developing an installation schedule and creating appropriate documentation.

5.6.2.5 Identify DHSS IT Staff Training Needs

SOA Governance recommendations and a comparison of the skill sets needed to develop and maintain shared services to the current IT resource skills, will allow DHSS to address any IT staff training needs. It may also be appropriate to consider adding additional staff with experience developing and maintaining specific software applications.

6.0 SUCCESSFUL PROCESS CHANGE REQUIRES CULTURAL CHANGE

As the Department moves toward enterprise architecture consistent with Medicaid Information Technology Architecture (MITA) and Service Oriented Architecture (SOA), changes to business processes, procedures, and paradigms will be as significant as changes in technology. Division leadership and managers will need to look for opportunities to leverage existing functionality and shared services. Changing the culture and breaking down silos will be challenging as leadership broadens its perspectives while maintaining a focus on program requirements. However, as Divisions begin to see the benefits of leveraging shared functionality/services, including enhanced information, decreased costs, reduced levels of effort, fewer risks, and quicker implementations, it will be easier to adopt new processes and change the culture.

Department leadership will need to support and enforce procurement standards that require identification of existing Department of Health and Social Services (DHSS) technology and services that can be leveraged for reuse prior including that functionality in a Request for Proposals (RFP). Additionally, RFPs should require vendors to leverage existing services rather than developing redundant functionality. Vendors should also be required to address and comply with licensing considerations and enterprise-wide standards to maximize the available services and functionalities that can be reused.

7.0 OUTCOMES

The Health Information Technology (HIT) vision and goals documented in the Roadmap Phase I are intended to transition the Department of Health and Social Services (DHSS) to a modular, Service Oriented Architecture (SOA)-based infrastructure that allows services and functionality to be shared and reused. As the Department moves forward with Roadmap Phase II recommendations, expected outcomes will include standardized business processes, streamlined functions, and reduced redundancy. This will allow DHSS to meet evolving business needs, respond to increasing demand for services, and comply with federal mandates through use of a modular, agile, and flexible infrastructure.

Implementation of Roadmap Phase II recommendations will provide the following benefits:

- Strong oversight and governance of Information Technology (IT) acquisition projects
- Improved IT service model
- Strengthened security oversight and measures
- Standardized business services, available and accessible through shared services
- Consolidation of systems
- Elimination of duplicate storage and unnecessary collection of data
- Creation of a statewide master shared services and data management strategy
- Standardized technology platform, available and accessible through multiple access channels
- Greater access by citizens and providers to health care information and services
- Higher level of shared knowledge
- Lower overall system acquisition and maintenance costs
- Ability to leverage enhanced Medicaid funding

8.0 EVALUATION AND METRICS

Once the infrastructure and shared functionality/services are implemented, the Department will need to determine if the anticipated outcomes have been achieved and progress toward the Health Information Technology (HIT) vision has been made.

The level of success achieved through implementation of Roadmap recommendations can be measured in terms of the savings in systems implementations and quality improvement. Leveraging shared services and functionality, as described in this document, should also result in increased alignment and standardization of business processes across Divisions. It should be noted that some of these measurements and processes are already being put into practice by the Project and Portfolio Management Review (PPMR) team. As part of the new procurement process, Divisions must complete the Information Technology (IT) Alignment Framework Template and define business needs prior to moving forward.

A comparison of key metrics over time will allow the Department to quantify progress in the transition from the As Is to the To Be that is consistent with the HIT vision and goals. The Department of Health and Social Services (DHSS) should set numerical or percentage increase targets to evaluate each expected result.

Table 5: Evaluating the Results of Implementing Roadmap Recommendations

Evaluating the Results of Implementing Roadmap Recommendations	
Metric	**Criteria**
Count of available DHSS shared services and functions	The number of services that can be exposed for consumption by DHSS applications should increase by the targeted amount once the infrastructure required to share services is implemented
Count of Divisions leveraging a particular service or function	The number of Divisions utilizing individual shared services, rather than recreating that functionality should increase by the targeted amount as more services are implemented and made available
Implementation costs per service	Costs should decrease with each additional implementation of a shared service due to the reuse of code, testing processes, and procedures consistent with percentage targets
Procurement Costs	As culture and processes change and Request for Proposals (RFPs) require vendors to leverage existing DHSS services and functionality, the decreased scope of work and required level of effort should result in decreased procurement costs consistent with percentage targets

9.0 Recommendations and Leveraging the Roadmap

Due to the complexity and volume of federal mandates, budget constraints, and Affordable Care Act (ACA) requirements, the Department of Health and Social Services (DHSS) needs an Information Technology (IT) architecture that is responsive, flexible, and adapts easily to change.

The Enterprise Roadmap Phase II represents an opportunity for change and modernization of state technology infrastructure. It positions and prepares the Department to standardize business processes and streamline functions. Development of a more modular, agile, and flexible infrastructure will enhance DHSS's ability to meet evolving business needs and reduce redundancy.

9.1 SOA Governance

DHSS should consider adding SOA Governance responsibilities within or reporting to the PPMR team. As part of this responsibility, PPMR could create an SOA governance plan.

PPMR should also analyze BizTalk's runtime topology to assess the future data interchange needs. The resulting data would provide enhanced ability to monitor and plan for the increased demand for services anticipated with Affordable Care Act (ACA) implementation.

Another SOA Governance responsibility that could be assigned to PPMR would be to ensure development teams follow documentation standards so that consistency and continuity is provided, regardless of staff turnover.

DHSS should consider requiring vendors to interface with those functions and use pre-established Web Service Definition Language (WSDL) definitions. PPMR could provide oversight to ensure uniformity and standardization of WSDLs, as well as transparency and creation of interface control documents.

DHSS should also consider designating a small team of senior developers, analysts, and other staff who would be responsible for developing and maintaining:

- BizTalk Enterprise Service Bus (ESB)
- Business Rules Engine (BRE)
- Master Client Index (MCI)
- Shared functionality/services
- Business processes, workflows, and service testing using Business Process Execution Language (BPEL)
- Business Process Model and Notation (BPMN)

9.2 BizTalk Enterprise Service Bus

DHSS IT has selected the BizTalk ESB as an enterprise-level, key component of the Department's SOA. BizTalk currently supports the MultiVue MCI and has the ability to provide full ESB functionality.

The BizTalk ESB implementation is critical in moving toward a shared services model that will support business and operational needs. A fully functional ESB will support current Department projects, including the Medicaid Management Information System (MMIS) and Eligibility Information System (EIS) Replacement projects. These initiatives require interoperability with external systems, such as the Federally Facilitated Exchange (FFE) and the Federal Services Data Hub.

Cognosante recommends using a hardware architecture and internal connectivity that are highly available, redundant, and failsafe, based on the latest distributed architecture. By deploying two identical hardware components, DHSS IT can efficiently distribute load. Redundancy allows the duplicate component to continue to provide the required functionality and eliminate the impact of unexpected hardware failure.

This will allow DHSS IT to prevent system downtime and service delivery disruptions while replacing failed hardware. Cognosante also recommends using virtualized environments to deploy Microsoft BizTalk as well as the use of a dedicated and robust test environment.

9.3 Enterprise-Level Components

DHSS should consider leveraging enterprise-level components such as a BRE, Business Activity Monitoring (BAM), and a Business Process Workflow Engine. Creating a centralized repository for the Department's business rules in a BRE would:

- Allow the business rules to be stored in a common repository
- Create a centralized knowledge bank of business rules
- Eliminate the costs associated with duplicate rules engine licenses and instances
- Provide the ability for DHSS business analysts to learn to create and maintain rules in a common rules engine, saving training costs

DHSS may want to consider including the requirement that vendors utilize the IBM WebSphere ILOG JRules BRE utilized by the EIS for any future replacement system RFPs. The WebSphere ILOG JRules BRE could also be leveraged over time to become the central repository for DHSS business rules.

9.4 MultiVue MCI

The Department needs to implement near real-time interoperability between the MCI and its associated systems to enhance the ability to coordinate services across the Department. This will also improve data quality and allow the MultiVue MCI to be established as the repository of the golden record.

The myAlaska portal could be leveraged as the shared functionality for social services and Public Health Record (PHR) access. This functionality should be implemented using SOA to provide the ability to use the MultiVue MCI database to validate user demographics as new applications for social services are submitted.

The Department should consider evaluating the proficiency and knowledge DHSS IT resources related to MultiVue MCI and determine if additional training is needed or if additional DHSS IT staff should be hired. Another option to consider would be to secure a vendor to implement and maintain the MultiVue MCI.

DHSS IT should ensure MCI interoperability implementation includes thorough system documentation, including a data dictionary.

DHSS should also implement the following recommendations of the MCI Architectural Review:

- Utilize the integration engine capabilities of BizTalk to transform data requests to standard formats for submission to the MultiVue MCI for match processing
- Standardize the data submission process to decrease the time required to integrate DHSS Division systems
- Implement a shared Web Service with the BizTalk ESB to support real-time access to the MultiVue tool
- Determine the transaction volumes anticipated during the ACA Medicaid open enrollment period and perform volume stress tests to ensure sufficient capacity to handle the expected number of applicants
- Review BizTalk hardware to determine fault-tolerance, high-availability capability, and processing capacity

9.5 Shared Functionality/Services

Shared Services create efficiency and eliminate the need for each Division, program, or project to re-procure the same functionality. Implementing shared functionality will assist the Department in meeting increasing service demands while reducing costs. SOA and standard tools, such as an ESB, enable services to be developed once and reused throughout Department applications, saving development resources, time, and cost.

Cognosante researched shared services commonly deployed by health and human services agencies to increase efficiency and productivity, while reducing costs. Cognosante identified areas of focus that the Department may want to consider when determining the highest priorities for shared functionality/services. Factors considered included:

- The number of DHSS Divisions or applications that would benefit from the shared service
- How well implementation of the service supports DHSS next steps for the BizTalk ESB and MultiVue MCI
- The potential of each service to provide a "quick win" for the Department
- The level of increased efficiency, time and cost savings
- Ability of the service to increase productivity
- Potential reduction in manual tasks

As existing systems are prioritized for replacement and system maintenance contracts renegotiated, there may be additional shared services that DHSS should consider implementing. The services listed below are not exhaustive. However, they have been successfully implemented in other health and human services agencies and should be considered as potential opportunities as DHSS continues to move forward with a shared services model.

- Person Look-Up Service
- Address Validation Service
- Address Look-Up Service
- Person Add/Update Service
- Person Record Locator Service
- Identity Management Service
- Provider Directory Service
- Identity Proofing Service
- Payment Processing Service
- Hardcopy Notice Sending Service
- Softcopy Correspondence Generation Service

9.5.1 Case Management as a Shared Service

DHSS has already procured some of these services which can be exposed for reuse. Additional services should be prioritized for implementation. Multiple DHSS systems contain case management functionality. By separating case management into smaller, more modular capabilities, the Department could leverage common functionalities as shared services.

For example, DHSS may want to consider leveraging services such as:

- Grievance and appeals service
- Fraud, waste, and abuse tracking service
- Incident tracking

By leveraging these case management functionalities as shared services, the Department could increase consistency, improve data quality and transparency, and reduce the amount of time required for staff to complete case management tasks. This would reduce costs and allow current staffing levels to meet increased service demands.

As shared functionality/services are implemented, DHSS IT should utilize a dedicated test environment to thoroughly test each service prior to promoting code to the production environment. Implementation of shared functionality/services should follow the Software Development Life Cycle (SDLC) and include standard artifacts, diagrams, and detailed documentation.

9.5.2 Electronic Document Management System as a Shared Service

Each Division within the Department is required to collect, process, manage, store, retrieve, maintain, and provide search capability for documents as an integral part of day-to-day operations.. Documents for a given individual are stored in separate repositories, requiring different access technologies, separate storage, maintenance, and product licensing costs, as well as different business processes, retrieval, and search procedures. The end result for DHSS is duplicate costs across Divisions, lack of standardization of business processes, and difficulty in sharing or retrieving documents for the same individual across different systems.

Differences in each Division's business processes and storage needs make this one of the more challenging functions to implement as a shared service. Challenges include differences in the business processes, document types, workflow, storage requirements, and access needs of each Division.

Implementing EDMS as a shared service will require more than selecting the right technology component. Each Division's requirements will need to be documented in order to develop EDMS as a shared service and to ensure understanding of the current documentation needs. However, the evolution of EDMS to a shared function offers the following potential benefits to Alaska:

- Total lower cost of ownership: elimination of multiple technology and consolidation of current document storage reduces product license and maintenance costs, and allows DHSS to leverage economy of scale for storage of larger documents
- Reduced Duplication of Documents: a single repository also minimizes the potential duplication of documents across different Division level repositories
- Improved Access: leveraging shared services standardizes storage and access routines across the Department, allowing multiple Divisions the capability to securely search for and access documents appropriately
- Standardized Business Processes: document workflow and processes can be automated and standardized across the Department, improving the ability of different Divisions to access documentation. Workflow can be automated across Divisions for documentation notification, eliminating the need to electronically or physically pass documentation from one Division to another. Alerts and notifications can be automated as part of the centralized workflow
- Centralized Security: with a shared repository, document security is centralized, which reduces the security risks incurred with multiple repository environments

Cognosante recommends DHSS proceed with establishing EDMS as a shared service. Work will be required to identify common storage and retrieval requirements across Divisions and implement these as the initial services for the EDMS shared service. The Department will also need to gather statistics for current and future data storage requirements to accurately price the solution and procure the necessary storage.

9.6 Leveraging the Roadmap

9.6.1 Roadmap Phase I

The Enterprise Roadmap Phase I documented the Department's current Health Information Technology (HIT) environment. The current program-centric model creates redundancy as systems and functions are duplicated to meet the specific needs of each program. The DHSS's vision includes transitioning to an enterprise approach where services and functionality are procured once and shared or reused wherever needed throughout the Department.

9.6.2 Roadmap Phase II

The Roadmap Phase II provides recommendations and next steps needed to establish the infrastructure DHSS needs to implement shared services. This includes implementation of a SOA and key components such as a fully functional BizTalk ESB. Establishing an SOA-based infrastructure will enhance the Department's ability to automate business processes and achieve a higher level of Medicaid Information Technology Architecture (MITA) maturity.

In addition to infrastructure implementation, business processes need to be adjusted to ensure new projects and technology procurements align with the HIT vision and achieve the desired outcomes. For example, as projects are approved, Divisions should identify existing services that can be leveraged to meet business needs. RFPs should require vendors to use the identified services, rather than re-procuring the same functionality. RFPs should also require vendors to deliver systems that are SOA-compliant and able to share services without modification. The Department should review RFPs to ensure vendors are required to address standard licensing considerations.

DHSS has already implemented processes to ensure opportunities for leveraging shared components and services are recognized, i.e., when multiple projects request a similar functionality and when one project requests a new or enhanced functionality or service that could be reused in multiple programs.

9.6.2.1 Establish Necessary Governance and Blueprint for the Department Architecture

Include Service Oriented Architecture (SOA) Governance as a responsibility of Project and Portfolio Management Review (PPMR)

- Create an SOA Governance Plan
- Develop a blueprint for the Department overall architecture
- Develop conceptual, logical, and technical models of the To Be architecture
- Develop and maintain a list of shared services and components
- Require Interface Control Documents for each shared service

9.6.2.2 Make Necessary Changes to the Procurement Process to Support the Migration to Shared Services and Architecture

- Require that each new Request for Proposal (RFP) enforce the use of Shared Services
  - Use the IT Framework Alignment process to identify shared services
  - Ensure all new procurements utilize existing or planned share services
  - Publish Interface Control Documents for shared services that are expected to be leveraged within a procurement as an Request for Proposal (RFP) Appendix
  - Require vendors to leverage existing shared services and documented interfaces
  - Ensure that vendors are not including licenses, products, or hardware costs for existing shared services

9.6.2.3 Develop the Technical Infrastructure to Support the Implementation of a Service Oriented Architecture

- Update/upgrade the current hosting infrastructure for BizTalk
- Enable and implement all required components for the BizTalk Enterprise Service Bus (ESB)
- Prioritize recommended shared functionality/services implementation
- Identify hosting, life cycles, and required parameters for each existing and priority service
- Create measurable success criteria for all new applications and shared services
- Utilize the ESB to expose existing and all future shared functionality/services
- Ensure all future applications and services are strictly following SOA standards
- Evaluate the proficiency and knowledge of DHSS IT staff for the BizTalk ESB and MultiVue Master Client Index (MCI) and determine if additional training is needed
- Determine if additional DHSS IT staff should be hired, or a vendor secured to implement and maintain enhanced functionality within BizTalk ESB and MultiVue MCI

9.6.3 Next Steps

To realize these gains, DHSS will need to review existing applications to determine which systems are in most need of enhancement or replacement. IT project prioritization criteria requires analysis to determine which projects will provide the largest gains in MITA maturity and provide the highest return on investment (ROI). Additional factors include systems that:

- Are built on older or obsolete technology
- Applications whose support staff are approaching retirement and the institutional knowledge of the system is not well documented
- Require substantial IT staff and a high level of effort to maintain
- Have high maintenance and operations costs, based on total cost and per client served
- Frequently experience down time
- Are more vulnerable to hacking and exploitation
- Have low availability of experienced system maintenance staff
- Constrain program/Division staff to use labor intensive workflows and business processes

Systems meeting multiple factors should be considered for potential enhancement or replacement and are likely to provide the largest ROI.

Appendix A – Acronyms

Acronym	Definition
ACA	Affordable Care Act
AeHN	Alaska electronic Health Network
AKAIMS	Alaska's Automated Information Management System
API	Application Programming Interface
ARRA	American Recovery and Reinvestment Act
BAM	Business Activity Monitoring
BPEL	Business Process Execution Language
BPMN	Business Process Model and Notation
BRE	Business Rules Engine
COTS	Commercial off-the-shelf
CPU	Central Processing Unit
DBA	Database Administrator
DDI	Design, Development, and Implementation
DEA	Drug Enforcement Agency
DHSS	Department of Health and Social Services
DOB	Date of Birth
DS3	Data System 3
EDI	Electronic Data Interchange
EDMS	Electronic Document Management System
EHR	Electronic Health Record
EIS	Eligibility Information System
EIS-R	Eligibility Information System-Replacement
ELR	Electronic Laboratory Record
EMS	Emergency Medical Services
ESB	Enterprise Service Bus
ET	Eligibility Technician
FFE	Federally Facilitated Exchange
GUI	Graphical User Interface
HIE	Health Information Exchange
HIPAA	Health Insurance Portability and Accountability Act
HIT	Health Information Technology
HITECH	Health Information Technology for Economic and Clinical Health Act
HL7	Health Level 7
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IIEP	Iowa Integrated Eligibility Project
IT	Information Technology
IVR	Interactive Voice Response
JOMIS	Juvenile Offender Management Information System
LDAP	Lightweight Directory Access Protocol
LIMS	Laboratory Information Management System
LOB	Line of Business
LTC	Long-term Care

Acronym	Definition
MCI	Master Client Index
MDM	Master Data Management
MITA	Medicaid Information Technology Architecture
MMIS	Medicaid Management Information System
MPI	Medicaid Provider Number
NPI	National Provider Identifier
OPA	Oracle Policy Automation
ORCA	Online Resource for the Children of Alaska
OS	Operating System
PFD	Permanent Fund Dividend
PHI	Protected Health Information
PII	Personally Identifiable Information
PHR	Public Health Record
PPMR	Project and Portfolio Management Review
QOS	Quality of Service
RFP	Request for Proposal
SDLC	Software Development Life Cycle
SDS-DS3	Senior and Disabilities Services-Data System 3
SFTP	Secure File Transfer Protocol
SLA	Service Level Agreement
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
SNAP	Supplemental Nutrition Assistance Program
SOA	Service Oriented Architecture
SSL	Secure Sockets Layer
SSN	Social Security Number
SSO	Single Sign-On
TANF	Temporary Assistance for Needy Families
TCO	Total Cost of Ownership
UAT	User Acceptance Testing
UDDI	Universal Description Discovery and Integration
UPIN	Unique Physician Identification Number
USPS	United States Postal Service
WSDL	Web Service Definition Language
XML	Extensible Markup Language
ZIP	Zone Improvement Plan