

# Medicaid Enterprise System (MES) Procurement Project Strategic Enterprise Advisory Services (SEAS)

## T-4: Technical Management Strategy

24/2018

**Created By:** The SEAS Vendor

**Submitted To:** AHCA MES Project Management



## Revision History

DATE	VERSION	DESCRIPTION	AUTHOR
4/15/2018	001	T-4 Technical Management Strategy Initial Draft Version	Rene Cabral, Steve Quante, Paul Moore
5/17/2018	002	T-4 Technical Management Strategy Revisions to Agency Review	Rene Cabral, Steve Quante, Paul Moore
5/24/2018	003	T-4 Technical Management Strategy Revisions for Final Draft	Steve Quante
5/25/2018	100	T-4 Technical Management Strategy baseline version	Sean Gibbs

Modifications to the approved baseline version (100) of this artifact must be made in accordance with the Change Control process that is part of the Scope Management Plan.

## Quality Review History

DATE	REVIEWER	COMMENTS
4/15/2018	Sean Gibbs	QA Submission Review
5/17/2018	Sean Gibbs	QA Submission Review
5/24/2018	Sean Gibbs	QA Submission Review

## Table of Contents

Section 1	Introduction .....	1
1.1	Background.....	1
1.2	Purpose .....	1
1.3	Scope Statement .....	2
1.4	Goals and Objectives.....	3
1.5	Referenced Documents .....	4
Section 2	Roles and Responsibilities .....	5
Section 3	Technical Management Approach .....	6
3.1	Technical Management Approach Summary.....	6
3.2	Technical Management Strategy.....	11
3.3	Enterprise Service Bus (ESB) .....	12
3.4	Performance Management Validation .....	12
3.5	Information Technology Security Standards.....	14
3.6	Cloud Computing .....	14
3.6.1	Characteristics of Cloud Computing.....	14
3.6.2	Cloud Computing Delivery Models .....	15
3.6.3	Cloud Computing Deployment Models .....	16
3.6.4	Cloud Computing Considerations.....	17
3.6.5	The Federal Risk and Authorization Management Program (FedRamp) .....	17
3.6.6	Cloud for Government.....	18
3.6.7	Cloud Adoption Strategy .....	19
3.7	Common UI Framework.....	21
3.8	Standards and Technology Maturity.....	22
3.9	COTS Usage .....	24
3.10	Activity Prioritization .....	24
3.11	Technical Service Availability Strategy (TSAS) .....	25
3.11.1	Datacenter Availability .....	25
3.11.2	Availability Principles for Application Modules and their Services.....	26

3.11.3	COTS Considerations .....	26
3.11.4	SaaS considerations .....	27
Section 4	Transformation Challenges .....	28
4.1	Overview.....	28
4.2	Inventory of Technology Challenges .....	28
Section 5	Technical Services Governance .....	36
5.1	Service Contracts.....	36
5.2	Use of MES Governance Processes .....	36
5.3	Roles and Responsibilities .....	37
5.4	RACI Matrix .....	37
5.5	Governance Process .....	38
5.6	Subject Areas for Governance .....	39
Section 6	Collaborative Governance .....	40
6.1	Collaborative Governance Overview .....	40
6.2	Collaborative governance principles .....	40
6.3	MES Governance Strategy .....	41
6.4	Collaborative Governance RACI .....	42
6.5	Collaborative Governance Tools and Techniques .....	42
Section 7	Technical Principles .....	44
7.1	MES Technical Principles .....	44
7.2	SOA Technical Principles for Module and System Implementation .....	45
Section 8	Technical Goals and Objectives .....	47
Section 9	Transition Plans.....	50
9.1	Overview.....	50
9.2	Key Transition Principles.....	52
9.3	MES Modular Strategy.....	53
9.4	MES Enabling Technologies .....	54
9.4.1	Web Services.....	54
9.4.2	Service Oriented Architecture (SOA) .....	55
9.4.3	Business Rules Engines .....	55
9.4.4	NIEM adoption .....	56

---

9.4.5	Customer Relationship Management .....	57
9.4.6	Operational Data Store (ODS) .....	57
9.4.7	Enterprise Architecture .....	57
Section 10 State Specific MITA Additions .....		58
10.1	Cognitive Services .....	58
10.1.1	Machine Learning .....	58
10.1.2	AI Bots .....	59

## Table of Exhibits

Exhibit 1-1: SEAS Technology Deliverables .....	3
Exhibit 2-1: Roles and Responsibilities .....	5
Exhibit 3-1: Data Management Strategy Vision To-Be Diagram .....	7
Exhibit 3-2: MES Technical Management Approach .....	10
Exhibit 3-3: Technical Management Approach Benefits Mapping .....	11
Exhibit 3-4: NIST DCC Five Cloud Key Characteristics .....	15
Exhibit 3-5: NIST DCC Four Cloud Delivery Models .....	16
Exhibit 3-6: MES Future State Cloud Adoption.....	19
Exhibit 3-7: Rogers Bell Curve: Category percentages are across all industries.....	23
Exhibit 4-1: Transformational Challenges Details .....	35
Exhibit 5-1: Technical Services Roles and Responsibilities .....	37
Exhibit 5-2: RACI Matrix for Technical Services Governance .....	38
Exhibit 10-1: Cognitive Services Use Cases. ....	58

---

## Table of Strategic Topics

Strategic Topic 3-1: MES Infrastructure Cloud Computing Adoption .....	21
Strategic Topic 3-2: Agency UI Strategy for MES and Non-FMMIS .....	22
Strategic Topic 3-3: MES Technology Adoption Category .....	24
Strategic Topic 9-1: MES Degree of Modularity.....	53

## SECTION 1 INTRODUCTION

### 1.1 BACKGROUND

The Florida Agency for Health Care Administration (Agency) is preparing for the changing landscape of health care administration and increased use of the Centers for Medicare and Medicaid Services (CMS) Medicaid Information Technology Architecture (MITA) to improve the administration and operation of the Florida Medicaid Enterprise. The current Florida Medicaid Enterprise includes services, business processes, data management and processes, technical processes within the Agency, and interconnections and touch points with systems that reside outside the Agency necessary for administration of the Florida Medicaid program. The current Florida Medicaid Enterprise System (MES) includes the Florida Medicaid Management Information System (FMMIS) and Decision Support System (DSS), operated by DXC Technologies. The MES also includes a mix of systems, some of which are operated by vendors and others by Agency staff. These systems in the MES interface primarily through the exchange of data files, primarily through Secured File Transfer Protocol. These point-to-point interfaces become more complex and costly as the number of systems and applications increase. The future of the Florida Medicaid Enterprise integration is to allow Florida Medicaid to secure services that can interoperate and communicate without relying on a common platform or technology. Connecting services and infrastructures, and developing integration standards are the next steps for advancing the MES level of MITA maturity and system modularity modernization.

The CMS released the Medicaid Program Final Rule: Mechanized Claims Processing and Information Retrieval Systems in December 2015. This final rule modifies regulations pertaining to 42 Code of Federal Regulations (CFR) 433 and 45 CFR 95.6111, effective January 1, 2016. Among other changes, this final rule supports increased use of the MITA Framework. MITA is a CMS initiative that fosters an integrated business and information technology (IT) transformation across the Medicaid Enterprise to improve the administration and operation of the Medicaid program. The Agency documents its high-level plans to increase service interoperability and advance the maturity of the MES in accordance with the MITA Framework in the Florida MES Procurement Strategy document.

### 1.2 PURPOSE

The purpose of the MES T-4: Technical Management Strategy (MES TMS) is to develop and establish the Agency's Technical Management Strategy. The MES TMS aligns with the MITA 3.0 Part III Technical Architecture - Chapter 2 Technical Management Strategy (MITA TMS) while prioritizing unique Agency requirements. The MES TMS is the product of current state discovery, stakeholder input, strategic analysis, program strategy and direction about techniques and priorities to support overall improvement of Medicaid program outcomes.

The MES TMS document may contain links to updated versions of documents and diagrams, referenced in the following sections of this document that resides in the MES Projects Repository.

As per MITA guidance, the MES TMS will include the following content:

- Technical Management Approach
- Transformation Challenges
- Technical Services Governance
- Collaborative Governance
- Current Technical Principles
- Technical Goals and Objectives
- Transition Plans
- State-specific MITA Additions

The primary audience for the MES TMS is state Health and Human Services (HHS) executives and lead architects.

### 1.3 SCOPE STATEMENT

The MES TMS provides technology guidance for the procurement, development, implementation, integration, and maintenance of MES technology systems and investments. The MES TMS works in alignment with the MES Data Management Strategy and other MES Strategic Enterprise Advisory Services (SEAS) Project Technology Domain deliverables to support the business organizations implementation of the MES Strategic Priorities.

Technology strategy is a broad topic that could include almost any organizational asset other than people. The MES TMS provides guidance for the MES Program in the following areas of technical architecture:

- Application Models and Frameworks
- Infrastructure and Hosting Supporting Applications and Systems
- Integration Technologies
- User Interface Consistency
- Transition from Existing System(s)
- Introduction of New Technologies
- Information Technology Security Standards

**Exhibit 1-1: SEAS Technology Deliverables** lists SEAS Technology Domain deliverables that contain strategic direction and guidance in additional areas of technology.

SEAS TECHNOLOGY DELIVERABLE	DESCRIPTION
T-1: Data Management Strategy	Technology strategy focused on overall data strategy, conceptual data management vision and data governance approach
T-2: Information Architecture Documentation	Technology strategy documenting MES conceptual and logical data models
T-3: Data Standards	Technology strategy focused on MES Data Standards and data definitions
T-4: Technical Management Strategy	Technology strategy focused on platform and infrastructure to support MES modules
T-5: Technical Architecture Documentation	Technology strategy focused on application architecture within MES modules
T-6: Technology Standards	Technology standards and communication and governance process for all technology standards
T-7: Design and Implementation Management Standards	Technology strategy focused on the design and system implementation lifecycle
T-8: Enterprise Data Security Plan	Technology strategy focused on MES security considerations

### Exhibit 1-1: SEAS Technology Deliverables

This iteration of the deliverable discusses the technologies needed to achieve optimal sharing of the state’s services and data with emphasis on the foundational capabilities of the Integration Services Integration Platform (ISIP) including Enterprise Service Bus (ESB), Enterprise Data Warehouse (EDW), Operational Data Store (ODS), Reporting Data Store (RDS), and Modular capability implementation. This document provides the Agency context, aligned with MITA, required for planning purposes.

#### 1.4 GOALS AND OBJECTIVES

- Goal 1 - Establish the MITA compliant Florida Medicaid Technical Management Strategy.
  - › Objective 1 – Define and document each of the core Technical Management Strategy areas for the Agency that aligns to the MITA standard as described in Section 1.3 Scope Statement.
  - › Objective 2 – Use this deliverable as the key strategic Technical Management reference for future planning and solicitations as part of the Agency’s modular implementation approach.
- Goal 2 - Provide a Technical Management Strategy that addresses the transformational challenges within the Agency while remaining aligned to the MITA Standard.
  - › Objective 1 – Through discovery sessions and current state analysis identify the critical pain points within the Agency related to Technology Management.

- › Objective 2 – Recommend approaches, processes, technologies, and tools that provide a future vision for resolving the transformational challenges identified.

## 1.5 REFERENCED DOCUMENTS

Documents referenced to support the development of this plan include the following:

- Guidance for Exchange and Medicaid Information Technology (IT) Systems. CMS. 2.0
- MITA 3.0 Part III, Chapter 2 Technical Management Strategy
- MITA 3.0 Part III, Chapter 4 Technical Services
- The Open Group SOA Source Book, 7th Edition
- Rogers, E. (2003). Diffusion of Innovations. Free Press. 2018
- MES T-3 Data Standards, available for review on the MES Projects Repository
- MES T-5 Technical Architecture Documentation, available for review on the MES Projects Repository
- MES T-6 Technology Standards, available for review on the MES Projects Repository
- MES T-6 Attachment E: Technology Standards Communication, Support, Compliance, and Compliance Reporting Procedures
- MES T-8 Enterprise Data Security Plan, available for review on the MES Projects Repository
- MES S-4 Strategic Project Portfolio Management Plan, available for review on the MES Projects Repository

## SECTION 2 ROLES AND RESPONSIBILITIES

This section identifies the roles and responsibilities for the primary stakeholders that maintain or use this document.

ROLE	RESPONSIBILITY
SEAS Vendor Technical Architect	<ul style="list-style-type: none"> <li>▪ Identifies the technologies and related processes necessary to improve the Medicaid Enterprise.</li> <li>▪ Propose technology management solutions that align to MITA 3.0, State, and Agency specific Medicaid requirements.</li> <li>▪ Reviews and proposes new emerging technologies to the Agency.</li> <li>▪ Maintains the Agency Technical Management Strategy.</li> <li>▪ Supports vendor procurements by providing information, extracts and details related to the Technical Management Strategy.</li> </ul>
AHCA MES Technical Domain Lead	<ul style="list-style-type: none"> <li>▪ Coordinates the participation of Agency stakeholders that identify technical management strategy topics needing definition, decision or elaboration, review and provide feedback on proposed technical management strategy topics.</li> <li>▪ Communicates technical management strategy to AHCA MES Domain Leads.</li> <li>▪ Supports MES Project leadership communication to AHCA executive leadership.</li> <li>▪ Approves communications between the SEAS Vendor and MES Stakeholder Organizations related to MES Technical Management Strategy.</li> </ul>
MES Project Vendors (SEAS, EDW, Module)	<ul style="list-style-type: none"> <li>▪ Follows the strategic direction in the Technical Management Strategy in proposing, discussing, and implementing technology for the Medicaid Enterprise.</li> <li>▪ When necessary, recommends technologies and solutions applicable to the implementation of MES Projects that align to MITA 3.0 and the Technical Management Strategy.</li> </ul>
MES Stakeholder Organizations	<ul style="list-style-type: none"> <li>▪ Reviews and as appropriate may align technology solutions with MES technology standards, systems and processes per the Technical Management Strategy to achieve the Agency's mission of "Better Health Care for All Floridians".</li> </ul>

### Exhibit 2-1: Roles and Responsibilities

## SECTION 3 TECHNICAL MANAGEMENT APPROACH

### 3.1 TECHNICAL MANAGEMENT APPROACH SUMMARY

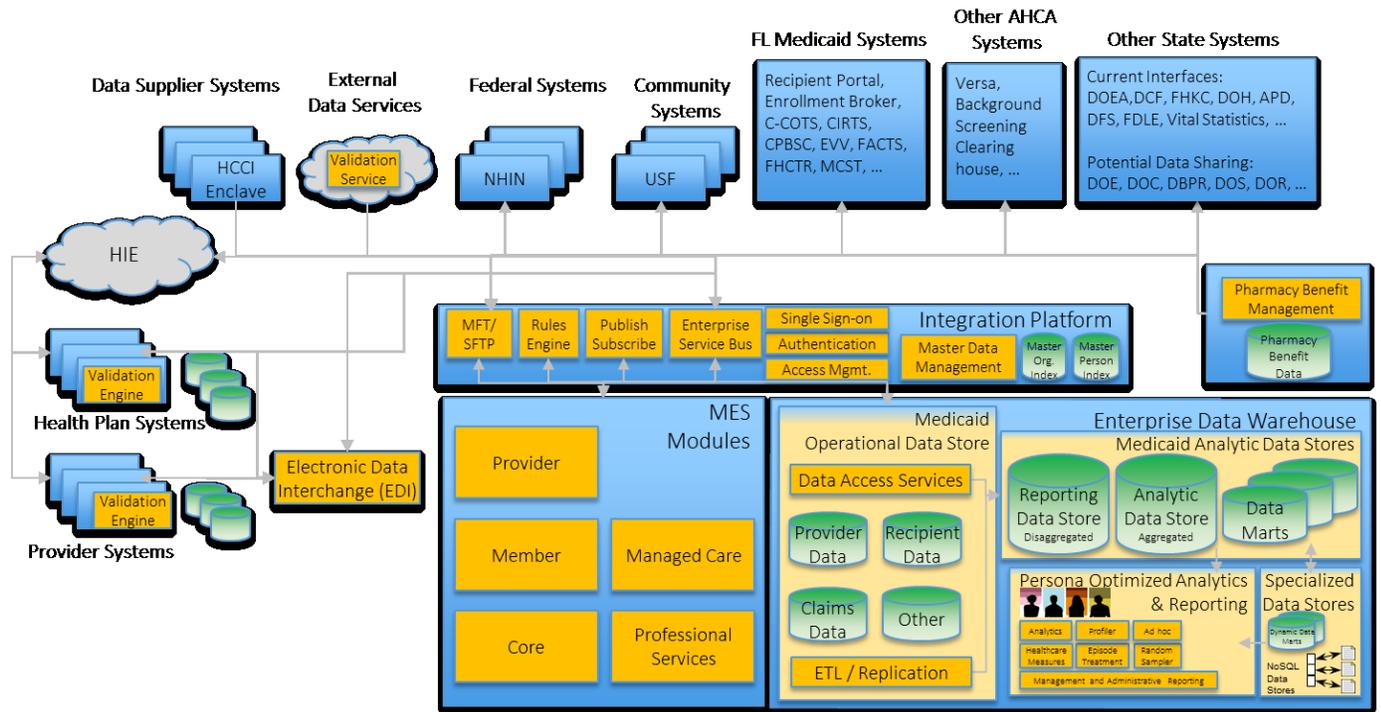
The MES Technical Management Approach (TMA) uses a business-driven technology enabling strategy to help the Agency achieve its mission of “Better Health Care for All Floridians”.

The approach aligns to the industry direction of Everything-as-a-Service (EaaS). EaaS is an outcome-focused strategy that emphasizes delivery of results as opposed to dictating the process or mechanics of how work occurs. With the defined standards of performance, interoperability standards, and enterprise integration capabilities, each system, organization, or entire ecosystem can reuse services. The consistency and scalability provided through use of services technology provides large economic benefits in the delivery of healthcare services. Service based technology implementations are proven to promote reuse, scale more easily when compared to monolithic technology solutions, are less costly to support and enhance, and due to their modular design are less costly and disruptive to replace as technology changes.

There are many technology adoptions of EaaS:

- Data-as-a-Service (DaaS)
- Platform-as-a-Service (PaaS)
- Infrastructure-as-a-Service (IaaS)
- Software-as-a-Service (SaaS)
- Network-as-a-Service (NaaS)
- Identity-as-a-Service (IDaaS)
- Security-as-a-Service (SECaaS)

The MES TMS provides guidance for the MES Project implementation of technology related to the above technology services. The context of the MES TMS is the to-be vision depicted in **Exhibit 3-1: Data Management Strategy Vision To-Be Diagram**. The diagram provides a conceptual overview of the FMMIS evolution to MES and data processing landscape of the MES.



**Exhibit 3-1: Data Management Strategy Vision To-Be Diagram**

In the Agency’s current landscape, FMMIS and other systems use technologies which are current within the last 10 years. Most applications and systems use a service oriented architecture (SOA), communicate using XML, and have web services that allow sharing and reuse. Likewise, several systems are implementing architectures that simplify replacement of Commercial off-the-shelf (COTS) solution based system software with flexible architectures. There are some small applications built with dated technologies more suitable for workgroup development (including MS FoxPro, MS Excel and others). Some of these small applications may not scale for use by the entire Medicaid Enterprise. The MES Program portfolio management process will evaluate potential MES Projects to rewrite or industrialize any existing applications for MES use.

MES strategic priorities and CMS MITA guidance emphasize increasing technology maturity in data sharing, integration, and use of cloud infrastructure. A component of the MES Technical Management Strategy is to reduce proliferation of systems and copies of data. The approach is to enable people and systems to use the Integration Platform to access information in near real time from the authoritative source of truth system and data as opposed to replicating and copying data between systems using interfaces. From a technology platform and infrastructure perspective, the MES technical management strategy emphasizes use of scalable virtual infrastructure that provides redundancy, high availability, failover processing and dynamic provisioning of capacity.

The MES Technical Management Approach emphasizes six primary technology management strategies that align with the overall MES strategic priorities:

- Enable a MITA aligned Service Oriented Architecture (SOA) through an Enterprise Service Bus
- Build modules from fine-grained modular business, technology and data services exposed through standards-based Application Programming Interfaces (API's)
- Leverage a common User Interface (UI) Framework and decoupled thin UI layer for all MES functionality
- Deploy cloud-ready MES modules in the Government only, FedRAMP (recommended) authorized cloud. Less critical applications such as Agency information portals can leverage the public cloud
- Follow a “do no harm” business disruption strategy in the development and deployment of new modules
- Enable the application of new technologies

***Enable a MITA aligned Service Oriented Architecture through an Enterprise Service Bus (ESB).*** Today, the Agency's system integration approach is primarily the exchange of files, custom data transformation processes, Secure File Transfer Protocol (SFTP), and some point-to-point system integration. As the technical landscape of the Agency becomes more complex, both internally and with a growing number of external system touch points, the current approach to system and data integration becomes increasingly more costly and complex. The MES strategy is to deploy an ESB which is an integration architecture that allows communication via a common communication layer between providers and consumers of data and services. Key functions of the ESB include message management, data management, service coordination, rules engine, single sign on (SSO), and business logic which enable complex orchestration of services. The ESB is a key enabler to allow the Agency greater integration possibilities with modern technologies across multiple vendors.

***Build modules from fine-grained modular business, technology and data services exposed through standards-based API's.*** Today, with few exceptions, the Agency approach is to build and deploy purpose specific systems that are tightly coupled with proprietary data stores. Planning for or ability to reuse components or services is secondary. An exception to this is some of the more recent work completed by AHCA IT where focus was placed on designing and building reusable data and application services exposed through API's. While these instances align directionally to the future state strategy, across the entire Agency code base they are exceptions rather than the rule. The MES technology strategy is to design and build discrete services that provide independent functionality. Discrete independent services promote reuse, more flexibility in targeted application scaling, are easier to reliably test, promote test automation, and are less costly to maintain over time. As part of module implementation, discrete services allow development of more intelligent composite services to provide additional system functionality to the Agency.

***Leverage a common UI Framework and decoupled thin UI layer for all MES functionality.*** Today, interChange, the FMMIS user interface built by the current fiscal agent, DXE Technologies, is the Agency's primary operations portal with common branding uniting the recipient portal, provider portal, and the operations user interfaces. While interChange does

provide some commonality in user interface across FMMIS, the UI is not decoupled and therefore not easy to modify or replace. Some Non-FMMIS Agency systems have a different look, feel and functionality further complicating the user experience within the Agency. The MES strategy is to describe and deploy a common unified user interface framework that defines look and feel consistency, accessibility standards, naming conventions, field validations, JavaScript usage guidelines, security guidelines, interaction guidelines, etc. The implementation of single sign-on functionality by the ISIP Vendor will also improve the consistency of the user interface when authenticating to MES applications. All new MES modules will use the new common UI framework with a bias towards greater future use across all AHCA systems.

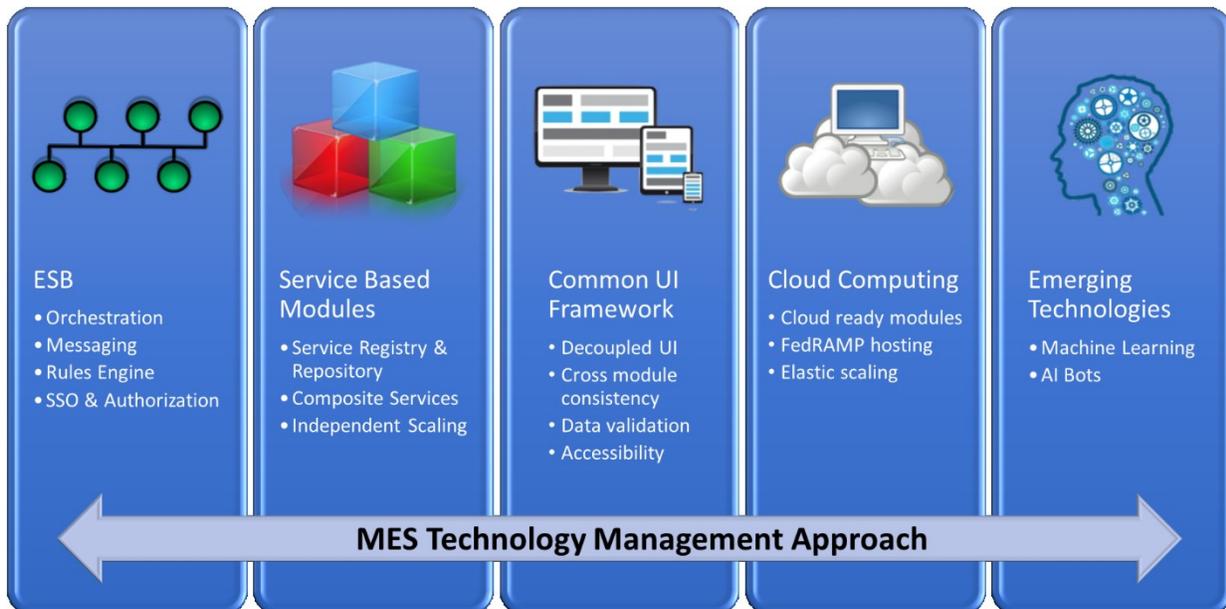
***Deploy cloud-ready MMIS modules in the Government only, FedRAMP authorized cloud. Less critical applications such as Agency information portals can leverage the public cloud.*** Today, the Agency’s hosting strategy uses multiple hosting providers. FMMIS uses a third-party administrator (TPA) provided data center in Orlando, FL. AHCA IT systems and applications use the Agency for State Technology (AST) data center. Office 365 uses Azure Government for hosting. The hosting of Agency applications is increasingly technology restrictive, costly and unaligned with industry hosting trends and capabilities toward use of cloud-based infrastructure. The MES strategy recommendation is to deploy new MMIS modules in a government only FedRAMP authorized cloud. FedRAMP is a government-wide program that provides a standardized approach to the security assessment, authorization, and continuous monitoring for cloud products and services providing a safe cloud-based hosting option for critical government systems which contain sensitive information. Agency applications with public information or information that is not sensitive can deploy using a public cloud provider. Regardless of hosting location, an important tenet of the Agency’s modular strategy is specifying that all vendor solutions should be cloud-ready even if deployed in a traditional centrally hosted environment.

***Follow a “do no harm” business disruption strategy in the development and deployment of new modules.*** The processing of Medicaid claims and payment of healthcare vendors represents almost 30% of the State’s spending. The MES modernization strategy is to use technology selection, design, testing, implementation and operation techniques that prevent avoidable disruption to the core mission of the Agency. This means processing in the new and legacy system both must work together to provide seamless operation during the transition. Components of the FMMIS system will remain operational while being incrementally replaced with MES modules resulting in a hybrid environment throughout the duration of the migration. To recipients, providers, and health plans their interactions with the Agency should appear the result of a single cohesive system. This strategy means designing, developing and implementing in a way that prevents having different inconsistent versions of data presented in different systems, producing duplicate correspondence or not providing correspondence, denying duplicate transactions, or showing duplicated or inaccurate information on portals or reports.

***Enable use of new technologies.*** The MES strategy is to enable the adoption of new technologies. For example, use of artificial intelligence bots, machine learning, real-time natural language processing, and advanced predictive analytics are increasing in health care and other

industries. By establishing a standards-based framework for interoperability, MES Project can adopt new technologies quickly and at lower cost.

**Exhibit 3-2: MES Technical Management Approach** depicts the primary technology management strategies that make up the MES Technology Management.



**Exhibit 3-2: MES Technical Management Approach**

**Exhibit 3-3: Technical Management Approach Benefits Mapping** shows each technical management approach benefit mapped to the pillars of the Technical Management Approach.

TECHNICAL MANAGEMENT APPROACH BENEFITS	ENTERPRISE SERVICE BUS (ESB)	SERVICE BASED MODULES	COMMON UI FRAMEWORK	CLOUD COMPUTING	EMERGING TECHNOLOGIES
Promote reuse	✓	✓	✓	✓	
Reduce support and enhancement cost		✓	✓		
Reduce copies of data		✓			

TECHNICAL MANAGEMENT APPROACH BENEFITS	ENTERPRISE SERVICE BUS (ESB)	SERVICE BASED MODULES	COMMON UI FRAMEWORK	CLOUD COMPUTING	EMERGING TECHNOLOGIES
Improve integration of disparate technologies	✓				
Increased flexibility in application scaling		✓		✓	
Virtual hot site, and rapid deployment		✓		✓	
Promote test automation		✓			
Environment elastic scaling as needed		✓		✓	
Consistency in experience across modules		✓	✓		
Module redundancy, high availability, and failover		✓		✓	
Maximize fraud prevention				✓	✓
Improve recipient care by detecting important patterns in recipient data				✓	✓

**Exhibit 3-3: Technical Management Approach Benefits Mapping**

### 3.2 TECHNICAL MANAGEMENT STRATEGY

The MES TMS identifies mature and emerging technologies and standards and protocols that aid the sharing of data and application services. The MES TMS also discusses the prioritization of activities based on business need and business value. The resulting MES TMS Approach enables the development efforts of many organizations to contribute to the target technical management environment.

The MES TMS will focus on the following:

- Enterprise Service Bus (ESB)
- Performance Management Validation
- Information Technology Security Standards
- Cloud Computing

- Common UI Framework
- Standards and Technology Maturity
- COTS Usage
- Activity Prioritization
- Technical Service Availability Strategy

### 3.3 ENTERPRISE SERVICE BUS (ESB)

The ESB provides a communication system where software applications interact in a service-oriented architecture (SOA). The SOA is an organization-wide, shared, reusable service model used by all applications integrated using the ESB. Software applications integrated in this manner provide data and processing through web services. The ESB performs message management, service authorization and access control, availability management, usage and cost accounting, and service coordination for complex orchestration of services.

The ESB is a key architectural piece of the Medicaid Enterprise System (MES) TMS and future key enabler of the MITA SOA. The ESB decouples the network design from the underlying platform and allows the Agency greater integration possibilities with modern technologies across multiple vendors, multiple platforms (e.g. cloud, COTS), and supports the Agency's Everything-as-a-Service approach. The ESB also supports the approach by enabling near real time information sharing between applications. This reduces the need for nightly batch interfaces that replicate large amounts of information between systems. The ESB simplifies integration complexity and enhances standardization by performing the most complex and challenging aspects of interoperability with common architecture. Specifically, the ESB can enforce and support transformation of message vocabulary and data formats between systems to a standard consistent vocabulary. When messages are in or transformed to a standard vocabulary, the ESB can perform fine grained access controls based on many characteristics including content values. The ESB can enforce security policy to mask data values (e.g. SSN) or filter entire message content based on policy. These and many other capabilities enable the vision of secure data sharing and service reuse that will reduce the duplication of data and increase the timeliness and accuracy of information.

### 3.4 PERFORMANCE MANAGEMENT VALIDATION

Performance Management (PM) includes activities to confirm systems and MES Project Vendors consistently meet performance goals in an effective and efficient manner. These activities should adhere to the CMS document Guidance for Exchange and Medicaid Information Technology (IT) Systems (IT Guidance):

- Ensure quality, integrity, accuracy, and usefulness of functionality and information
- Provide timely information transaction processing, including maximizing real-time determinations and decisions
- Ensure systems are highly available and respond in a timely manner to customer requests

The MITA Framework provides guidance for a basic three (3) tier performance monitoring structure, which the Agency will use in its expression of Performance Management:

- Performance Standard - A management-approved expression of the performance threshold(s), requirement(s), or expectation(s) that CMS expects States to meet to appraise at a particular level of performance.
- Performance Measure - Based on established Performance Standards and tracks past, present, and future business activity.
- Performance Metric - A measure of an organization's activities and performance also known as a Key Performance Indicator (KPI). Often closely tied in with outputs, performance metrics usually encourage improvement, effectiveness, and appropriate levels of control.

The technical requirements for technology procurements should specify performance metrics. Performance validation occurs at different stages of the delivery of the technology. Prior to system integration, modules must pass standard development testing such as unit tests, functional tests, end-to-end tests, stress tests, etc. After successful module or system specific testing, modules should pass integration and specification testing in a staging environment.

Systems, applications, and modules brought into the Agency should have standards-based mechanisms that allow data collection on performance such as log files, service-based status indicators, log or service-based usage statistics, etc.

In modern distributed systems, it is common practice to use Software Monitoring Systems, such as Splunk, which monitor, aggregate, analyze, and can perform actions based on monitoring conditions or events originating from the monitored performance data sources. After integration of each new data source, the setup of custom filters creates uniform data entries for analysis and reporting. This input flexibility allows the simultaneous integration of various solutions like custom software, COTS, and cloud service offerings. This monitoring software can centralize performance data and monitoring for all software systems in the enterprise.

When new systems, applications, or modules are deployed into the production environment they should be connected in a way that allows monitoring and alerting on any metric defined in the performance standards pertinent to that system, application, or module.

A modern Software Monitoring System with a minimum of the following features is a key enabler to continuous performance validation:

- Monitoring
- Alerting
- Dashboards
- Visualizations
- Reporting

- SSO

### 3.5 INFORMATION TECHNOLOGY SECURITY STANDARDS

ISIP, EDW and module vendors need to adhere to the security requirements, processes, policies and standards of the MES. MES security standards reside in the Technology Standards Reference Guide (TSRG).

The TSRG is a repository of standards relevant to technology components that identifies and prioritizes the relevance of specific technology standards in the enterprise. MES technology standards entries categorized in the [security area of the TSRG](#) provide transparency to required security standards applicable to MES Projects and describes the standards compliance approach used to confirm the implementation of security standards. The TSRG is an important tool to document and govern relevant standards and provide clear communication between the Agency and vendors.

### 3.6 CLOUD COMPUTING

This section provides significant background, definition and context about cloud computing. Section 3.6.7 Cloud Adoption Strategy summarizes the MES direction related to adoption of cloud technologies.

The Executive Order "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure" issued May 11, 2017, reinforces the directive to use shared IT services for federal systems; including a cloud-first approach where possible. This aligns with the overall industry's move to hosting platforms, infrastructure, and software as services within both privately and publicly accessible cloud environments.

Cloud computing is a model which enables dynamically scalable resources to be provisioned as services over a network. These resources can be networks, servers, storage, applications, services, platforms, datacenter infrastructure, etc. Cloud computing infrastructure is a combination of hardware and software. Cloud Computing is enabled by two key technologies: Service Oriented Architecture (SOA) and Virtualization Technologies.

#### 3.6.1 CHARACTERISTICS OF CLOUD COMPUTING

According to the National Institute of Standards and Technology (NIST) Definition of Cloud Computing (DCC), cloud computing infrastructure enables five key characteristics: on-demand self-service, broad network access, resource pooling, rapid elasticity and measured service.

#### **Exhibit 3-4: NIST DCC Five Cloud Key Characteristics.**

CHARACTERISTIC	DESCRIPTION
On-demand Self-service	A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.

CHARACTERISTIC	DESCRIPTION
Broad Network Access	Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick recipient platforms (e.g., mobile phones, tablets, laptops, and workstations).
Resource Pooling	The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., datacenter). Examples of resources include storage, processing, memory, and network bandwidth.
Rapid Elasticity	Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.
Measured Service	Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the used service.

### Exhibit 3-4: NIST DCC Five Cloud Key Characteristics

#### 3.6.2 CLOUD COMPUTING DELIVERY MODELS

The NIST DCC was authored in 2011 and describes three delivery models: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). Server-less computing is a new delivery model which became publicly available in 2014 and has been added to the models list. Detailed descriptions are provided in **Exhibit 3-5: NIST DCC Four Cloud Delivery Models**.

DELIVERY MODEL	DESCRIPTION
SaaS	The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various recipient devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

DELIVERY MODEL	DESCRIPTION
PaaS	The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.
IaaS	The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer can deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).
Server-less	Server-less computing relies on the infrastructure vendor to manage capacity planning and management of the underlying servers. Server-less computing offerings range from application engines which run custom code functions to data warehousing, analytics and machine learning. The benefits of a server-less architecture include reduced management from not having to administer servers, and a true pay-as-you-go model that only bills users for the resources used to run their functions and does not charge them for idle time.

### Exhibit 3-5: NIST DCC Four Cloud Delivery Models

#### 3.6.3 CLOUD COMPUTING DEPLOYMENT MODELS

The NIST DCC identifies four deployment models for cloud infrastructure: private, community, public, and hybrid.

- **Private Cloud** – In this model the consumer organization has exclusive access to and usage of the cloud infrastructure. The deployment can be on-site or outsourced to a third-party provider.
- **Community Cloud** – This deployment is a multi-tenant version of private cloud that supports a community of consumers with a shared mission, objectives, security, privacy, and compliance policy. The deployment can be on-site or outsourced to a third-party provider.
- **Public Cloud** – This deployment is cloud infrastructure made available to the public over a public network and managed by the provider.
- **Hybrid Cloud** – This deployment model uses at least two distinct cloud infrastructure deployments. Although these deployments remain unique entities, they are connected. The MES Vendor orchestrates use of services and resources for the deployment models used in the solution.

### 3.6.4 CLOUD COMPUTING CONSIDERATIONS

The considerations in deciding where to use cloud technology in the enterprise are security, privacy, and performance. Adopting cloud technology means giving control over several issues that may affect any of these aspects.

The planned Medicaid Enterprise System (MES) includes the Enterprise Service Bus (ESB), Enterprise Data Warehouse (EDW), Operational Data Store (ODS), Reporting Data Services (RDS) and Application Modules (AM).

Implementing the MES infrastructure in a private or community cloud on startup would enable the Agency to retain some of the benefits of on-premise infrastructure like data privacy, predictable latency and isolation. Private cloud deployment of the MES infrastructure will also benefit from cloud infrastructure features like elastic resource allocation and node clustering. The ESB infrastructure is most effective when there is low network latency communication between the ESB and the highest volume data sources (e.g. operational data) and services.

### 3.6.5 THE FEDERAL RISK AND AUTHORIZATION MANAGEMENT PROGRAM (FedRAMP)

FedRAMP is a government-wide program that provides a standardized approach to the security assessment, authorization, and continuous monitoring for cloud products and services. The General Services Administration, as the Federal government's generic authority for management of information technology policy and practices across civilian agencies, is responsible for implementation of FedRAMP.

FedRAMP uses a "do once, use many times" framework that reduces cost, saves time, and staff resources required to conduct redundant agency security assessments. Where the Agency requirements and mission needs support the use of specific cloud services (IaaS, PaaS, or SaaS), services with a current FedRAMP authorization should be included in the total set of products and services evaluated. The potential for cost reduction, which includes meeting baseline security requirements, should be addressed in the Agency IT procurement guidance.

The Government Accountability Office (GAO) has described the purposes of FedRAMP to be:

- Ensure that cloud-based services have adequate information security
- Ensure FedRAMP supports all needed security control baselines to match security requirements to risk.
- Eliminate duplication of effort and reduce risk management costs
- Enable rapid and cost-effective procurement of information systems/services for Federal agencies

Additionally, continuous monitoring provides risk visibility into and across FedRAMP approved services while assisting Cloud Service Providers (CSP) to maintain secure baselines over time. This also provides a risk framework that could identify and report security breaches.

There are two types of FedRAMP authorizations: Provisional Authority to Operate (P-ATO) which is issued by the Joint Authorization Board (JAB) and an Agency Authority to Operate (ATO) which is issued by the Agency planning to use the Cloud Service. A JAB P-ATO is not a risk acceptance, but an assurance to Agencies that the risk posture of the system has been reviewed and approved by Federal agencies such as Department of Defense (DoD), Department of Homeland Security (DHS), and General Services Administration (GSA). Each Agency planning to use the Cloud Service Offering (CSO) reviews and issues their own ATO, which covers their Agency's use of the cloud service. More information is available at the FedRAMP official website: <https://www.fedramp.gov>.

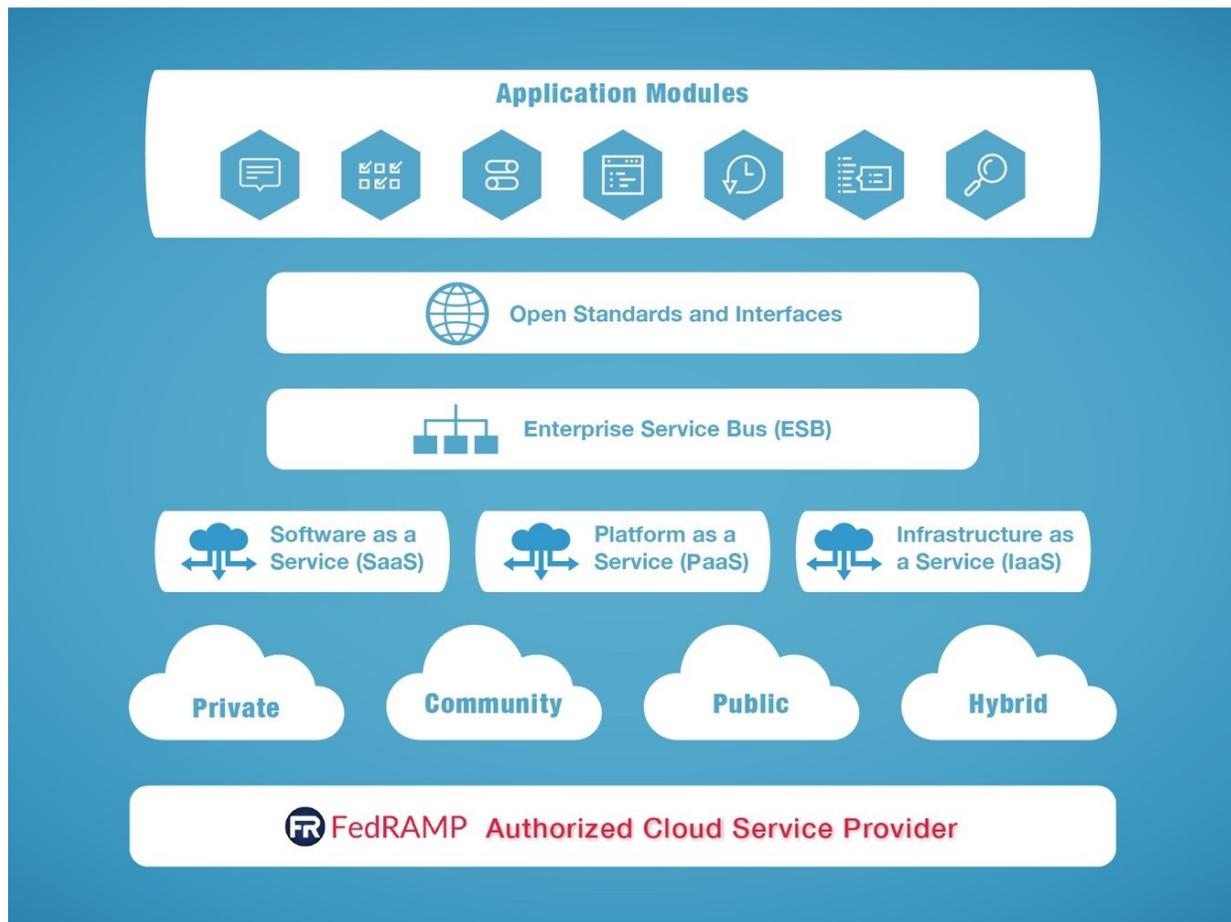
Although the full participation in the FedRAMP program is designed for federal agencies, state agencies can use the FedRAMP JAB P-ATO as an assurance that the risk posture of the system has been reviewed and approved by DoD, DHS, and GSA. The JAB will only authorize multi-tenant clouds (public, hybrid, and community), and not private cloud.

The Agency's cloud strategy recommendation is to favor CSP's that have obtained a FedRAMP JAB P-ATO.

### **3.6.6 CLOUD FOR GOVERNMENT**

A Government-only cloud or Cloud for Government demonstrates that the CSP has a dedicated, physically isolated cloud environment instance designed specifically to meet government requirements and serve only public-sector tenants. This service is usually a configuration of the hybrid cloud model.

The Agency's cloud strategy recommendation is to favor solutions that deploy in a government cloud.



**Exhibit 3-6: MES Future State Cloud Adoption.**

### 3.6.7 CLOUD ADOPTION STRATEGY

The MES cloud adoption strategy defines the acceptable use of cloud for MES modules and systems. The cloud adoption strategy defines the recommended future state and maps the progression from the current state. Through the progression toward the future state, the enabling foundations incrementally develop capability and maturity for realization of the future state.

**Strategic Topic 3-1: MES Infrastructure Cloud Computing Adoption** describes the recommended hosting strategy direction for the MES Infrastructure (ESB, EDW, RDS, ODS, and Application Modules) and its context with the existing FMMIS system.

CLOUD ADOPTION LEVEL	TIMELINE				
	Current	2018	2020	2022	2025
On Premise					
AST Hosted	Non-FMMIS	->			
Third Party TPA Data Center	FMMIS	FMMIS ESB (2019)	FMMIS	->	
Vendor Hosted					
State Private Cloud					
Cloud for Government (FedRAMP)			ESB, ODS, RDS, EDW, App Modules, Non-FMMIS	-> Evaluate FMMIS	
Public Cloud			App Modules, Non-FMMIS, Dev Environments	->	

#### ANALYSIS

The MES cloud strategy is a gradual migration to cloud. See Figure 3-3. The deployment of the ESB should be geographically close to the data services (FMMIS Orlando Data Center, Orlando, FL). This could preferably be within the same datacenter. As the origin of data services begins to shift from FMMIS to the EDW and ODS solutions, the geographical constraint will shift toward the EDW and ODS locations as well. The ESB infrastructure is most effective when there is low network latency between the ESB and highest volume data sources (EDW, ODS).

During the transition away from FMMIS the speed of data replication, between FMMIS and the ODS, plays a key enabling role. The tight data dependency between the systems requires that they both have access to current data. The replication speed should be fast enough to not be disruptive to the operations of FMMIS. Geographical proximity and fast networks are key enablers of near-real-time replication.

The recommended future state is deployment in Government only FedRAMP authorized cloud for mission-critical applications and sensitive data. Less critical applications such as Agency information portals can leverage the public cloud. Services and resources can be orchestrated in a Public Cloud when security, privacy and performance requirements are satisfied for that deployment. Although FedRAMP compliance is not a state level mandate, the Agency will favor solutions that use CSP's with a JAB P-ATO.

Cloud enabling virtualization technologies like containers, e.g. Docker, and container clustering technologies, e.g. Kubernetes, are recommended to enable solution portability, platform independence, and rapid deployment.

All vendor solutions should be cloud-ready and deployable in a traditional hosted environment. In the future state, Modules will be geographically near to the data services, preferably be within the same datacenter or connected via low latency network with adequate bandwidth.

## Strategic Topic 3-1: MES Infrastructure Cloud Computing Adoption

### 3.7 COMMON UI FRAMEWORK

A Common UI Framework defines look and feel consistency, accessibility standards, naming conventions (e.g. buttons, field tags), field validation, JavaScript usage guidelines, security guidelines, interaction guidelines, system role-based access control guidelines, embedded SQL, etc.

### Strategic Topic 3-2: Agency UI Strategy for MES and Non-FMMIS

AGENCY UI DIRECTION	Current	TIMELINE			
		2018	2020	2022	2025
Each Application Defines its own UI	Agency applications, and contracted Medicaid applications (Enrollment Broker, TPL) have unique UI	->	Agency Approved Exceptions (e.g. some COTS)	->	
Common UI Framework with Module Specific Portals			Residual Interchange UI		
Common UI Framework for all MMIS functionality (e.g. Interchange like)	All users access Interchange UI		Slight Preference for consistency between MES Modules (starting 2019) based on number of users and cost of consistency	->	
Common UI Framework for all MES projects					
Common UI Framework for all AHCA Agency Systems				AHCA Non-Medicaid Applications	->
Common UI framework used for Systems accessed by Medicaid Agencies				Available for use, Organization preference level of use	->

AGENCY UI DIRECTION	TIMELINE				
	Current	2018	2020	2022	2025
Common UI framework Used by All Agencies, Plans and Providers				Available for use, Organization preference level of use	->

### ANALYSIS

The Agency's approach to achieving a Common UI Framework will be practical and gradual. Solutions will observe the defined branding and style guidelines to customize the look and feel of their existing user interfaces within user segments. Solutions which have decoupled UI layers and expose services to thin clients can serve to lay a foundation for a future effort to unify the MES interface by using a common UI software library.

FMMIS currently uses the interChange user interface across the operations portal to interface with FMMIS data. Common Branding unites the recipient portal, the provider portal and the business user/operations user interfaces.

The desired future state, pending cost and value consideration, will have an MES Common UI Framework leveraged across the MES for the recipient portal, the provider portal and the business user/operations user interfaces. The MES Common UI Framework will allow for a cohesive and intuitive user experience even if different vendors implement Module or Service solutions. The UI Framework will also enable AHCA-developed Medicaid related applications to deliver and contribute to a consistent user interface.

Vendors that deliver COTS based solutions are expected to provide a user experience that is consistent with the MES UI Framework.

## Strategic Topic 3-2: Agency UI Strategy for MES and Non-FMMIS

### 3.8 STANDARDS AND TECHNOLOGY MATURITY

To achieve best value for the MES Program, it is important to consider the maturity of the standards and technologies used in modules and MES Projects. Continuous improvement and market driven incentives will always present new opportunities to improve cost or service delivery effectiveness. The MES Program recognizes that while newer standards and technologies can provide benefits there may also be uncertainty, risks and costs associated with the implementation of new standards and technology. The MES Program also recognizes that use of mature technologies also increases the risk of obsolescence or higher operational costs. The MES Program seeks to implement solutions that consider these factors and aligns with the Agency's desired level of solution maturity.

The Rogers Bell curve, **Exhibit 3-7: Rogers Bell Curve: Category percentages are across all industries** categorizes an organizations tolerance for change and novelty. Note the chart graphically depicts the percentages of organizations in each category as the area under the curve. The MES Technology adoption toward innovation recognizes the principle of preventing avoidable Agency disruption. Looking at the chosen categories in **Strategic Topic 3-3: MES Technology Adoption Category** can be useful in understanding the Agency's position on the desired maturity of adopted technology.



**Exhibit 3-7: Rogers Bell Curve: Category percentages are across all industries**

**Strategic Topic 3-3: MES Technology Adoption Category** describes the MES Program adoption category positions over time.

ADOPTION CATEGORY	Current	TIMELINE			
		2018	2020	2022	2025
Innovators					
Early Adopter		MES	->		
Early Majority	AHCA IT, Non-FMMIS	->			MES
Late Majority	FMMIS				
Laggards					

**ANALYSIS**

ADOPTION CATEGORY	TIMELINE			
	Current	2018	2020	2022
<p>Currently AHCA IT and Non-FMMIS applications are in the early majority category and are expected to remain that way to balance technological innovation with stability and security requirements. FMMIS is currently in the late majority.</p> <p>The Agency position on MES is to be an early adopter in the Medicaid space, of technology which is established in other industry sectors. The technologies that will differentiate FMMIS as late majority versus the MES as an early adopter are, for example, cloud computing, EaaS, fine-grained modular services, ESB, and decoupled UI framework.</p> <p>It is expected that by 2025 the Agency's strategic position will move to early majority because MES will have a certain level of maturity and will likely be looking at new proven solutions implemented in other states and other markets.</p>				

### Strategic Topic 3-3: MES Technology Adoption Category

#### 3.9 COTS USAGE

COTS products exist on a wide spectrum, from turnkey systems like the Microsoft Office Suite, to system components like the InRule rules engine to full claims processing products like Pega Claims Processing Software and CNSI eCams. Moving toward the components end of the spectrum, the value of well-defined interfaces which use open standards for file formats and communication protocols grows substantially.

When open standards are not required and promoted, integration of COTS products toward the components end of the spectrum can require tightly-coupled custom code, referred to as "glue code", to be integrated into the system. The more customized the integration the more complex the decision process to adopt and the subsequent implementation of the product integration. This type of tightly-coupled integration adds inflexibility to the system and increases the overall system costs of maintenance and support.

A strong adherence to open standards and discouraging highly coupled integrations requiring "glue code" will encourage and facilitate the integration of COTS products and allow the Agency to maximize the savings benefit of using off the shelf solutions. Loosely coupled integrations through an ESB, API's and fine-grained services that use open standards are highly reusable, testable and less complex to maintain and upgrade.

An important consideration when adopting a COTS technology is the adoption risk. MES will consider technology adoption risk to realize better returns from COTS product investments.

#### 3.10 ACTIVITY PRIORITIZATION

The MES will prioritize activities based on the business needs and on the resulting business value. The Agency's portfolio management process: MES S-4: Strategic Project Portfolio Management Plan (SPPMP) will evaluate business value continually as the platform matures and requirements become more defined and targeted. As with most enterprises, the Agency has resource constraints with respect to funding, staff, and time. The SPPMP helps identify,

categorize, evaluate across multiple dimensions, and select appropriate MES projects. Section 2 of the SPPMP, Exhibit 2–2: System Strategy and Portfolio Management, presents a visualization of the Agency’s portfolio management process.

### 3.11 TECHNICAL SERVICE AVAILABILITY STRATEGY (TSAS)

Ensuring high technical service availability is paramount in maintaining continuous operations in the MES. All components of the MES from the enabling infrastructure (e.g. servers, storage, communications, platforms, etc.) to the technical services exposed by the application modules will participate in the TSAS. The TSAS also covers datacenter considerations.

#### 3.11.1 DATACENTER AVAILABILITY

The MES technology strategy recommendation is to use a carrier-neutral datacenter to address capacity and resilience requirements and maintain high service availability.

Use of an alternate site can improve datacenter availability. The alternate site must support the same system operations as the main site. The three alternate site types are cold sites, warm sites, and hot sites.

- **Cold Site** - is datacenter space without any server-related equipment installed. The cold site provides power, and cooling which can be used if there is a significant outage to the main datacenter. The cold site will need extensive engineering and IT personnel, in addition to all necessary servers and equipment set up, migrated and made functional. Cold sites incur the longest delay to achieve full operation and are the least expensive choice to use. This choice is suited for non-critical applications that can have long downtimes.
- **Warm Site** - offers datacenter space and has the hardware necessary to achieve full production operation. A warm site will have only servers ready for the installation of production environments. Systems must be updated; latest backups must be delivered, and restoration completed in before service can be restored. This choice is suited for non-critical applications that can have moderate downtimes and need some degree of redundancy.
- **Hot Site** - is a mirror of the current datacenter infrastructure. The most important feature offered from a hot site is that the production environment(s) are running concurrently with the main datacenter. System deployments, application deployments and data replication keep both the main site and the hot site in sync. In case of a significant outage event to the main datacenter, the hot site can take the place of the affected site immediately. This choice is the most expensive one to use. This choice is suited for mission-critical applications that can have minimal downtimes and need a high degree of redundancy.

In light of the critical services that the MES provides, the MES disaster recovery strategy recommendation for MES technical services is to use a hot site. The main site houses production, development and testing tiers. The alternate hot site houses a mirror of the

production site used for failover. Both the main and alternate hot site continuously synchronize information and systems artifacts to keep the hot site current in case it is needed for failover. Either site should provide system operations as necessary in case of a disaster or outage. Additionally, the MES must follow Agency standards and practices for backing up data and systems including the use of offsite storage where appropriate.

It is worth noting that the MES TMS cloud strategy future state is designed to eliminate the need for a physical hot site expense and substitutes the availability strategy with a combination of hot site cloud failover deployment, node clustering, and rapid cloud deployments.

### 3.11.2 AVAILABILITY PRINCIPLES FOR APPLICATION MODULES AND THEIR SERVICES

Application modules should adhere to the following principles to participate in the TSAS.

- **Deploy in virtualized environments** - application modules will deploy in virtualized environments, register and communicate with the ESB using standard protocols and interfaces.
- **Handle large request volumes and provide high availability** – Application modules must have a high availability strategy such as load balanced multiple instances, node clustering, etc.
- **Possess rapid deployment capabilities** – Application modules must have clear image build configurations and versioned image builds available for download from secure repositories.
- **Self-configure on startup** – Application modules must be able to configure themselves on startup using parameters supplied by a configuration management service.
- **Participate in the MES deployment** - MES services in both locations have the same availability requirements and participate in the same deployment orchestration. Application modules deployed to the main site production tier usually deploy simultaneously to the alternate hot site. To reduce risk associated with deployment of new or updated modules or changes in data, the deployment approach may introduce changes at a single site and take the other site offline until validation of the new deployment completes. This allows use of the alternate site to restore service if deployment back-out processes are complex or time consuming.
- **Configuration Item or Data Corruption** – In a hot site model with simultaneous deployment and near real time data synchronization, there is a risk the corruption of an application software core, configuration item or data would reduce the ability to operate from either location. Deployment processes must consider this risk and provide the ability to recover from corruption events within service standards.

### 3.11.3 COTS CONSIDERATIONS

When considering a hot alternate site, software license agreements may be affected. COTS products should have clear licensing options to support the hot site deployment, as the

applications will be in operation. Some license agreements allow for the installation of software at a hot site at no additional cost, if only one site is in operation at a time.

#### **3.11.4 SAAS CONSIDERATIONS**

While SaaS products may not adhere to the specific implementation details of MES Technical Service Availability, they should adhere to the principle which prescribes application modules to load balance requests, avoid single points of failure, and provide high availability. SaaS application modules also participate in the ESB service registration.

Because SaaS products may lack transparency of technology architecture, infrastructure, operations monitoring and implementation details, the Agency should:

- Define specific SLAs and performance criteria for SaaS solutions
- Specify testing to assess risk including stress, volume and continuous operation testing
- Include requirements for notification of internal operations deployments, changes and maintenance that affect system availability
- Require visibility to internal solution architecture and operations monitoring insights of the solution

## SECTION 4 TRANSFORMATION CHALLENGES

### 4.1 OVERVIEW

There will be many technology challenges to overcome on the transformation to the Medicaid Enterprise System. The primary categories of technology challenges span a wide spectrum including:

- Technology implementation
- Operations considerations
- Technology interoperability
- Scalability and capacity
- Security
- Technology industry and market disruptors
- Technology change management

The MES Technology Strategy identifies, communicates, engages and monitors MES Projects for the purposes of avoiding, mitigating and overcoming technology challenges.

### 4.2 INVENTORY OF TECHNOLOGY CHALLENGES

CHALLENGE	IMPACT	MITIGATION
<b>Technology Implementation</b>		
MES technologies implementations need to consider the entire technology ecosystem including technology modernization impacts to health plans, providers and recipients	<ul style="list-style-type: none"> <li>▪ Modernization efforts external to the Agency may not align with MES technology direction</li> <li>▪ May want to expand use and reuse of technology and data services for use outside of traditional system scope areas</li> </ul>	<ul style="list-style-type: none"> <li>▪ Ongoing communication of strategy</li> <li>▪ Use of collaborative governance processes</li> <li>▪ Perform periodic strategy refreshes considering overall ecosystem</li> <li>▪ Use technical requirements verification and validation.</li> </ul>
Increased role of technology in business processing (e.g. enterprise business rules, real-time analytics, artificial intelligence bots)	<ul style="list-style-type: none"> <li>▪ Difficult to change ingrained and mature business processes</li> <li>▪ More attention on system availability, capacity and scalability</li> <li>▪ Organizational change and position descriptions affected</li> </ul>	<ul style="list-style-type: none"> <li>▪ Include organizational change management in transition services</li> <li>▪ Validate capacity, availability, and scalability assumptions early</li> </ul>

CHALLENGE	IMPACT	MITIGATION
Modular technology solution implementation takes longer to implement	<ul style="list-style-type: none"> <li>▪ Increased elapsed time and total cost to modernize entire system</li> </ul>	<ul style="list-style-type: none"> <li>▪ Communicate and manage expectations</li> <li>▪ Communicate benefits including: reduced risk, faster and larger outcomes, increased competition, increased business agility</li> <li>▪ Use technical requirements verification and validation.</li> <li>▪ Use MES Modularity Strategy.</li> </ul>
Inconsistent user interfaces (UI) and user experiences across multiple vendor solutions	<ul style="list-style-type: none"> <li>▪ Higher training and change management</li> <li>▪ Reduced user productivity</li> </ul>	<ul style="list-style-type: none"> <li>▪ Develop an Agency standard Common UI Framework and promote use of the framework</li> <li>▪ At a minimum enforce UI style standards</li> <li>▪ Use technical requirements verification and validation.</li> </ul>
Modularity increases use of multiple technology vendors	<ul style="list-style-type: none"> <li>▪ Increased integration complexity</li> <li>▪ Increased vendor management costs</li> <li>▪ Reduced licensing negotiating power</li> <li>▪ Increased variety in maintenance and support skills</li> <li>▪ Increased dependency on vendors</li> </ul>	<ul style="list-style-type: none"> <li>▪ Ongoing analysis of cost and benefits</li> <li>▪ Select appropriate mix that balances competition and synergy impacts</li> <li>▪ Knowledge transfer to AHCA FTE's.</li> </ul>
Monitoring and auditing multi-vendor solutions	<ul style="list-style-type: none"> <li>▪ Each technology solution could require unique monitoring and audit tools and techniques</li> </ul>	<ul style="list-style-type: none"> <li>▪ Use a centralized logging and monitoring solution that correlates system events with service requests</li> <li>▪ Require services to have default monitoring methods</li> <li>▪ Use technical requirements verification and validation.</li> </ul>
Technology procurement and implementation process have significant bureaucracy	<ul style="list-style-type: none"> <li>▪ Benefits of modular technology implementation diminished by overhead in procurement and project implementation</li> </ul>	<ul style="list-style-type: none"> <li>▪ Evolve to agile procurement and technology implementation processes</li> <li>▪ Embrace “fail fast” for technologies or projects that don't produce outcomes or where better alternatives exist</li> </ul>

CHALLENGE	IMPACT	MITIGATION
Service versioning and service introduction	<ul style="list-style-type: none"> <li>▪ Upgrades and changes to business, technology or data services used across modules is difficult to coordinate and implement</li> </ul>	<ul style="list-style-type: none"> <li>▪ Design integration platform, service providers and service consumers to support concurrent use of service versions to simplify deployment coordination</li> <li>▪ Dependency management solutions will allow a system to be composed of independently developed modules and services which are at different levels of maturity. These solutions rely on versioning standards and the service registry.</li> <li>▪ Use technical requirements verification and validation.</li> </ul>
Vendor adoption of MES Data and Technology Strategy	<ul style="list-style-type: none"> <li>▪ Modularity and decoupling of proprietary application data stores commoditizes the market and reduces vendor profit potential</li> <li>▪ Smaller project sizes may reduce interest causing fewer technology opportunities and increased vulnerability to single vendor dependence.</li> </ul>	<ul style="list-style-type: none"> <li>▪ Use buying power to shape market toward modern, standards-based architectures, communication protocols, and technologies that align with market and industry trends</li> <li>▪ Proactively communicate expectations with vendor community</li> <li>▪ Coordinate with other states to accelerate vendor adoption.</li> </ul>
Technical challenges with use of data replication as transition strategy between ODS and FMMIS	<ul style="list-style-type: none"> <li>▪ Cross system data inconsistencies</li> <li>▪ Decreased data integrity</li> </ul>	<ul style="list-style-type: none"> <li>▪ Evaluate which data to replicate or synch and at what frequency</li> <li>▪ Test and validate replication speed requirements of the MES and the requirements for transactional consistency</li> <li>▪ Geographical proximity and fast networks may reduce latency issues.</li> <li>▪ Use technical requirements verification and validation.</li> </ul>

**Operations Considerations**

CHALLENGE	IMPACT	MITIGATION
Maintenance of technologies and systems that will be replaced	<ul style="list-style-type: none"> <li>▪ Difficult to justify maintenance and upgrade expenditures for technology and systems that will be replaced</li> <li>▪ Business improvement frozen during period of transition to new technology and systems</li> </ul>	<ul style="list-style-type: none"> <li>▪ Prioritize replacement of technologies that are deemed crucial to MES business continuity to avoid pressures to upgrade old systems.</li> <li>▪ As the transition occurs, identify dependencies and make their continuous operation a requirement of integration testing.</li> </ul>
Difficult to incrementally replace or upgrade parts of a large highly integrated system (e.g. FMMIS, FLORIDA)	<ul style="list-style-type: none"> <li>▪ The large legacy system will need to expend transition service costs to perform maintenance to allow parallel operation or partial decommissioning during transition</li> </ul>	<ul style="list-style-type: none"> <li>▪ Use strategies (e.g. interim data replication) that reduce changes to the large system as functionality is decommissioned</li> <li>▪ Evaluate benefit of integrating new components to legacy system for interim benefits to legacy system</li> <li>▪ Use technical requirements verification and validation.</li> </ul>
Monitoring use of cloud-based infrastructure and systems management of cloud-based services	<ul style="list-style-type: none"> <li>▪ Inability of modules to scale on demand (auto-scale)</li> <li>▪ Cloud services costs incurred in excess of use</li> </ul>	<ul style="list-style-type: none"> <li>▪ Use a cloud management module that can integrate modules and systems to the cloud infrastructure provisioning API's and dynamically allocate and de-allocate nodes as needed.</li> </ul>
<b>Technology Interoperability</b>		
Use of multiple technology architectures and platforms (e.g. Java, .NET, PaaS, SaaS)	<ul style="list-style-type: none"> <li>▪ Increased vendor management</li> <li>▪ Increased monitoring complexity</li> <li>▪ Reduced reuse and processing consistency</li> <li>▪ Resistance to use of enterprise technology services</li> <li>▪ Vendor and platform dependence</li> <li>▪ Increased skill variety for maintenance and support</li> </ul>	<ul style="list-style-type: none"> <li>▪ Define and communicate core acceptable platforms and preference for use of core platforms</li> <li>▪ Ongoing analysis of cost and benefits</li> <li>▪ Transition solutions on non-core or outdated platforms to core platforms over time</li> </ul>

CHALLENGE	IMPACT	MITIGATION
Platform dependence due to a lack of a standards-based service layer on the platform	<ul style="list-style-type: none"> <li>▪ Creates a dependence on the underlying platform's custom communication protocols and data formats</li> </ul>	<ul style="list-style-type: none"> <li>▪ Technical standards, a universal data dictionary, a business and technical service dictionary, and standard definitions of common elements will enable the MES's platform independence.</li> <li>▪ Use technical requirements verification and validation.</li> </ul>
Coordination between technology and module vendors	<ul style="list-style-type: none"> <li>▪ Increases in collaborative governance requirements, potential for strategy misalignment, issue tracking.</li> </ul>	<ul style="list-style-type: none"> <li>▪ Vendor that provides Interoperability Services and Integration Platform provide leadership and coordination between technology solutions</li> <li>▪ Use MES strategy for collaborative governance</li> </ul>
Continuous technology deployment across a distributed ecosystem	<ul style="list-style-type: none"> <li>▪ Configuration management and release management complexity increases based on the number and types of technology deployed</li> </ul>	<ul style="list-style-type: none"> <li>▪ Use a continuous integration infrastructure and process that can validate integration testing of new or updated technology before deployment to production environments</li> <li>▪ Use a change management approach for continuous deployment.</li> <li>▪ Use technical requirements verification and validation.</li> </ul>
<b>Scalability and Capacity</b>		
Ability to support scale and capacity due to new projects such as the 360 view where information exchanges could increase exponentially	<ul style="list-style-type: none"> <li>▪ The inability to support large data volumes and data access requests could result in system crashes, outages, service disruption, and slow system response time</li> <li>▪ Some vendor solutions may not be viable at the scale envisioned to support the Medicaid Enterprise</li> </ul>	<ul style="list-style-type: none"> <li>▪ Validate solutions early and often beginning at procurement phase</li> <li>▪ Seek solutions that incorporate high capacity techniques like: Cloud auto-scaling, application node monitoring, database clustering, database partitioning, sharing and caching strategies.</li> <li>▪ Use technical requirements verification and validation.</li> </ul>

CHALLENGE	IMPACT	MITIGATION
Continuous high availability needed by SOA	<ul style="list-style-type: none"> <li>Service instances can become unresponsive due to a high request volume.</li> </ul>	<ul style="list-style-type: none"> <li>An increase of load balanced service instances, and request work queues.</li> <li>Use technical requirements verification and validation.</li> </ul>
Storage strategy for rapid increases in data volume	<ul style="list-style-type: none"> <li>Storage requirements increase over time. Transitioning to a SOA is anticipated to further increase storage requirements.</li> </ul>	<ul style="list-style-type: none"> <li>Proactively perform storage capacity planning and monitoring</li> <li>Stay closely aligned with business on changes in storage usage factors</li> <li>Use elastic resource allocation capabilities inherent in cloud solutions (e.g. Storage as a Service)</li> <li>Use technical requirements verification and validation.</li> </ul>
Network capacity and resiliency	<ul style="list-style-type: none"> <li>The deployment of MES modules on remote cloud technologies increases the dependency on network capacity and resiliency for system access and processing availability. Increasing recipient populations, encounter data, real-time integrations, and reuse of business and technical services place additional demands on the network.</li> </ul>	<ul style="list-style-type: none"> <li>Capacity modeling, testing, and proactive monitoring help avoid impacts</li> <li>Consider Ethernet backbones in carrier neutral facilities to address capacity and resilience. Virtualization technologies can play a critical role in addressing resiliency issues.</li> </ul>
Communications latency due to increased services over the network	<ul style="list-style-type: none"> <li>Quality of user experience could be degraded</li> <li>Processing delays in MES services (e.g. eligibility responses)</li> </ul>	<ul style="list-style-type: none"> <li>Optimize physical proximity of highly interactive services, increased bandwidth allocation, system design, and caching strategies.</li> </ul>
Change in network usage patterns	<ul style="list-style-type: none"> <li>Changes in size and number of network messages may alter network design requirements</li> </ul>	<ul style="list-style-type: none"> <li>Model, test and monitor network throughout technology and system implementation lifecycle</li> </ul>

**Security**

CHALLENGE	IMPACT	MITIGATION
Data privacy and security technologies and responsibilities are distributed across many vendors and service providers	<ul style="list-style-type: none"> <li>▪ Increased coordination effort between vendors</li> <li>▪ Increased effort to monitor and address issues that could cause compromised recipient data, system user data and security breaches.</li> </ul>	<ul style="list-style-type: none"> <li>▪ A comprehensive security strategy focused on prevention</li> <li>▪ Interoperability services vendor plays active role</li> <li>▪ Clear communication to vendors on security requirements in MES T-8 Enterprise Data Security Plan and MES Technology Security Standards in TSRG</li> <li>▪ Use technical requirements verification and validation.</li> </ul>
Departmental and personal data stores and applications may not use enterprise security policy	<ul style="list-style-type: none"> <li>▪ Bypass access controls</li> <li>▪ No logging of usage</li> <li>▪ Unknown data loss</li> <li>▪ Higher risk of data breach</li> <li>▪ Processes to identify and respond to data breach are less mature</li> </ul>	<ul style="list-style-type: none"> <li>▪ Enforce enterprise security policy and standards with equal to all systems with sensitive data</li> <li>▪ Eliminate need for departmental and personal data stores and applications</li> </ul>
<b>Technology and Industry Market Disruptors</b>		
Technology industry and market disruptors (e.g. Blockchain, crypto currency, telemedicine, cognitive processing, behavioral economic processing) gain rapid adoption	<ul style="list-style-type: none"> <li>▪ Current MES technology and module planned MES infrastructure investments could be disrupted or not used</li> <li>▪ New investments of capital and resources needed to accelerate adoption of disruptive technologies</li> </ul>	<ul style="list-style-type: none"> <li>▪ Consider technology strategy contingency strategy if technology market disruptors accelerate or fail</li> <li>▪ Perform ongoing strategy refresh to assess market disruptors and adjust strategy</li> <li>▪ SPPMP</li> </ul>
COTS solution vendor reluctance to use Enterprise Services	<ul style="list-style-type: none"> <li>▪ COTS solutions that use their own custom or proprietary services could introduce processing inconsistency</li> <li>▪ Duplication of processing could raise long term maintenance cost</li> <li>▪ Vendors charge “extra” to use MES Enterprise services</li> </ul>	<ul style="list-style-type: none"> <li>▪ Validate COTS solutions’ use of open standards and protocols and ability to use MES services.</li> <li>▪ Use technical requirements verification and validation.</li> </ul>
Open source technology solutions and conversion of vendor modules to open source	<ul style="list-style-type: none"> <li>▪ Lack of support and maintenance</li> <li>▪ Lack of ongoing investment in module improvement</li> <li>▪ Reduced opportunity for vendor investment recovery across multiple states</li> </ul>	<ul style="list-style-type: none"> <li>▪ Select open source products if vendor support is available</li> <li>▪ Monitor use of open source solutions by other states</li> <li>▪ Use technical requirements verification and validation.</li> <li>▪ Use MES TMS</li> </ul>

CHALLENGE	IMPACT	MITIGATION
<b>Technology Change Management</b>		
Establishing a culture of real-time information and integration	<ul style="list-style-type: none"> <li>Resistance to adoption of real-time information exchange and data access may drive legacy processing styles into design that undermines benefit to the Program</li> </ul>	<ul style="list-style-type: none"> <li>Agency and MES Project leadership should reinforce importance of real-time high-quality data to support decision making and program operations where appropriate.</li> </ul>
Culture of analyzing data in the new MES	<ul style="list-style-type: none"> <li>Resistance to data analysis tool changes, utilization of data marts and perceived loss of control of data may drive legacy data handling and ownership styles into design that undermines benefit to the Program</li> </ul>	<ul style="list-style-type: none"> <li>Agency and MES Program leadership support for future vision</li> <li>Selection of appropriate persona specific tools</li> <li>Appropriate data mart design</li> <li>Appropriate user tool training</li> </ul>
Data sharing agreements to enable use of social determinants of health data	<ul style="list-style-type: none"> <li>Organizations routinely describe large value propositions of using data from other systems but are reluctant to share data in their own systems.</li> </ul>	<ul style="list-style-type: none"> <li>Strong executive sponsorship is the most effective technique to break down data sharing barriers</li> <li>Simplify / Streamline data sharing agreement process</li> </ul>
Data duplication and data ownership issues	<ul style="list-style-type: none"> <li>Business units create data silos independent from the authoritative data sources. Use of these data silos results in inconsistent implementation of policy, inaccurate reporting, and decision making based on different data sources</li> </ul>	<ul style="list-style-type: none"> <li>The MES Data Strategy including use of the ODS, RDS and EDW will provide the single source of truth for MES data</li> <li>A granular implementation of data services, caching strategies and persona-based data marts will facilitate quick access to data avoiding the need for business unit specific implementations.</li> </ul>

**Exhibit 4-1: Transformational Challenges Details**

## SECTION 5 TECHNICAL SERVICES GOVERNANCE

MES Technical Services Governance is a specific implementation and use of the MES Project governance processes and framework defined in SEAS deliverable S-1 Medicaid Enterprise Systems Governance Plan. MES Technical Services Governance describes the use of the MES Governance Plan to make and implement MES Technical Services decisions.

This section discusses technical management topics governed through the structures and processes described in the MES Governance Plan. This section describes technical architects, both Agency and sister Agencies, and MES project vendors. In the MES Governance plan, each of these roles is a specialized type of subject matter expert. Technical architects perform important roles of identifying and communicating issues requiring decisions and implementing decisions resulting from the MES Governance processes. The MES Governance processes and structure support the MES Technical Services Governance. The following discussion about MES Technical Services Governance does not imply a different or additional governance structure for the MES Project.

For the MES Project, Technical Services Governance (TSG) refers to the overall process of promoting and ensuring trusted technical models support all business areas and control redundancy management. The benefits of standardizing services across systems in the enterprise are a decrease in data and application replication, improved cost effectiveness of data sharing, and an increase in system and data quality.

### 5.1 SERVICE CONTRACTS

Services are configured using a service contract and an orchestration language. The service contract defines access to an individual service. Orchestration is the process to define a flow that links several services together.

A service contract describes the interface's expected behavior and the service's security and privacy constraints. The contract enables thorough testing of the service through various scenarios to validate service contract compliance.

As a governance tool, a service contract reflects the purpose, capability, and interface content quantity approved by MES Technical Services Governance.

### 5.2 USE OF MES GOVERNANCE PROCESSES

The MES Governance provides a tiered structure and processes that provide leadership, guidance, decision making and overall direction for the MES Project. Technical Services Governance applies this same structure and process.

The Technology Asset Team (TAT) is the primary governance entity for technology management subjects. The TAT can escalate or coordinate with other MES governance entities as needed. The Technology Asset Team supports both planning and control functions.

### 5.3 ROLES AND RESPONSIBILITIES

ROLE	RESPONSIBILITIES
SEAS Technical Architect	<ul style="list-style-type: none"> <li>Identifies the Technical Services to perform within the system</li> <li>Evaluates Technical Service Request</li> <li>Proposes new, updates and retirement of technology service components to the Technical Asset Governance using the Technical Service Request</li> <li>Maintains Service Registry</li> </ul>
MES Technology Governance (MTG)	<ul style="list-style-type: none"> <li>Reviews proposed Technical Services</li> <li>Approves or denies Technical Services</li> </ul>
MES Sister Agencies	<ul style="list-style-type: none"> <li>Reviews and may align technology solutions to MES technology architecture service standards</li> <li>Contributes recommendations for enhancements to existing Service Registry entries</li> <li>Contributes recommendations for new Service Registry entries</li> </ul>
Integration Services Integration Platform (ISIP) Vendor	<ul style="list-style-type: none"> <li>Consults with technology stakeholders in the use of integration platform</li> <li>Consults and guides MES Project Vendors in designing, implementing and maintaining interoperability between MES modular components</li> </ul>
MES Project Vendor	<ul style="list-style-type: none"> <li>Identifies and understands MES Service Registry Entries</li> <li>Provides vendor specific Service Registry entries</li> </ul>

#### Exhibit 5-1: Technical Services Roles and Responsibilities

### 5.4 RACI MATRIX

**Exhibit 5-2: RACI Matrix for Technical Services Governance** presents a sample Responsible, Accountable, Consulted, and Informed (RACI) table for an initial set of MES data governance activities.

Legend: **R** (Responsible), **A** (Accountable), **C** (Consulted), **I** (Informed)

SERVICE ACTIVITIES	ROLE RESPONSIBILITIES				
	SEAS TECHNICAL ARCHITECT	MES TECHNOLOGY GOVERNANCE	MES SISTER AGENCIES	ISIP VENDOR	MES PROJECT VENDOR
Identifies the Technical Services to perform within the system	RA	C	C	C	C
Evaluates Technical Service Request	RA	C	C	C	C

SERVICE ACTIVITIES	ROLE RESPONSIBILITIES				
Proposes new, updates and retirement of technology service components to the MES Technology Governance using the Technical Service Request	RA	C	C	C	C
Maintains Service Registry	RA	I	I	C	C
Reviews proposed Technical Service.	C	RA	C	C	C
Approves or denies Technical Services	C	RA	I	C	I
Reviews and may align technology solutions to MES technology architecture service standards	C	C	RA	I	I
Contributes recommendations for enhancements to existing Service Registry entries	C	C	RA	I	I
Contributes recommendations for new Service Registry entries	C	C	RA	I	I
Identifies and understands MES Service Registry Entries	C	C	I	C	RA
Provides vendor specific Service Registry entries	C	C	I	C	RA

**Exhibit 5-2: RACI Matrix for Technical Services Governance**

## 5.5 GOVERNANCE PROCESS

Technical services governance processes align with the MES Technology Domain standards setting processes. For this reason, the Agency and SEAS Vendor will leverage the processes and tools used for MES Technology domain standards.

The governance of MES Technology domain standards follows a defined process to communicate, support vendors, assess compliance, and report compliance to MES Technology domain standards. A summary of the defined process is that:

- The AHCA Technology Asset Team (TAT) governance entity makes and approves technology decisions related to the technology assets of the Agency. Technology

services are a type of technology asset and thus the Technology Asset Team is the entry point for data governance decisions.

- The SEAS Vendor researches, advises, and prepares materials for TAT governance approval. The SEAS Vendor develops communication materials, implements the communication processes, provides MES Project Vendor support, conducts compliance assessments and reports compliance to the Agency.
- The AHCA MES Technical Domain Lead directs the SEAS Vendor and authorizes the release of communications, providing vendor support, conducting compliance assessments and reporting compliance to the Agency.

The document that describes the complete process is accessible via hyperlink below to the document on the MES Repository.

[SEAS NH T-6 Technology Standards Communication, Support, Compliance and Compliance Reporting Procedures](#)

## 5.6 SUBJECT AREAS FOR GOVERNANCE

From MITA Part III, Chapter 4 Technical Services, there are three broad groupings or areas where technical services governance applies. They are:

- **Access and Delivery** – Access and Delivery focus on the way users (e.g. AHCA staff, sister agencies, the public) gain access to Agency systems and technology and consume information (via technical services) from Agency systems and technology. For the MES Project, this includes topics like technical services for authentication and authorization, forms, reports, business intelligence (BI) capabilities, portals, etc. Technical services related to Access and Delivery will be governed using the TSG process.
- **Intermediary and Interface** – Intermediary and Interface focus on the way systems, both internal and external to the Agency, communicate and share information to provide business value to the Agency. Technical services in this category communicate using the Integration Platform and focus on business process management, workflow, service orchestration, and data sharing. Technical services related to Intermediary and Interface use the TSG processes.
- **Integration and Utility** – Integration and Utility focus on traditional technical cross cutting capabilities like logging, auditing, configuration management, rules engine and data access enabled via composite data services. Technical services related to Integration and Utility use the TSG process.

Across the three subject areas for technical services governance there are two classifications of technical services. One classification is technical services that are unique to a specific use case within a subject area. The second classification is technical services that are reusable across a broad set of MES use cases. Both classifications of technical services use the TSG process.

## SECTION 6 COLLABORATIVE GOVERNANCE

### 6.1 COLLABORATIVE GOVERNANCE OVERVIEW

The Collaborative governance strategy defines direction, processes and tools to implement modules and systems in an open and flexible way that promotes interoperability. Collaborative governance focuses on communication, input gathering, technology information and asset sharing, and technology decision making including with indirect stakeholders to the MES Project. Indirect stakeholders to MES Project Technology include sister agencies, other states, Providers, Health Plans, healthcare software vendors, the general public, and other stakeholders. Section 5 Technical Services Governance describes the governance processes for technology service implementation by direct stakeholders that implement modules and systems as part of MES Projects.

### 6.2 COLLABORATIVE GOVERNANCE PRINCIPLES

The MES Project seeks to leverage the insights, expertise and collective synergies of stakeholders to the MES Project to create the most effective use of Technology. The Program seeks engagement and trust enhancing contributions and communications among the MES Technology community. Below are collaborative governance principles:

The TREATS acronym highlights collaborative governance principles of the MES strategy and vision:

- Trust -Trusted relationships with organizations and individuals achieve more with less. The MES collaboration approach emphasizes communications that establish, maintain, and enhance system and human interactions using the power of increased trust.
- Reliability - Reliability is an important foundation of trust-based collaboration. MES emphasizes that MES Project Vendors and indirect stakeholders provide reliable information, insights, and discussion on architecture, technology, implementation, and strategy. The result of collaboration is reliable delivery by people that provide or use MES services.
- Experience enabling – Experience enabling refers to MES Project’s simultaneous focus on customer experience and experience-based analytics.
- Agility – Agility in collaboration governance refers to collaborative communication, and decision making at speed. Likewise, the pace of change affecting Medicaid is accelerating. Collaborative governance positions the MES Project to quickly adapt to opportunities and issues that arise from changes in technology, policy, process, or funding.
- Technology – Collaborative governance related to technology includes alignment with MITA and balancing emerging and future technologies with understanding of risk and practicality.
- Services – Collaborative communications related to technology emphasize service orientation. The MES Technical Management Approach emphasizes services. These

include services vendors provide, the service-oriented architecture technology in MITA, and modular processing capabilities provided as technology or business services.

### 6.3 MES GOVERNANCE STRATEGY

The MES Governance Strategy defines the governance structure for decision making and communication directly related to MES Projects. The initial implementation of the MES Governance Strategy supports MES Projects focused on Agency systems. The MES Governance Strategy includes mechanisms for communication with other agencies that are Medicaid stakeholders. The MES Governance Strategy will evolve to optimize communication with the statewide Medicaid Enterprise when planning and implementation of MES Enterprise Integrations and modules begin.

Below is an overview of collaborative governance of technology topics. The approaches described support direct and indirect MES stakeholders.

- Communication – The SEAS vendor is the central point of focus for bi-directional communications about MES technology topics. The SEAS vendor manages the MES Project Repository that holds technology information and assets on a wide range of topics related to MES. Other organizations including the Agency, IV&V Vendor, MES Project Vendors, ISIP vendor coordinate the development and release of technology related communications via the SEAS vendor.
- Input gathering – The SEAS vendor solicits and accepts MES technology related input and recommendations from direct and indirect stakeholders to the MES Project. The SEAS vendor uses the equivalent technology standards governance processes to process input received about technology standards.
- Technology information and asset sharing – The SEAS vendor manages the MES Project Repository including access, content publication and distribution. The vendor that is responsible for the Integration Platform manages technology web service information and asset using the service registry, service repository and service contract management tools described below.
- Technology decision – Technology decisions identified via collaborative governance process follow the normal process used for MES Technology standards governance process. The SEAS Vendor works with the Agency MES Technical Domain Lead to make decisions about communication and escalation of technology related issues identified or introduced by indirect stakeholders to the MES Project.

At a tactical level collaborative governance of technology services, the SEAS vendor will use capabilities provided in the procured Integration Platform to establish and maintain a collaborative environment for all users of technical services, both providers and consumers. The MES Technical Management Approach to modular implementation requires all module vendors and system integrator(s) to closely use the collaborative governance enablers.

The key governance enablers for collaborative governance are:

- Service Registry
- Service Repository
- Service Contract Management

**Exhibit 1-1: SEAS Technology Deliverables** lists SEAS Technology Domain deliverables that contain strategic direction and guidance in additional areas of technology. Together, these areas contribute to the overall effort to foster a common awareness of the standards, strategic approach, and processes governing the strategic management of technology in the MES. The common reference and language used in the SEAS Technology Deliverables is a key enabler of the MES Collaborative Governance strategy.

The governance process to populate and maintain the service registry, service repository, and service contracts follows the Technical Services Governance process as described in Section 5 with specific accountabilities and responsibilities as follows:

#### 6.4 COLLABORATIVE GOVERNANCE RACI

Legend: **R** (Responsible), **A** (Accountable), **C** (Consulted), **I** (Informed)

SERVICE ACTIVITIES	ROLE RESPONSIBILITIES			
	SEAS VENDOR	INTEGRATION SERVICES AND INTEGRATION PLATFORM VENDOR	MODULE VENDOR	AHCA
Install, configure, develop, implement, support, and maintain an enterprise service registry, repository, and contracts	A	R	I	I
Populate enterprise service registry, repository, and contract entries	A	R	I	I
Develop and maintain module specific service registry, repository, and contracts	A	C	R	I

**Exhibit 6-1: RACI Matrix for Collaborative Services Governance**

#### 6.5 COLLABORATIVE GOVERNANCE TOOLS AND TECHNIQUES

Collaborative governance tools provide the repository of technology service information. The tools facilitate a communication strategy that provides quick access to information of interest by providers and consumers of technology services. Collaborative governance is enabled through the following three tools described below. The service registry, service repository, and service contracts are the tools, specifications and service vocabulary that provide the enabling

technology to aid in achieving the Agency strategy of building modules from fine-grained modular services, data services and micro services exposed through standards-based API's.

- **Service Registry** – The Service Registry is a catalog of services, their instances and their locations which helps in service definition, service selection and in enforcing service policies. Service providers register service instances to the service registry at startup and deregister instances on shutdown. Consumers of the service and routers query the service registry to find the available instances of a service.
- **Service Repository** – The Service Repository stores artifacts and assets about the services including functional specs, user and other documentation, and SLAs that define transaction capacity, maximum throughput, downtime etc. The service registry manages run-time assets. The service repository manages both for design time and run-time assets.
- **Service Contract Management** – The Service Contract Management Tool(s) manage the technical web service contract metadata that defines what a service offers and how and where to access the service.
- **MES Project Repository** – The MES Project Repository is the hub of technology vision, strategy, standards and other reference information. It also documents direction on a wide range of technology topics and enables interactive discussion among MES Stakeholders.

Many quality COTS API Management tools in the marketplace provide service registry, service repository and service contract management. Selection and implementation of a specific product occurs with the Integration Platform implementation.

## SECTION 7 TECHNICAL PRINCIPLES

MES Technical Principles provides direction for making technology decisions to implement Medicaid Enterprise System technology services. The MES Technical Principles guide module and system implementation to create an MES future state that is:

- Aligned with MITA
- SOA-based
- Cloud-deployed
- Built in open and flexible way that promotes interoperability

The Technical Principles are accessible to stakeholders of the MES Project. The principles also reside in the Guiding Principles List in the MES Projects Repository.

### 7.1 MES TECHNICAL PRINCIPLES

**Business Driven** - Business needs and opportunities that create business value are the basis for technology selection and use. MES adopts and uses technologies that support business goals or objectives. Technology implementations are to enable achievement of business needs.

**Platform Independence** - Stakeholders will develop solutions that are reusable and platform-independent. Technologies used are to be cloud-ready and SOA-based.

**Adaptability, Extensibility, and Scalability** – MES module, system and service design and implementations are to enable reuse. MES solutions are to provide and use flexible responsive technologies that support future use, growth, and adaptation.

**Open Technology and Standards Based** - Stakeholders will leverage the advantages of standardization (e.g. data sharing, interoperability). Solutions and services should be accessible through open, standard interfaces that are easy to integrate, extend, and reuse. Stakeholders will adhere to the technology standards in the MES Technology Standards Reference Guide ([TSRG](#)).

**Integrated Security & Privacy** – MES modules, systems and services will secure and protect the privacy of MES data.

**Interoperability** – MES modules, systems and services will use the MES Project interoperability enablers including the integration platform, enterprise service bus, MES standards, and the guidance and direction of the SEAS and ISIP vendors to enable data exchange and reuse between services and other entities.

**Quality Data** – Technologies are to provide high quality data via the services they provide. Services are to provide data that is accurate, relevant, accessible and understandable data aligned with the Data Quality Framework described in the MES Data Management Strategy.

**Current and Proven Technology** – The MES Project is to use technologies that are market relevant, available, supported and where possible proven to support the processing complexities and scale of the MES Project.

## 7.2 SOA TECHNICAL PRINCIPLES FOR MODULE AND SYSTEM IMPLEMENTATION

In addition to aligning with MES Technical Principles, MES technology services are to follow the technical principles in the [Best Practices section](#) in The Open Group's "SOA Source Book". The SOA Source Book describes widely agreed upon key principles for services.

### Well-Defined Service Contract

A well-defined service contract is one which describes all available functionality the service provides. Service providers and consumers are to use well-defined service contract standards (e.g., WSDL) that describes details of use to assist the service requestor to invoke the service(s) required. Automatic generation of service contracts from APIs or services that are undocumented or under documented is unacceptable. Likewise, direct database-to-schema conversion contract generation is also unacceptable because it introduces tight-coupling between message and database.

### Define Services with Appropriate Granularity

Service providers are to design services for appropriate granularities that offer greater flexibility to service requestors without affecting the performance and security. Services granularity should make it easy for service requestors to assemble services to execute business scenarios. This is not always possible, especially for (multi-step) transaction-oriented systems. Each service should define the granularity of the service (e.g., which steps of functionality and invocations of other services or modules take place).

### Loosely-Coupled Services

Service requestors can consume services without any knowledge about the technical details associated with a service implementation. As long as the implementation meets the specified Service-Level Agreement (SLA), knowledge of the technical solution implementation is unnecessary. This also relates to the principle of well-defined service contract, described earlier.

### Design Services for Stateless Operation

Services invocation is to be independent of the state of other services and each service invocation has all the required information from one request to another.

### **Ensure Services have Appropriate Security Enforcement Standards**

Service providers are to design and implement services with appropriate security policy enforcement mechanisms to ensure that only authorized requesters can successfully invoke them. An objective of the MES Integration platform is to centralize identity management and access policies at the integration layer to enforce consistency of security policy.

### **Follow SOA Ontology/Vocabulary Standard**

The MES Project will communicate using common vocabulary standard throughout the services lifecycle to effectively facilitate SOA adoption and have required alignment between the business and IT communities. An MES ontology defines the SOA concepts and semantics commonly understood by all stakeholders and enables effective communications. Refer to Section 5.8 of the SEAS Deliverable [T-5: Technical Architecture Documentation](#).

## SECTION 8 TECHNICAL GOALS AND OBJECTIVES

In addition to being aligned with MITA technical goals in Part III Chapter 2 Technical Management Strategy, the MES Technical Goals and Objectives are achievement targets aligned with the MES Strategic objectives that support the Agency mission to improve health care for all Floridians.

- Goal 1: Apply Cloud Computing concepts where possible and feasible.
  - › Objective 1: Enable scalability, elastic resource allocation, and high availability across the MES.
- Goal 2: Use rules engines technologies, where possible, to extend the system configuration abilities to the business community.
  - › Objective 1: Enable and support interoperability, integration, and open architectures.
- Goal 3: Follow MES performance standards for accountability and planning.
  - › Objective 1: Review national standards for health and data exchange and open standards for technical solutions, using existing national standards whenever possible. When Medicaid-specific standards are necessary, the Centers for Medicare and Medicaid Services (CMS) will support collaboration efforts of industry groups in the submittal of proposed standards to national standards organizations for review and approval.
  - › Objective 2: Use the set of MITA Framework common business processes and Data Standards to make it possible to develop performance standards, measurement techniques, and corresponding utility services.
- Goal 4: Develop systems that can effectively communicate to achieve common program goals through interoperability and common standards.
  - › Objective 1: Adhere to technology standards, specifically open standards, to facilitate integration of Commercial Off-the-Shelf (COTS) solutions and the reuse of solutions within the Agency and the State, resulting in lower development costs and reduced development risk.
  - › Objective 2: Adopt data and industry standards and promote the development of appropriate standards when needed.
  - › Objective 3: Promote the use of data and technology standards to improve the cost effectiveness of development. The use of Data Standards provides better access to data by promoting data consistency and enhanced sharing through common data-access mechanisms.
  - › Objective 4: Use standard definition formats to map data to standard data elements, where appropriate, and provide the data descriptions when the data elements are nonstandard.
  - › Objective 5: Represent security and privacy access rules for each data element in a standard manner.

- › Objective 6: Employ a collection of services to read the data descriptions and security/access rules to release information to authorized users for processing.
- › Objective 7: Promote secure data exchange. MITA defines and integrates security and privacy capabilities throughout the architecture by identifying access requirements in the business processes, defining them within the data models, and applying them through the MITA technical models.
- Goal 5: Promote an environment that supports flexibility, adaptability, and rapid response to changes in programs and technology.
  - › Objective 1: Promote reusable software and hardware components and modularity.
  - › Objective 2: Maximize the benefit across the State Medicaid Enterprise, while promoting innovation and creativity in the MES environment.
  - › Objective 3: Enable and support interoperability, integration, and open architectures.
  - › Objective 4: Employ services that make it possible to deploy common interoperability (i.e., system-to-system communication) and access (i.e., system-to-person communication).
  - › Objective 5: Package common functionality and capabilities with standard, well-defined interfaces (i.e., services), used by new applications, legacy applications, COTS software, or all three, to invoke the functionality.
  - › Objective 6: Provide adaptability and extensibility. An adaptation (i.e., the capability that allows users to change the specifics of processes, data, or technical solutions using configuration files) enables the Agency to customize MES elements to meet their unique needs. An extension (i.e., the capability that allows users to add functionality and capabilities) enables Agency to add new functionality to MES elements to meet their needs, while still meeting MITA goals and objectives.
- Goal 6: Provide data that is timely, accurate, usable, and easily accessible to support program analysis and decision-making.
  - › Objective 1: Develop reusable services to allow a single service to pass eligibility information from a variety of program systems to a mechanized claims processing, information retrieval, or eligibility determination systems.
  - › Objective 2: Improve data quality by using Data Standards, applying standard performance standards, and relying on the availability of the enhanced data exchange and sharing provided by the hub architecture.
- Goal 7: Reduce duplication of costs by collecting data already available elsewhere and using that data to administer the program more effectively.
  - › Objective 1: Enable data sharing without requiring extraction and loading of the data to a central location allowing each organization control and ownership of its own data.
- Goal 8: Put the best interest of the recipients first

- › Objective 1: Provide a recipient-centric focus of operations.

## SECTION 9 TRANSITION PLANS

### 9.1 OVERVIEW

The MES Project applies outcome-driven decision making to achieve the MES Strategic Priorities. The future state is a statewide Medicaid Enterprise optimized to use its people, technology and processes to deliver better health care for all Floridians. Some of the technology characteristics of the MES future state are:

- Cross-Agency use of high quality, real-time, “single source of the truth” information. Additional details on the single source of truth and master data management (MDM) are in Section 5 – Common Data Architecture in the T-1 Data Management Strategy.
- Reuse of business, technology and data services
- Seamless integration and interoperability between business, technology and data services
- A “single source of the truth” electronic policy including data edits, validations, transformations, and business rules
- Data analytic capabilities to identify and act on data driven insights
- Agile maintenance and change to business processing
- Data capture, validation and data-driven decision making at the point of recipient and provider interactions
- A consistent user interface and user experience especially for recipients, providers and Agency users that use multiple business or technical services
- A highly-available dynamic, scalable infrastructure and network that supports business and technology services
- Secure protection of business and technology assets
- Defense in depth protection of data and privacy for recipient and provider information

The MES Project is using a systematic, risk averse approach to execute the transition that will make the statewide Medicaid Enterprise vision a reality. The transition plan follows and builds upon Agency 2016 MES Procurement Approach that initially focuses on replacement of the FMMIS:

- Phase 1 - Contract with a SEAS and IV&V vendor to establish the vision, strategy, standards and implementation enablers for a MES modular implementation
- Phase 2 - Establish the MES Infrastructure to support
  - › Enterprise Integration (e.g. ESB)
  - › Enterprise Data Management (e.g. ODS/EDW)

- Phase 3 - Use the MES Infrastructure to implement MES Enterprise system integrations, data sharing and interoperability between Agency systems, and with other agency systems
- Phase 4 - Implement modular systems and services to improve processing currently performed within the MES enterprise

The MES Project is actively implementing Phase 1 and Phase 2 of the MES procurement strategy. The specific sequencing of Phase 3 Medicaid Enterprise Integrations and Phase 4 Module implementations is under evaluation to define specific MES integrations and MES Projects. The transition strategy is to leverage the technology enablers implemented in Phase 2 MES Infrastructure, as the specific capabilities are available. The specific sequencing of integrations and module implementations will consider the impact on the MES strategic priorities and the overall impact and improvement in health care for all Floridians. The sequencing will also consider whether the integrations should initially focus on only FMMIS, Agency Medicaid Systems, all Agency systems, or include considerations of other systems in other agencies. An additional consideration is the net value of other MES Projects. The scope for sequencing determination must be vetted through the MES S-4 Strategic Project Portfolio Management Plan (SPPMP).

While the SEAS Portfolio Management Process helps the program make prioritization decisions, the recommendation is for the transition approach to use an Agile, incremental “wade in” vs. a “big bang” or “jump in” approach. Preceding significant investment in MES Enterprise Integrations and modules, the MES Project will start small or pilot a small number of MES Enterprise Integrations and modules to industrialize the process. The first modules developed for the MES will establish and enable a formal module integration process to mature. The MES Data Management Strategy and MES Technical Management Strategy includes technology implementation recommendations for Phase 2 MES infrastructure that have significant complexity and organizational impact.

The recommended implementation of technology services that will enable the business are implementation and use of the:

- Integration Platform Technologies
- Operational Data Store
- Enterprise Data Warehouse, Data Marts, Business Intelligence and Analytic tools
- Centralized electronic policy (e.g. rules engine) source of the truth
- Data Validation Services and Data Validation Engines for Provider and Health Plan use
- Unified user interface technology, policy, and templates for module use

After the above enabling technology capabilities are established, the Agency will expand availability and access to these tools for integration of:

- FMMIS integrations (e.g. ODS / FMMIS data replication)

- AHCA IT Medicaid Systems Integrations (e.g. AHCA SunFocus, ASPEN)
- FMMIS modular system and services implementation (e.g. Provider, Recipient, Health Plan)
- AHCA IT Systems modular business capability replacement (e.g. Statewide Medicaid Managed Care Complaint Form (SMMC))
- Sister Agency Integrations (e.g. Department of Health (DOH) deaths and births)
- Sister Agency modular business capability replacements (e.g. eligibility determination, case management, appeals processing, common letter writer module)

A strategic priority of the MES TMS is a “do no harm” business disruption strategy, which recognizes the importance of maintaining business continuity across the enterprise. Components of the FMMIS system will remain operational while being incrementally replaced with MES modules. The Agency expects there could be some residual FMMIS functionality retained or refactored to operate in the MES.

## 9.2 KEY TRANSITION PRINCIPLES

**Incremental Delivery** – MES Projects will incrementally implement new modules, business, technology, and data services to supplement and replace the functionality of FMMIS modules and Non-FMMIS Medicaid applications to create the MES.

**Maximize Business Value** - Module functional scope will be determined on a case-by-case basis and guided by the MES Portfolio Management processes.

**Parallel Runtime** - New solutions and the legacy systems or applications being replaced must be able to run side by side to satisfy testing and validation requirements.

**Contingency Planning** - Transitions to new systems and applications which take over legacy systems and applications must have a plan to revert to the legacy applications, before implementation.

**New Modules Use of Integration Platform ESB and Data Services** - New modules communicate with other modules, systems and APIs via Web Services through the Integration Platform ESB. New modules access existing FMMIS web services via the Integration Platform connection to the FMMIS web services. Communications from modules to legacy systems are also via the Integration Platform ESB. If any legacy systems communicate with new modules, the legacy systems access a registered service wrapper in the ESB and use the messaging and Data Standards of the MES.

**New Modules use of Operational Data Store Data Services** – New modules access data via data services to the operational data store. Applications and individual users will not access databases directly or have native SQL access to databases.

**Minimal Business Disruption** – The existing systems and applications on which agency business units depend must remain operational until superseded by new systems and applications which satisfy their business requirements.

### 9.3 MES MODULAR STRATEGY

**Strategic Topic 9-1: MES Degree of Modularity** describes the direction on the degree of modularity for the MES as it evolves over time.

DEGREE OF MODULARITY	TIMELINE				
	Current	2018	2020	2022	2025
Monolithic Integrated Solution from a single vendor	FMMIS	->			
Multiple Vendor Applications	Enrollment Broker, TPL		MES		
Application Modules by Business Area Function	AHCA IT Medicaid		MES Acceptable		MES
Fine-grained Business and Technical Services			MES Acceptable		
Fine-grained Business and Technical Modular Services and APIs	AHCA IT		MES Preferred	->	
Data Services			ODS / RDS / Data Warehouse / Data Marts	->	
Micro Services					Reevaluate strategy and market adoption

#### ANALYSIS

The FMMIS current state of modularization can be described as an Integrated Solution by a single vendor which has an SOA architecture at the application level. Modularization occurs at a deep level within the application logic which is tightly coupled to the system. FMMIS also has external services that are consumed by other State and Private systems.

The strategy for the MES modularity future state is to have fine-grained modular services, data services and micro services exposed through standards-based API's. This approach aligns with the evolving CMS direction to thinking of modular implementation at a much more granular level.

A key feature of this approach is the flexibility in designing solutions which minimize disruptions to the business of the Agency. The Agency expects modularity to provide more strategic opportunities as FMMIS transitions to a modular MES system.

### Strategic Topic 9-1: MES Degree of Modularity

## 9.4 MES ENABLING TECHNOLOGIES

The MES foundational infrastructure includes five main enabling technologies: the Enterprise Service Bus (ESB) described in Section 3.3, Web Services, Service Oriented Architecture (SOA), Business Rules Engine (BRE), and the Operational Data Store (ODS).

### 9.4.1 WEB SERVICES

A web service is a reusable software service that interacts with other software components by exchanging standards-based messages. The following are web service standards:

- Remote Procedure Call (RPC)
- Simple Object Access Protocol (SOAP)
- Universal Description Discovery and Integration (UDDI)
- Web Services Description Language (WSDL)
- Extensible Markup Language (XML)

Representational State Transfer (REST) is a Web Services architectural style based on HTTP verbs. In section [3.1.3 Relationship to the World Wide Web and REST Architectures of the W3C Web Services Architecture](#), Web Services are separated in two major classes.

- REST-compliant Web services, in which the primary purpose of the service is to manipulate XML representations of Web resources using a uniform set of "stateless" operations; and
- Arbitrary Web services, such as Simple Object Access Protocol (SOAP), in which the service may expose an arbitrary set of operations.

It is worth noting that in current usage, REST-compliance does not rely on the message format and resources today are represented in various formats such as JavaScript Object Notation (JSON). Additionally, SOAP can be used in a manner consistent with REST.

MITA leverages industry-standard message enablers of the Application Programming Interface (API) and XML to create its own message formats for special Medicaid transmissions (e.g., Accredited Standards Committee (ASC) X12N Insurance Electronic Data Interchange (EDI) Standards). A set of standardized messages replace the individual point-to-point interfaces. All interface modifications are local to a single set of interfaces for consistent maintenance.

The MITA Framework standardizes the use of XML-based message interchange among business services and across organizational boundaries. XML messages are self-documenting, where each field in the message has a tag that defines the field (e.g., a field with the tag "Last\_Name" contains a person's last name). Consumers of a message look for and use fields required for their processing and may ignore optional or situational fields; therefore, if the stakeholder adds a new field (e.g., "Middle\_Initial"), there is no need to modify the consuming

service. This approach minimizes the effort to implement changes to Medicaid Enterprise systems.

### 9.4.2 SERVICE ORIENTED ARCHITECTURE (SOA)

SOA is a design principle that uses business functions and selected technical functions through documented interfaces. SOA is an architectural framework that integrates many different technologies. MITA requires the use of a modular, flexible approach to systems development. Modularity is breaking down systems requirements into component parts. Extremely complex systems can be developed as part of a SOA.

The ESB provides the key functions required for realizing a SOA:

- **Message Management** – This consists of reliable delivery of messages between services and built-in recovery.
- **Data Management** – This involves converting all messages between services to a common format and converting the common format to the application-specific format, within a service. To ensure interoperability, the message format uses XML standards. Stakeholders define information sharing and event notification standards to allow aggregated and integrated information.
- **Service Coordination** – This consists of orchestrating the execution of an end-to-end business process through all required services on the ESB. Services adapt to changes in environment and support a standards-based set of service management capabilities.

The system invokes each service in a standard way using one or more messages and each message results in the invocation of one of the documented functions supported by the service, regardless of deployment details.

In a SOA, systems invoke business functions as services with standard, message-driven interfaces. Systems can invoke services or reuse them in a platform-independent manner across the enterprise.

Existing applications are wrapped and invoked as service-provider systems. The linking between service consumers and service providers can happen at run time via a service registry. A new deployment or modification can replace an individual service without affecting the rest of the enterprise.

### 9.4.3 BUSINESS RULES ENGINES

Business rules engines are an effective way to make rapid changes to the logic of the system. A major benefit of rules engines is that logic is external to system application program code. MITA requires the separation of business rules from core programming, and the availability of business rules in both human and machine-readable formats.

The Agency's recommended strategy is to use a business rules engine implemented as part of ISIP to separate business rules from core programming and provide information about the change control process that will manage development and implementation of business rules. This strategy allows the Agency to accommodate changes to business rules on a regular schedule and on an emergency basis. Business rules that have cross state value may be submitted to a central federal repository per MITA.

A key recommendation of the MES Data Management Strategy is to establish a single source of policy truth including data edits, data transformations, and business rules. The MES TMS strategy is to use business rules engines to create policy services that provide the single source of policy truth that is reusable and decoupled from specific applications. This goal is a potential MES Project that may include:

- create inventory of all locations and system implementations of policy
- extract policy maintained in existing rules engines and custom code
- validate system implementations of policy
- migrate policy implementations to reusable services
- modify systems to use the services that contain policy implementation
- establish the organizational structure and resources that validates and tests the implementation of policy used by systems and services

The long-term strategy is that reusable policy services use an enterprise rules engine to decouple all system implementations of policy from proprietary applications. The strategy recognizes that some COTS products may use proprietary rules engines. If a COTS product is the definitive source of policy, the MES Program would provide guidance to expose the rules and policy as a reusable service that is accessible by other modules or systems via the ESB. If a COTS system requires internal use of business rules, the strategy would be for the COTS module to consume the business rules from the enterprise service for use in the COTS module internal service.

#### **9.4.4 NIEM ADOPTION**

The MES will align with forthcoming NIEM agreed-upon messaging formats. This involves planning for the day when there are NIEM messaging formats provided for the healthcare committee. There are initiatives under way to build human services and healthcare domains. Until they are complete, the primary interest is in the ability to use the NIEM Core domain elements for transaction messages with the federal institutions that have sufficient NIEM domains created. The MITA Technical Architecture expects the NIEM to provide data naming and structure addressing for custom transformation services on the edge of the State Medicaid Enterprise environment.

#### 9.4.5 CUSTOMER RELATIONSHIP MANAGEMENT

CRM is a strategy that uses technology to organize, automate, and synchronize business processes. Originally applied in the private sector to determine the needs of company clients, this concept extends to the Health Care Insurance Industry. As applied in the MITA Framework, this concept focuses on recipient and provider access to Electronic Health Record (EHR) data and individual access to health insurance alternatives. Some areas that require CRM include:

- EHR
  - › An electronic record of health-related information on an individual that conforms to nationally recognized interoperability standards, and that authorized clinicians and staff across more than one healthcare organization can create, manage, and consult.
- Health Information Exchange (HIE)
  - › The electronic movement of health-related information among organizations according to nationally recognized standards.

#### 9.4.6 OPERATIONAL DATA STORE (ODS)

The Operational Data Store establishes a single source of truth for transactional data. Data in the ODS is independent of a specific application or system. For this reason, after migration to the ODS, the Agency can replace a module from one vendor with modules from another vendor. Applications access data in the ODS using data services or API calls as opposed to passing SQL language directly to a proprietary database. Primary information on the ODS is in the MES Data Management Strategy Deliverable and **Strategic Topic 9-1: MES Degree of Modularity** .

#### 9.4.7 ENTERPRISE ARCHITECTURE

Enterprise architecture will be elaborated in a future iteration of this deliverable corresponding to the ISIP procurement.

## SECTION 10 STATE SPECIFIC MITA ADDITIONS

The MES has considered the following additions of new functionality and will be watching for advancements of technological capabilities to leverage in the future. While these additions are not integrated into the current timeline, the MES TMS recommendation is that they be explored as possible additions to the MES future state as mature, industry-specific offerings appear in the vendor landscape.

### 10.1 COGNITIVE SERVICES

Cognitive Services is an emerging area which delivers cognitive computing technologies based on artificial intelligence and signal processing. Cognitive Services includes two rapidly evolving technologies: machine learning and natural language processing.



**Exhibit 10-1: Cognitive Services Use Cases.**

#### 10.1.1 MACHINE LEARNING

As the Agency's upgrades to a modular infrastructure and some systems move toward cloud, the application of machine learning technologies becomes increasingly relevant and accessible. Major cloud service providers (CSP) have accessible machine learning offerings as a service. The Agency could use these solutions to maximize fraud prevention, improve recipient care by detecting important patterns in recipient data, or offer an Artificial Intelligence (AI) chatbot that improves customer service.

**Real-time Improper Payment Detection and Prevention** – Bad actors constantly increase the sophistication and speed at which they perpetrate fraud. Increasingly their techniques are tactical and focused on quick gains and result in lower risk of detection and reduced opportunities for the recovery of losses. Applying machine learning to the examination of MES information (e.g. new claims and provider enrollment applications) could allow proactive identification and prevention. The enabling technologies learn to identify new techniques or new patterns in real time as they emerge to help to avoid the improper payments or improve the coordination of care.

**Predictive Recipient Outcomes** – Datasets including recipient demographics, diagnosis, admissions, procedures, vitals taken at doctor visits, history of medications, and lab results could be created using anonymized recipient data. Machine learning could be applied to predict which recipients are more at risk for being hospitalized, develop substance dependencies, or are at risk of having a heart attack. Once identified, these recipients could be candidates for health interventions via education, treatment, or services which could prevent the adverse outcome.

### 10.1.2 AI BOTS

**Customer Service AI Chatbots** - AI chatbots make use of Cognitive Computing technologies like Natural Language Processing, and Machine Learning to interpret user requests and mimic human conversation to respond to those requests. Chatbots could be deployed to tackle routine questions about providers, benefits, or enrollment. More complex chatbots could be deployed to answer questions like provider requests for recipient eligibility, that helps to remediate a claim or encounter, or directs recipients to care options.