AHCA Florida Health Care Connections (FX)

P-4: Medicaid Enterprise Certification Management Plan

Version: 500

Date: March 14, 2023

Author: The SEAS Vendor

Submitted To: FX Program Administration Team

Revision History

DATE	VERSION	DESCRIPTION	AUTHOR
3/28/2018	001	Development Draft Version	Vivian de la Gandara /Ellen Emenheiser/Fred Knapp
5/2/2018	002	P-4: Medicaid Enterprise Certification Management Plan Development Draft Version	Vivian de la Gandara/Ellen Emenheiser
5/15/2018	003	P-4: Medicaid Enterprise Certification Management Plan Development Draft Version	Vivian de la Gandara/ Ellen Emenheiser
5/16/2018	100	P-4: Medicaid Enterprise Certification Management Plan Development Final Version	Sean Gibbs
8/8/2018	101	P-4: Medicaid Enterprise Certification Management Plan revisions to address review highlighting and bullet/section header issues	Sean Gibbs
4/26/2019	101	P-4: Medicaid Enterprise Certification Management Plan Development – Annual Refresh Version – Draft 1	Fred Knapp
5/11/2019	101	P-4: Medicaid Enterprise Certification Management Plan Development – Annual Refresh Version – Draft 2	Fred Knapp
5/15/2019	200	P-4: Medicaid Enterprise Certification Management Plan Development – Annual Refresh Version – Final	Fred Knapp
3/23/2020	201	P-4: Medicaid Enterprise Certification Management Plan Development – Annual Refresh	Fred Knapp
5/1/2020	201	P-4: Medicaid Enterprise Certification Management Plan Development – Annual Refresh – Draft 2	Fred Knapp
5/4/2020	300	P-4: Medicaid Enterprise Certification Management Plan Development – Annual Refresh Version – Final	Fred Knapp
12/6/2021	301	P-4: Medicaid Enterprise Certification Management Plan – draft rewrite	Fred Knapp
1/10/2022	302	P-4: Medicaid Enterprise Certification Management Plan – remediate addressing reviewer comments	Fred Knapp
1/14/2022	400	P-4: Medicaid Enterprise Certification Management Plan – Approved Final	Carol Williams
12/28/2022	401	P-4: Medicaid Enterprise Certification Management Plan updated in accordance with DET #571 and to bring this deliverable current	Fred Knapp

DATE	VERSION	DESCRIPTION	AUTHOR
2/10/2023	402	P-4: Medicaid Enterprise Certification Management Plan updated in accordance with DET #571 – remediate addressing reviewer's comments	Fred Knapp
3/14/2023	500	P-4: Medicaid Enterprise Certification Management Plan – Approved Final	Fred Knapp

Modifications to the approved baseline version (100) of this artifact must be made in accordance with the FX Artifact Management Standards.

Quality Review History

DATE	REVIEWER	COMMENTS
3/29/2018	Sean Gibbs	QA Review for submission
3/30/2018	Fred Knapp	QA Programmatic Review
5/3/2018	Robert Flasch	QA Programmatic Review
5/4/2018	Sean Gibbs	QA Review for Submission
5/15/2018	Fred Knapp	QA Programmatic Review
5/15/2018	Sean Gibbs	QA Review for Submission
4/24/2019	Mary Lindsay Ryan	QA Review for Submission
7/26/2019	Carol Williams	QA Review for Submission
4/9/2020	Eric Steinkuehler	QA Review for Submission
11/29/2021	Carol Williams	Conducted QC review
10/25/2022	Austin Williams, Alan Ashurst, Michael Stephens	Peer Review
12/27/2022	Carol Williams	Conducted quality review

Table of Contents

Table of Exhibits

SECTION 1 INTRODUCTION

1.1 BACKGROUND

The Florida Agency for Health Care Administration (AHCA or Agency) is adapting to the changing landscape of healthcare 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 is complex; it includes services, business processes, data management and processes, technical processes within the Agency, and interconnections and touchpoints with systems necessary for administration of the Florida Medicaid program that reside outside the Agency. The future of the Florida Medicaid Enterprise integration is to allow the Agency to secure services that can interoperate and communicate without relying on a common platform or technology.

The Florida Medicaid Management Information System (FMMIS) has historically been the central system within the Florida Medicaid Enterprise; functioning as the single, integrated system for claims processing and information retrieval. As the Medicaid program has grown more complex, the systems needed to support the Florida Medicaid Enterprise have grown in number and complexity.

The Medicaid Enterprise System (MES) Procurement Project was re-named Florida Health Care Connections (FX) in the summer of 2018. FX is a multi-year transformation to modernize the current Medicaid technology using a modular approach, while simultaneously improving overall Agency functionality and building better connections to other data sources and programs.

1.2 PURPOSE

The purpose of the Medicaid Enterprise Certification (MEC) Management Plan is to provide an overall plan to manage the Planning, Development, and Production phases throughout the MES Certification life cycle for each applicable FX module along with recommendations to consider as the Agency moves forward with the modular approach to replacing the current Medicaid Management Information System (MMIS). The Plan will outline the steps for the Agency to conduct and comply with the MES Certification process, including gathering documentation and managing readiness reviews. CMS guidance around MITA and module certification has evolved much in the last few years and this document is updated regularly to support Florida in applying this guidance accurately and in a way that drives value for the Agency and Floridians

1.3 SCOPE STATEMENT

The MES Certification process is the prescribed validation process from CMS for states to request and obtain enhanced Federal Financial Participation (FFP) to develop, implement, operate, and maintain their MES.

The MEC Management Plan outlines the steps to take for the Agency to comply with the federal certification requirements as it undertakes the replacement of its current MMIS and expands its IT capabilities to include an enterprise-wide approach to meet the needs of the Medicaid program and the various stakeholders that interact with Medicaid.

The MEC Management Plan contains the following sections:

Section 2 – Regulations and Guidance – Provides an overview of the federal MMIS Certification requirements, including: a brief history of the MMIS Certification process; the importance of certification in obtaining and maintaining enhanced FFP for managing the Medicaid program; and descriptions of the guidance documents provided by CMS.

Section 3 – Florida FX Certification Organization Roles and Responsibilities – Lists the responsibilities of stakeholders during the certification process and includes a process to inform and train impacted staff. Stakeholders include CMS, Florida Legislature and the Office of Policy and Budget (OPB) in the Office of the Governor, FX Executive Steering Committee and Agency Governance, Department of Management Services (DMS), AHCA FX Program Administration Team, Independent Verification and Validation (IV&V) Vendor, Strategic Enterprise Advisory Services (SEAS) Vendor, Integration Services and Integration Platform (IS/IP) Vendor, Enterprise Data Warehouse (EDW) Vendor, and other FX solution vendors.

Section 4 – Florida FX Medicaid Enterprise Streamlined Modular Certification (SMC) – Explains the MES Certification timeline with the two milestone reviews and shows how they fit within the four phases of the Agency's FX procurement timeline. This section also explains the process and steps that end with the final Certification Review (CR).

Section 5 – Required Project Artifacts and Reporting – Describes the tracking and reporting activities to manage the certification activities.

Section 6 – Updates and Impact Analysis – Provides a brief description of monitoring the changes to federal publications and updating the process documents to be compliant with new regulations.

1.4 GOALS AND OBJECTIVES

The Agency's MES Certification expectations for all stakeholders with the FX Program are outlined in the MEC Management Plan. The Agency's top goals and objectives of MES Certification for each FX Project include:

Goal #1 – To comply with federal requirements for seeking and receiving approval from CMS for the release of 90/10 FFP to aid Florida in the cost of Design, Development, and Implementation (DDI) for each FX module or function that is developed to replace the current MMIS solution.

Goal #2 – To comply with federal requirements for seeking 75/25 FFP to aid Florida in the cost of Operations and Maintenance (O&M) for each FX module or function that replaces the current MMIS solution and is operationalized.

Goal #3 – To receive full Certification authorization from CMS back to day one of operations for each FX module that has been implemented and operating for at least six months.

Goal #4 – To ensure that the State of Florida's current 75/25 FFP rate for O&M is safeguarded from additional unplanned costs associated with the failure to achieve Certification back to day one of operations for any FX module or functionality that is operationalized.

1.5 REFERENCED DOCUMENTS

The MEC Management Plan will be reviewed whenever an updated version or guidance on certification is released. Gaps between the previous version and the current version of the MEC Management Plan will be identified and updated accordingly to ensure the Agency and its vendors are adhering to the most current certification requirements.

The following documents were leveraged to support the development of this deliverable and the related MES Certification activities:

- Florida FX Procurement Strategy
- Florida Implementation Advanced Planning Document Update (IAPDU) MES Strategy and Strategic Enterprise Advisory Services (SEAS) Procurement
- Request for Information (RFI) SEAS
- State Medicaid Manual (SMM)
- State Medicaid Director Letters (SMDL)
- S-3: FX Strategic Plan
- CMS Streamlining Certification for Medicaid Enterprise Systems Guidance, Version 1, March 2021
- CMS Streamlining Modular Certification: "It's not a checklist – it's a conversation" slide deck, 2021
- CMS Certification Repository on Github.com
- CMS Certification Community of Practice (CoP) Certification Repository, October 12, 2021, slide deck
- CMS MES Advanced Planning Document (APD) CoP, February 3, 2021, slide deck
- CMS MES CoP, December 8, 2020, slide
- CMS MES Certification Community of Practice (CoP) Streamlined Modular Certification (SMC) for Medicaid Enterprise, May 18, 2022

- CMS State Medicaid Directors (SMD) Letter # 22-001 RE: Updated Medicaid Information Technology Systems Guidance: Streamlined Modular Certification for Medicaid Enterprise Systems, April 14, 2022
- CMS Streamlined Modular Certification for Medicaid Enterprise Systems Certification Guidance, Version 1, April 2022
- CMS Medicaid Enterprise Systems Testing Guidance Framework, April 2022
- Streamlined Modular Certification Intake Form
- Operational Report Workbook
- CMS-1: Unpacking the New Guidance: Streamlined Modular Certification, August 18, 2022, slide deck
- Medicaid Enterprise Systems (MES) Data Submissions and Intake Process Procedures Manual, September 1, 2022
- CMS Certification Repository Streamlined Modular Certification Frequently Asked Questions (FAQs)
- AHCA RFQ 015-21/22 FX Independent Verification and Validation (IV&V) Services

SECTION 2 REGULATIONS AND GUIDANCE

This section provides a summary of relevant federal MES Certification regulations and guidance including the history and importance of Certification. It explains how the SMM provides guidance to the states regarding MES Certification.

2.1 CERTIFICATION

Certification is a federal validation process where CMS reviews a state's new MMIS module or cohort of modules prior to granting 75/25 FFP for O&M of the system after implementation. A module is a packaged, functional business process or set of processes implemented through software, data, and interoperable interfaces that are enabled through design principles in which functions of a complex system are partitioned into discrete, scalable, reusable components. A MMIS module is a discrete piece (component) of software that can be used to implement a MMIS business area.

Objectives of the certification validation process for Florida will include:

- Verifying that each MES module procured is designed and implemented effectively and efficiently supporting management of the Florida Medicaid program
- Confirming that specific laws, regulations, and directives are met in the solution
- Ensuring that the new MES module is operating as described in the Advanced Planning Documents (APDs), Procurement Document Requirements, and Module Solution vendor's statement of work, and other related contracts
- Demonstrating that the desired measurable improvements and outcomes are being achieved

CMS defines the mechanized claims processing and information retrieval system, which states are required to have, as the MMIS.

CMS defines the MMIS as an integrated group of procedures and computer processing operations (modules) developed at the general design level to meet principal Title XIX Program objectives, including:

- Managing and controlling administrative costs
- Providing service to members and providers, including inquiries
- Managing claims control operations and computer capabilities
- Generating management reporting for planning and control

States are required to have a MMIS according to Section 1903(a)(3) of the Social Security Act and defined in regulation 42 CFR 433.111.

All states operate a MMIS to support Medicaid business functions and maintain information in such areas as provider enrollment; client eligibility, including third party liability; benefit package maintenance; managed care enrollment; claims and encounter processing; and prior authorization.

2.2 Importance of Certification

One of the most important tasks for the FX Project Team will be to ensure the new FX modules are all certified back to day one of operation. The ramifications of not passing Certification include:

- Not receiving enhanced federal matching funds to offset the cost of O&M for the solution
- Significant impact to the State of Florida budget, as this funding is typically planned for in the state Medicaid budget with Medicaid funding being one of the largest items in the state budget

2.3 Outcomes-Based Certification

CMS transitioned its systems certification process to one that evaluates how well Medicaid information technology systems support desired business outcomes, while reducing the burden on states. This streamlined, outcomes-based approach, or Outcomes-Based Certification (OBC), is designed to ensure that systems that receive FFP are meeting the business needs of the state and of CMS.

CMS piloted OBC through a combination of developing outcomes statements and evaluation criteria, identifying test cases for system demonstrations, and collecting and assessing operational data. CMS engaged states in OBC through pilots and release guidance as new OBC processes were refined.

OBC focuses on achieving business outcomes and is intended to reduce the certification burden on states. In doing so, CMS aims to ensure that systems receiving FFP are meeting the business needs of states and of CMS.

Electronic Visit Verification was the first system to which CMS applied an outcomes-based approach to certification

2.3.1 Streamlined Modular Certification

CMS issued State Medicaid Director Letter (SMD) 22-001 Updated Medicaid Information Technology Systems Guidance: Streamlined Modular Certification for Medicaid Enterprise Systems on April 14, 2022. This SMD provides updated guidance to further guide the transition to OBC through a process called Streamlined Modular Certification (SMC) under which certification is structured around the following three elements, rather than the older burdensome certification checklists.

- **Conditions for Enhanced Funding** – As a condition of receiving enhanced federal matching funds for state expenditures on MES, states must ensure that the system complies with all of the conditions for enhanced funding (CEF) as provided in 42 C.F.R. §433.112 and that the system remains compliant with federal Medicaid requirements for enhanced operations matching once it is in operation as provided in 42 C.F.R. §433.116.
- **Outcomes** – Outcomes describe the measurable improvements to a state's Medicaid program that should result from the delivery of a new module or enhancement to an existing system. Outcomes supporting Medicaid program priorities are directly enabled by the state's IT project and stated in the Advance Planning Document (APD). CMS is encouraging states to develop measurable, achievable outcomes that reflect the MES project's short-term goals.
    - **CMS-required outcomes** are based on statutory or regulatory requirements and provide a baseline for what is required of an MES, including the efficient, economical, and effective administration of the state's Medicaid program. CMS required outcomes are associated with the specific module(s) the project is trying to put in place or improve.
    - **State-specific outcomes** reflect the unique circumstances or characteristics of the state and its Medicaid program and focus on improvements to the program not specifically addressed by the CMS-required outcomes.
- **Metrics** – Provide evidence that the outcomes are met on an ongoing basis. In accordance with 42 C.F.R. §433.112(b)(15) and §433.116(b), (c), and (i), states must be capable of producing data, reports, and performance information from and about their MES modules to facilitate evaluation, continuous improvement in business operations, and transparency and accountability, as a condition for receiving enhanced federal matching for MES expenditures. Metrics reporting enhances transparency and accountability of IT solutions to help ensure the MES and its modules are meeting statutory and regulatory requirements as well as the state's program goals. State reporting also gives states and CMS early and ongoing insight into program evaluation and opportunities for continuous improvement.

For all systems that comprise the MES, the Streamlined Modular Certification approach is designed to:

- Demonstrate measurable improvements to a state's Medicaid program resulting from the delivery of a new module or enhancement to an existing system.
- Leverage data and testing to inform an assessment of the successful delivery of systems and inform subsequent funding decisions.
- Enable operational reporting for system performance and functionality to ensure ongoing oversight of data and evidence that demonstrates the continuous achievement of required and desired outcomes.
- Reduce burden on states and CMS during the certification process without compromising CMS' responsibility to ensure those systems satisfy all statutory and regulatory requirements.

- Advance incrementally toward a fully realized OBC process for the entirety of MES.

An important principle of Streamlined Modular Certification is to reduce burden on states and CMS during the certification process without compromising CMS' responsibility to ensure those systems satisfy all statutory and regulatory requirements.

CMS is providing SMC guidance to states as it is developed and will continue to provide guidance as SMC matures. Current CMS guidance is found in the following documents which are included in this plan.

- Appendix A – Conditions for Enhanced Funding
- Appendix B – CMS-Required Outcomes
- Appendix C – Required Artifacts List
- Appendix D – Framework for the Independent Third-Party Security and Privacy Assessment Guidelines for Medicaid Enterprise Systems
- Appendix E – Streamlined Modular Certification Intake Form
- Appendix F – CMS Medicaid Enterprise Systems Testing Guidance Framework, April 2022
- Appendix G – Operational Report Workbook
- Appendix H – Medicaid Enterprise Systems (MES) Data Submissions and Intake Process Procedures Manual, September 1, 2022

2.4 STATE MEDICAID MANUAL (SMM)

CMS created and published the SMM to help states implement the requirements in Title XIX, including requirements of the MMIS and other aspects of the Medicaid Program. It is both a tool for states and an official notification medium for CMS as noted below.

- As a tool, the SMM references informational and procedural material that is used by the states to help administer their Medicaid programs
- As an Official Notification Medium, CMS uses the SMM to issue mandatory, advisory, and optional Medicaid related policies and procedures to the State Medicaid Agencies (SMAs)

The remainder of this section provides additional requirements in the SMM for MMIS contracts.

2.4.1 CHAPTER 2-STATE ORGANIZATION AND GENERAL ADMINISTRATION

Chapter 2 of the SMM outlines requirements that states must comply with to manage Title XIX. This chapter defines the state organization and summarizes its responsibilities and general requirements for the administration of the program. There are specific requirements that state organizations must adhere to that are outlined in this chapter such as guidelines for contracting and subcontracting, stipulations for obtaining different types of FFP that are available to states,

federal reporting requirements, program and policy related information including how to request and maintain waivers, responsibilities for collecting overpayments and conducting fair hearings and appeals to name a few.

2.4.2 CHAPTER 11-MEDICAID MANAGEMENT INFORMATION SYSTEM (MMIS)

Chapter 11 of the SMM defines the MMIS and outlines system requirements that must be met to obtain FFP for the DDI of an MMIS. This chapter provides states with guidance on how and when to complete the APDs that must be submitted and approved by CMS to receive the FFP in addition to describing the system review process that states must undergo to receive enhanced FFP for O&M of the MMIS after it is implemented.

2.5 STATE MEDICAID DIRECTOR LETTER #16-010

SMD Letter#16-10 RE: CMS-2392-F MECHANIZED CLAIMS PROCESSING AND INFORMATION RETRIEVAL SYSTEMS – MODULARITY provides sub-regulatory guidance in the form of letters to State Medicaid Directors. This was the third letter in the series that addressed modular certification of Medicaid Management Information Systems (MMIS). Guidance included in this letter includes:

- States are encouraged to use a modular approach for replacing portions of a MMIS and discouraged from replacing an entire MMIS
- Modular certification will be applied to MMIS systems as new modules are introduced and existing modules are replaced
- Description of the system integrator role focusing on ensuring:
  - Integrity and interoperability of the Medicaid IT architecture
  - Cohesiveness of the various modules included in the Medicaid Enterprise
- Role of the IV&V Vendor
- MITA 3.0 compliance

2.6 STATE MEDICAID DIRECTOR LETTER #18-005

SMD #18-005 RE: CMS-2392-F MECHANIZED CLAIMS PROCESSING AND INFORMATION RETRIEVAL SYSTEMS – REUSE. This letter was to provide sub-regulatory guidance to supplement CMS-2392-F, *Mechanized Claims Processing, and Information Retrieval Systems (90/10),* which became effective January 1, 2016. This was the fourth letter in the series and that letter reaffirms the requirement for reuse in 42 CFR Part 433, Subpart C - Mechanized Claims Processing and Information Retrieval Systems. Guidance in this letter included enhanced funding requirements for reuse including:

- Expectations for states receiving FFP to share project artifacts, documents, and other related materials along with system components and code to other states for leverage and reuse

- How states can meet requirements for reuse by selecting solutions that maximize reuse opportunities
- Expectations for states to participate in work groups such as the MMIS Cohort, State Technical Advisory Group (S-TAG) and other work groups to facilitate knowledge sharing
- CMS is supplying additional assistance or guidance in order to ensure states are following reuse requirements through the following:
    - Web Resources and a repository are being provided so that states can share and reuse
    - State Cohort meetings are sponsored by CMS to help support reuse
    - APDs will be required to include reuse plans and CMS will help states identify opportunities
    - Cooperative Purchasing within the state or with other states
    - Acquisition Reviews will be reviewed to ensure they are consistent with the APD reuse plans
    - Design Guidance that should include how the solution can lend itself to reuse
    - Documentation Guidance to support operation of the solution by the state or another contractor
- Design Alternatives
- State Innovations in reuse

SECTION 3 FLORIDA FX CERTIFICATION ORGANIZATION ROLES AND RESPONSIBILITIES

CMS has an established set of roles and responsibilities for the certification process. According to 45 CFR § 95.626 (b) and (c) states are required to have an IV&V Vendor who is independent from the state unless the state receives a waiver after submitting an alternative approach. The Agency requested and received a waiver to manage its IV&V Vendor until the end of the first term, with the caveat that the Agency does not have the authority to preview or change IV&V reports. The IV&V Vendor submits reports to the CMS State Officer Team (SOT), Florida Legislature, OPB, FX Executive Steering Committee (ESC), and DMS, who provides project oversight while the Agency manages the IV&V Vendor, at the same time as the Agency. The Agency provides monthly reports to the CMS SOT, Florida Legislature, OPB, and Agency Management.

3.1 FX ORGANIZATION

Exhibit 3-1: FX below shows Florida's FX Governance Structure for the certification process. The governance structure provides executive-level oversight and recommendations for decision-making, including those related to certification.

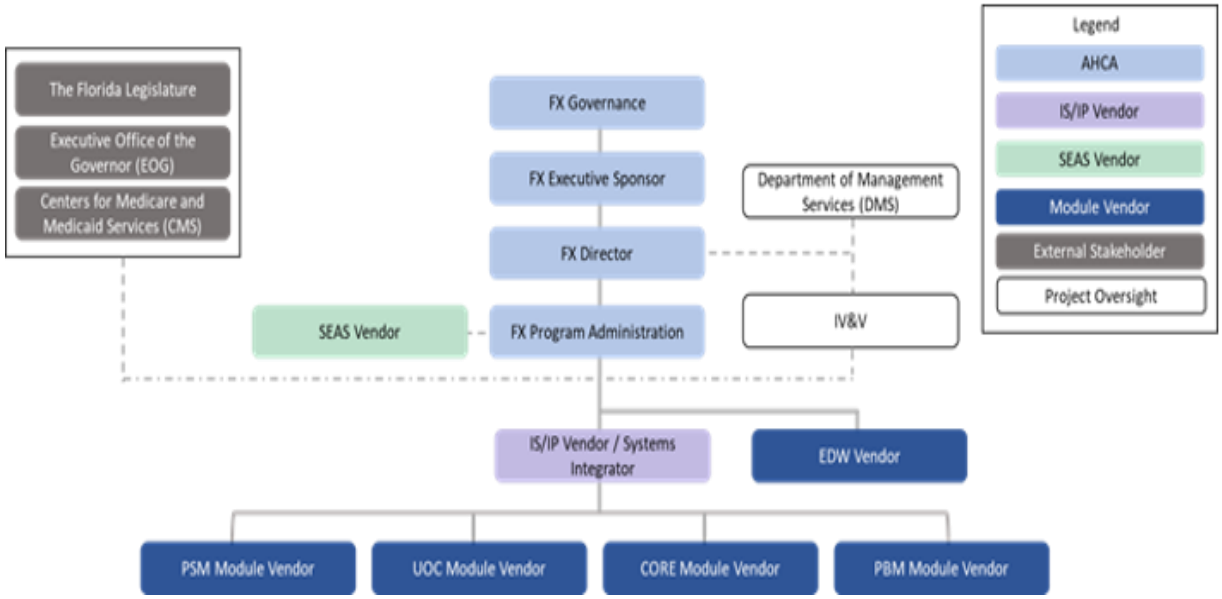

Exhibit 3-1: FX Organization

3.2 ROLES AND RESPONSIBILITIES

The SMC outlines certain roles and responsibilities for CMS, the state, and the IV&V Vendor (at the state's discretion) over the course of certification. In addition, the Agency developed a Standard Operating Procedure for Certification with assigned roles for the certification process

that has been incorporated in the MEC Management Plan. **Exhibit 3-2: Roles and Responsibilities** below describes the roles and responsibilities of the Agency, CMS, and its partners for pursuing MES Certification for various Florida FX modules.

ROLE	RESPONSIBILITY
CMS Central Office (CMS CO)	▪ Provides overall supervision for Certification and the SMC ▪ Attends Operational Readiness and Certification reviews ▪ Reviews and approves the IAPD ▪ Issues modules Certification Review Decision Letter
CMS Certification Review (CR) Team	▪ Conducts Operational Readiness (ORR) and CR reviews ▪ Reviews evidence to support outcomes and metrics ▪ Reviews Intake Form and required artifacts ▪ Makes recommendations to the CMS CO for decision-making
CMS Medicaid Enterprise State Officer Team (CMS SOT)	▪ Coordinates all certification activities with the CMS CO ▪ Serves as a resource and consults with the state on SMC ▪ Reviews and recommends IAPD for approval ▪ Participates in the ORR and CR reviews
Florida State Legislature/Office of Policy and Budget (OPB in the Governor's office)	▪ Provides project oversight and state funding authority
Department of Management Services (DMS)	▪ Provides project oversight including IV&V
FX Governance (Including ESC)	▪ Provides executive-level oversight
Agency Secretary	▪ Provides executive decision-making

ROLE	RESPONSIBILITY
Agency	▪ Plans and manages the FX Program including certification ▪ Designates a FX Certification Manager and Coordinator responsible for coordinating with all vendor certification counterparts on all activities related to certification plans, processes, and tools; certification reviews, and enterprise certification management across multiple projects ▪ Designates a Project Lead responsible for coordinating with all vendor certification counterparts on all project activities related to requirements and certification documentation ▪ Designates a Business Lead and subject matter expert (SME) for each project who is responsible for ensuring the assigned FX solution vendor meets project requirements. For certification, the Business Lead and SME are responsible for reviewing the FX solution vendors' certification artifacts ▪ Tracks and manages to resolution certification issues identified by the CMS, the MITRE Corporation (MITRE), and the IV&V Vendor ▪ Reviews and approves updates suggested by the SEAS Vendor for inclusion in the MEC Management Plan ▪ Informs and trains Agency leadership and impacted staff on certification tasks, roles, materials, and timeframes ▪ Complete assigned activities outlined in the MEC Management Plan ▪ Procures IV&V Vendor services for FX projects ▪ Develops APD documents and submits to the CMS ▪ Develops outcomes, metrics, and evidence in coordination with project teams and certification SMEs ▪ Plans Certification readiness reviews in coordination with the CMS Region IV Office ▪ Completes and submits monthly project status reports to the CMS ▪ Submits the Intake Form and required artifacts requesting an Operational Readiness Review and final Certification from the CMS ▪ Approves any ongoing changes to the MEC Management Plan
IV&V Vendor	▪ Assigns a dedicated certification resource with strong certification knowledge that is responsible for coordinating with the SEAS Vendor and FX solution vendors certification counterparts and all activities related to certification including understanding the MEC Management Plan ▪ Represents the CMS' interest by providing an independent and unbiased perspective on the progress of MES development including the integrity and functionality of the system ▪ Provides the Agency with a perspective and understanding related to the federal requirements certification, and enhanced federal funding match ▪ Evaluates and makes recommendations for the federal and state business outcomes and the Conditions for Enhanced Funding ▪ Assists with planning and development of metrics to demonstrate the success of each FX module in meeting the Agency's business outcomes ▪ Verifies and validates artifacts, Intake Forms, and reports required for the federal certification milestone for each FX module ▪ Assists with producing monthly and quarterly MES certification progress reports ▪ Participates in MES Certification Milestone Reviews including the Operational Readiness Review and the Certification Review

ROLE	RESPONSIBILITY
SEAS Vendor	▪ Assigns a Certification Lead Resource/SME responsible for coordinating contributions with the Agency, IV&V Vendor, and FX solution vendors certification counterparts on all activities related to certification including understanding the MEC Management Plan ▪ Assign certification roles and responsibilities to other SMEs/resources for each certifiable component as necessary ▪ Develops and documents the MEC Certification Management Plan ▪ Analyzes any subsequent updated documentation for new versions and guidance letters released by the CMS related to certification ▪ Reviews and provides input for APD development ▪ Provide SME participation for outcomes development, metric identification, and validation sessions, as needed ▪ Assist in reporting on the status of Certification at enterprise governance meetings for each FX Project ▪ Adheres to the MEC Management Plan ▪ Provide SME input and review on Enterprise Certification Management activities and the Jira Standards Work Group ▪ Assist the Agency led development of a framework for Source Pulse, which will serve as a certification and MITA repository ▪ Advise Agency Certification Lead on CMS certification requirements and best practices ▪ Provide quality control metric reporting after ORR ▪ Provide certification SME participation for Joint Application Design (JAD) sessions ▪ Provide input and review the FX Program Administration (FXPA) led development of a standards document/checklist for certification activities that will be added as an appendix to this *P-4: FX Medicaid Enterprise Certification Management Plan* ▪ Assist with program alignment of certification activities for all FX modules, including certification support between module vendors and supporting certification alignment with outcomes management and benefits realization against the overall FX strategy ▪ Review and provide feedback on select or prioritized draft certification artifacts for submission to CMS, with feedback focusing on the overall template, and the quality and completeness of the content types based on the CMS certification requirements ▪ Review and provide advice on feedback received from CMS on certification artifacts and planned activities (e.g., the ORR) ▪ Review and provide recommendations on certification planning activities to achieve schedule milestones ▪ Assist the Agency, identify and align Agency business processes, relevant MITA business processes, and certification outcomes to the FX Outcomes Management Framework ▪ Provide advice as needed for Agency benefits realization owners to leverage the FX Outcomes Management Framework, measurement, and benefits realization plan ▪ Assist the Agency in developing metrics needed to track outcomes achievement, for any new outcomes identified by the Agency, which are not already part of certification

ROLE	RESPONSIBILITY
IS/IP Vendor	▪ Provides applicable documentation of requirements as included in the certification process for each applicable MES project ▪ Provides a Certification Lead responsible for coordinating with the SEAS Vendor and IV&V Vendor certification counterparts on all activities related to certification including understanding the MEC Management Plan ▪ Supports the SMC process for all components that are certified ▪ Works with the Agency's IV&V Vendor to ensure that the IV&V Vendor has full access to project artifacts ▪ Participates and provides support as needed to the FX solution vendors for certification activities including participating in planning activities, meetings, and other activities as required by the CMS ▪ Assists the Agency in preparing certification artifacts, evidence, and presentation materials ▪ Provides all the required remediation activities, based on the certification findings after each readiness review, on a schedule to be approved by the CMS and the Agency ▪ Updates the documentation as necessary to support the certification process and to reflect changes that have been made to the solution during the certification process ▪ Adheres to the MEC Management Plan
FX Solution Vendors	▪ Provides applicable documentation of requirements as included in the certification process for each applicable FX Project ▪ Provides a Certification Lead who will coordinate with the Agency, SEAS Vendor, IV&V Vendor, and other FX solution vendor certification counterparts on all activities related to certification including understanding the MEC Management Plan ▪ Supports the SMC process for all components that are certified, as described in the current version of the SMC ▪ Works with the Agency's IV&V Vendor to ensure that the IV&V Vendor has full access to project artifacts ▪ Participates and provides support as needed to other FX solution vendors for module certification activities including participating in planning activities, meetings, and other activities as required by the CMS ▪ Identifies, produces, and tracks required artifacts and evidence for federal certification milestones for each FX module ▪ Prepares certification Intake Forms and reports ▪ Produces certification presentation materials ▪ Provides all the required remediation activities, based on the certification findings after each readiness review, on a schedule to be approved by the CMS and the Agency ▪ Updates the documentation as necessary to support the certification process and to reflect changes that have been made to the solution during the certification process ▪ Adheres to MEC Management Plan

Exhibit 3-2: Roles and Responsibilities

3.3 CERTIFICATION LEAD RESOURCES

It is critical that all parties (Agency, SEAS Vendor, IV&V Vendor, IS/IP Vendor, and FX solution vendors) designate a Certification Lead resource to be responsible for certification activities. The certification resource is expected to work collaboratively with their counterparts and serve

as the point of contact for certification for their respective organizations. The duties of the various dedicated certification resources will vary based on the entity for whom they work, however, the Certification Lead resources should have a working knowledge of the following:

- CMS SMC Guidance including CMS Testing Guidance Framework
- Federal Requirements for Planning Documents
- Outcomes, Metrics, and Conditions for Enhanced Funding (CEF)
- MITA
- Requirements Traceability Matrix (RTM)
- Configuration Design
- Data integration and Interface
- Data Conversion
- Systems Integration Testing (SIT) and User Acceptance Testing (UAT)
- Training and Communication Plans
- Deployment Plan
- Security Plan
- Disaster Recovery Plan
- Business Continuity
- Operations and Maintenance Plan

The Certification Lead resource for FX solution vendors will be expected to produce, gather, and deliver evidence documentation in specified formats, which the Agency Project Manager and Business Lead will review and approve. The IV&V Vendor certification resource will be responsible for evaluating whether the evidence supplied meets the certification criteria identified in the CMS SMC Certification Guidance and the Intake Form for the module that the Agency is seeking to certify.

Select deliverables required by vendors are also artifacts that must be provided in advance to the CMS and will be used as evidence for certification once approved by the Agency. All certification artifacts are stored in the Certification Repository within the Agency's FX Projects Repository (FXPR) to ensure access by all certification staff and are uploaded to the CMS Box Repository for CMS Certification reviewers when appropriate. See Appendix C – *Required Artifacts List* of this plan for specific details and minimum requirements for an ORR and CR.

SECTION 4 FLORIDA FX MEDICAID ENTERPRISE STREAMLINED MODULAR CERTIFICATION (SMC)

CMS continues to streamline the certification approach and move towards Outcomes-Based Certification (OBC) for Medicaid Enterprise Systems (MES) Information Technology (IT) projects. CMS introduced a significantly Streamlined Modular Certification process and formally sunset the existing processes known as the Medicaid Enterprise Certification Toolkit (MECT). The CMS outcomes-based approach to certification focuses on achieving business outcomes and is intended to reduce the certification burden on states without compromising CMS' responsibility to ensure those systems satisfy all statutory and regulatory requirements. Compared to the process found in the MECT, certification is streamlined in the following ways:

- Reduced the number of required state-submitted MES review artifacts from 29 to seven.
- IV&V Vendor Quarterly Certification Progress Reports no longer required.
- Streamlined Reviews. States undergo an ORR before the system goes live. At least six months after implementation (or Go-Live), a CR is conducted. Project Initiation Milestone reviews are eliminated.
- Introduced Performance Metric Reporting. The state reports on metrics at least once after the ORR and continues after certification. Annual reporting is required for as long as a state continues to receive enhanced funding for O&M unless the CMS State Officer (SO) request a more frequent reporting schedule.
- Reduced Artifacts List. Except for the certification request letter and system acceptance letter, the state does not need to prepare artifacts listed in MECT Appendix B, nor does it need to prepare a Project Partnership Understanding. SMC Appendix C – *Required Artifacts* details the revised artifact requirements.
- The State can submit an alternative format for the MITA State Self-Assessment (SS-A) to CMS, if preferred.

The Agency is required to provide the following data, reports, and performance information, pursuant to 42 C.F.R. §433.112(b)(15) and §433.116(b), (c), and (i), as applicable. This documentation will help demonstrate whether conditions for enhanced funding are met, intended outcomes are being achieved, and metrics are being successfully collected and reported.

- Evidence to support outcomes achievement may include, but is not limited to:
  - Demonstrations
  - Test results
  - Production reports
  - Plans for organizational change management (e.g., managing stakeholders and users, training, help desk)

The Agency provides the evidence used to determine the module is production-ready, which could include test results and other data illustrating the module's capability of achieving intended outcomes. The Agency also demonstrates that their operations staff are implementation-ready (e.g., documentation of trainings and other relevant organizational change management activities that have been conducted and/or are ongoing) to support the successful delivery of the module and ongoing operations. In addition, once the module is in operation, the Agency will provide evidence that they continue to comply with applicable regulations and meet programmatic outcomes.

The evidence from the metrics that are collected and reported are evaluated to determine whether the system is achieving the identified outcomes. As required by 42 C.F.R. §433.112(b)(15) and §433.116(b), (c), and (i), throughout the MES IT investment Lifecycle, the Agency will continue reporting on metrics to ensure that solutions meet regulatory requirements and are measurably supporting desired program outcomes. The CMS SO will collaborate with the Agency to conduct reviews and assessments based on metric reports, helping to ensure continued success and improvement of MES solutions.

4.1 TIMELINE

The Agency has developed a strategy to increase service interoperability and advance the maturity of the MES in accordance with the CMS conditions and standards and the MITA 3.0 Framework in the *Florida FX Procurement Strategy*. The Agency has formed a phased approach to replace the current Florida MES. **Exhibit 4-1: FX Procurement Roadmap Phase 3** below illustrates a timeline for Phase 3 of the projects as agreed upon by Agency executives as part of the Medicaid Enterprise Strategic Plan refresh.

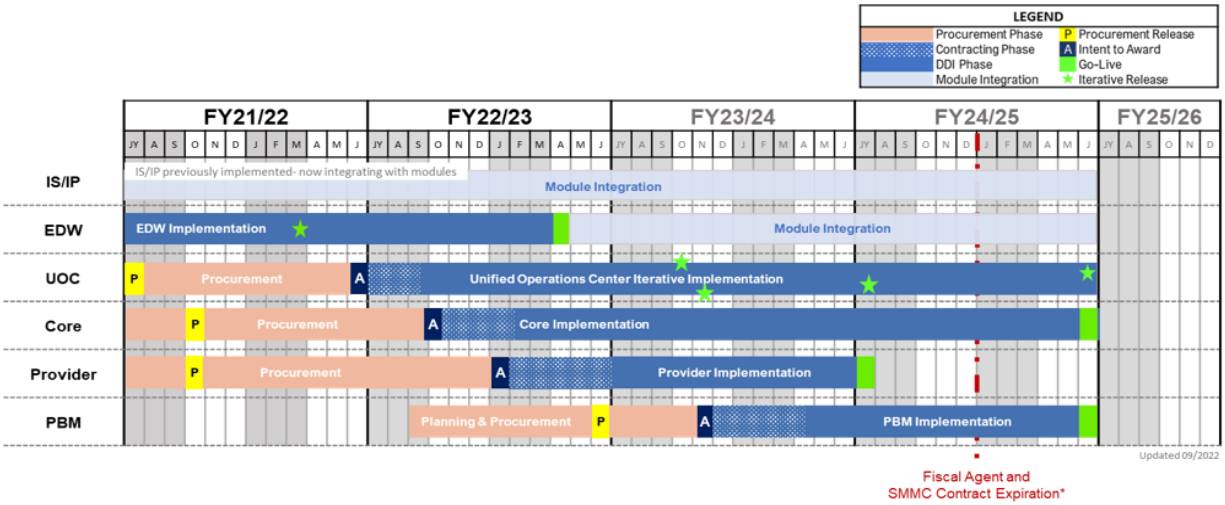

Exhibit 4-1: FX Procurement Roadmap Phase 3

As noted in **Exhibit 4-1: FX Procurement Roadmap Phase 3** above, there are four phases in the FX procurement timeline. Below is a description of each phase:

- **Phase 1** – The Agency procures a Strategic Enterprise Advisory Services (SEAS) Vendor to operate an enterprise-wide Project Management Office (PMO) while providing programmatic, strategic, and technical advisory services to the Agency regarding system integration. In addition, the Agency procures and Independent Verification and Validation (IV&V) Vendor to provide an independent evaluation and review that evaluates adherence to the standards, correctness, and quality of FX Program and projects' solutions to help the Agency ensure that projects are being developed and managed in accordance with Federal, State, and Agency requirements.
- **Phase 2** – The Agency and the SEAS Vendor collaborate to develop an FX infrastructure by procuring vendors to supply IS/IP and an EDW
- **Phase 3** – This phase includes activities to procure modules to transform and improve the business processes that are currently occurring within the FMMIS, replacing this functionality with solutions that are interoperable with other systems within FX, and potentially within the larger Florida Health and Human Services (HHS) Agency ecosystem.
- **Phase 4** – This phase implements the remaining non-FMMIS modules planned in the FX that are necessary to accomplish the FX vision of transforming the Medicaid Enterprise to provide the greatest quality, the best experience, and the highest value in healthcare.

4.2 Communicating and Coordinating with Impacted Staff

It is important that all impacted staff understand the critical role Certification has in the success of the project. Project team members must fully understand the SMC and the individual roles and responsibilities they have in the process. Targeted communication in addition to training is imperative to a successful MMIS Certification.

4.2.1 Communication with CMS SOT and the CMS Certification Review Team

To successfully manage the certification process, it is critical to ensure that the lines of communication are open with CMS. The Agency' Certification Manager tracks any certification related questions for CMS. The Agency Certification Manager requests responses from the CMS SOT who in turn coordinates responses or discussions with the CMS CR Team, if necessary. All certification questions and responses to and from the CMS SOT are tracked in a question log. The responses are shared with the FX Project Team during the regularly scheduled Certification Status Meeting.

Outside of the regular meetings with the CMS SOT during the development of each module, the CMS SOT also provides a CMS Certification Email where the Agency Certification Manager can send questions.

As the Agency nears the execution of each review, communication with the CMS CR Team will increase. All communications with the CMS Certification Team will go through the Agency Certification Manager to ensure consistent representation from the Agency.

4.2.2 MEETINGS AND WORK GROUPS

Certification Status Meeting

The Agency will implement, conduct, and facilitate a Certification Status Meeting with stakeholders, which will include all FX Project Managers and leadership from the Agency, SEAS Vendor, IV&V Vendor, IS/IP Vendor, and the FX solution vendors, along with their dedicated certification resources. The purpose of the Certification Status Meeting is to provide a high-level status of certification tasks, including development and collection of artifacts and evidence, discussion of any potential risks or issues associated with certification, and identification and management of any cross-project impacts. High-level status reports generated from the Certification Tracking Tool are also reviewed.

The meeting also serves as an avenue to disperse other critical information across all organizations. The SEAS Vendor is responsible for supporting the meeting by providing the project schedule status each month.

Certification Work Group by FX Project

A Certification Work Group meeting for each FX Project will be conducted on a regular basis (contingent on the level of certification activity necessitated by phase of the project) to ensure all parties work together with the Agency to ensure a successful certification. The Certification Work Group members will initially only include the Agency, SEAS Vendor, IV&V Vendor, IS/IP Vendor, and the FX solution vendors' designated certification resources, however, as the work group deems necessary, other critical members may be identified and expected to participate, especially as review planning activities begin for each review. The Certification Work Group is facilitated by the Agency Certification Manager.

The Certification Work Group will be responsible for identifying certification tasks, completing, or coordinating the effort throughout the SMC life cycle. Some of the work group responsibilities include reviewing and developing outcomes, metrics, and content for certification training, identifying certification communication topics, producing certification content for in inclusion in the FX Portal, making planning decisions, reviewing, and approving certification evidence and other required documentation, preparing for reviews, and executing each review. Members will all be assigned tasks that will be tracked in the meeting minutes. Action items not resolved in the work group by team members will be escalated as risks and documented using the enterprise risk process. All work group members assigned tasks are expected to complete assigned tasks in a timely manner to ensure that a successful review with the CMS. Some tasks the Certification Work Group members will complete, or ensure resources are assigned to complete, include:

- Outcomes and Metrics
  - Developing outcomes
  - Developing evaluation criteria to measure success
  - Developing metric to measure outcomes

- Certification Training
  - Identifying Topics
  - Developing Training Materials
  - Reviewing Training Materials
  - Supporting Training Sessions
    - Facilitating
    - Presenting
    - Projecting
- Certification Communications
  - Identifying Topics
  - Developing FX Portal Content / other communications content, etc.
  - Reviewing FX Portal Content / other communications content, etc.
- Certification Progress Review
  - Reviewing Certification Assignment status and updating tasks
  - Coordinating development of certification artifact documentation
  - Resolving certification evidence or artifact issues
- Review Planning Activities
  - Developing a style guide and other standards as necessary for all vendors to use and refer to when developing artifacts, presentations, evidence, etc.
  - Developing and finalizing agendas for the reviews
  - Scheduling online meetings/conference calls
  - Securing meeting rooms, equipment, and Microsoft (MS) Teams sessions for the reviews
  - Testing access prior to granting access to CMS reviewers
  - Granting and communicating access to the CMS CR Team
  - Assigning roles and responsibilities for the review meetings
- Review Preparation Activities
  - Identifying and developing presentations
  - Scheduling and participating in dry runs and practice reviews
  - Schedule and participating in ORR and CR Practice Sessions
  - Developing certification articles and content to be included in the FX Newsletter
  - Identifying outreach avenues to communicate with project stakeholders
- Review Execution Activities

- Facilitating communication and meeting access
- Presenting
- Projecting and Virtual Meeting/Sharing Responsibilities
- Documenting Meeting Minutes, actions, and decisions
- CMS Action Item Resolution Status

- Lessons Learned
  - Identifying and evaluating ways to address lessons learned in the current process
  - Recommending implementation of lessons learned for future projects

The Source Pulse Tracking Tool procured by the Agency will facilitate tracking of all certification activities for each project life cycle. The Source Pulse Tracking Tool is not intended as the place to store the artifact documents or evidence. The tool will provide links to artifacts and evidence stored in the FX PR. The Source Pulse Tracking Tool will track assignments for certification team members and events, including evidence gathering, scheduling/coordinating/preparing for CMS reviews, FX Vendor artifact submission and approval, and any other activities/tasks.

4.2.3 FX PORTAL

The FX Communications Plan includes the FX Portal published to the FX stakeholders. The FX Portal communicates to stakeholders who are not typically included in the development of the project but are users of the system. Disseminating certification related information helps reinforce training and ensures staff understand the new process and stays engaged in each review through final certification of each FX module.

The FX Portal will be leveraged and includes a certification section. This is a great avenue to communicate the upcoming certification training schedules and share other certification information such as review schedules, certification status, certification contacts for each organization, etc. Though anyone can suggest and provide content, the Certification Work Group is responsible for brainstorming ideas for articles, developing the certification related content, and working with the FX Portal editor/coordinator to submit and publish content in the FX Portal. The Certification Work Group will ensure that communications with stakeholders regarding certification is frequently provided to stakeholders throughout the life of the project.

4.3 TRAINING IMPACTED STAFF

Since compliance of federally mandated processes and procedures is a critical success factor for each FX module, a solid enterprise-wide certification training approach will help ensure successful outcomes are achieved. It also helps to ensure all affected stakeholders clearly understand the processes and the roles they play. For this reason, the Agency has developed a curriculum outline that includes identifying and training impacted staff on core Certification tasks, roles, materials, and timeframes. Once trained, impacted staff will have the information

and guidance they will need to successfully achieve full certification for each FX module implemented.

The new process engages stakeholders earlier than most stakeholders are accustomed to when compared to the previous MMIS Certification review protocol in place when Florida last went through the certification process. The Agency is responsible for planning and training tasks. This includes identifying impacted stakeholders as well as developing the curriculum and training materials in addition to scheduling and delivering certification training for project stakeholders.

4.4 Finalizing the Artifacts and Evidence

4.4.1 Joint Reviews

The Certification Work Group coordinates joint review sessions with the relevant SMEs as well as leads the dedicated certification resources from the Agency, SEAS Vendor, IV&V Vendor, IS/IP Vendor, and the FX solution vendors (for ORR and CR). Together they review the Intake Form required artifacts, and the evidence to validate that the certification criteria evidence demonstrates the expected outcomes. If deficiencies are identified, the Agency documents the deficiencies and assigns action items to the parties assigned to correct the deficiencies. The Agency Certification Lead monitors the action items through to resolution.

4.4.2 Quality Checks

The Certification Work Group members will conduct quality checks of all the artifacts after all the joint reviews are completed and before they are submitted to the Agency Certification Manager for final review prior to and upload to the CMS Box Repository.

Results of the quality reviews are shared with the Agency, SEAS Vendor, IV&V Vendor, IS/IP Vendor, and the FX solution vendors for necessary resolution and are entered and tracked in the Source Pulse Certification Tracking Tool. Quality errors are expected to be remediated and addressed in a timely manner to ensure timely, accurate delivery of the evidence to the IV&V Vendor.

4.4.3 IV&V Delivery and Review

Once the quality review, remediation, and quality checks are complete, the Certification Work Group ensures that all artifacts and evidence are finalized and stored in the FX Certification Repository. The Certification Work Group will validate that all files and folders are numbered, named, and filed correctly before handing it off to the Agency Certification Manager for final sign off and delivery to the IV&V Vendor for their review/assessment.

4.5 MILESTONE REVIEWS

This section details general information that applies to the ORR and CR described in Sections 4.6.3 – *The Operational Readiness Review (ORR)*, and 4.6.5 – *Certification Review (CR)*. For information unique to a specific review, please reference the specific review section for details.

4.5.1 PLANNING

As noted previously, the Certification Work Group is responsible for suggesting and making review planning decisions. The Certification Work Group also meets to plan for the reviews and identifies, assigns, and carries out the necessary planning activities to be completed to ensure a successful review.

Some activities, which must be completed as a part of the planning effort for all reviews, include:

- Determining, with CMS, whether the review will be virtual or on-site
- Scheduling and facilitating planning meetings/
  - Scheduling meeting rooms / MS Teams
  - Sending meeting invitations
- Documenting meeting minutes, actions, and decisions
- Tracking action items to closure
- Identifying the CMS Certification Team and MITRE members that need access to the required artifacts and evidence, if using the FX Certification Repository
- Identifying the FX Certification Team members that need access to the required artifacts and evidence, using the CMS Box Repository

4.5.2 PREPARATION

To prepare for all reviews, the Certification Work Group will ensure that all the required artifacts and evidence are stored securely in the FX Certification Repository with the appropriate working links in Source Pulse. The Agency Certification Manager will post final artifacts and evidence to the CMS Box Repository.

All Agency SMEs participating in the reviews should be familiar with the FX Certification Repository and content that the CMS Certification Team and MITRE will be reviewing from participating in the joint reviews. SMEs will be expected to continue to be familiar with these documents in preparation for the actual review.

Activities completed by the Certification Work Group as a part of the preparation effort for all reviews include:

- Scheduling meeting rooms for planning, practice, and review sessions

- Sending meeting invitations for practice sessions
- Developing and reviewing presentation materials to be used for the reviews
- Planning and conducting practice sessions with all Agency and FX Vendor participants
- Coordinating requests and access set up for CMS Certification Team and MITRE reviewers including:
    - Providing credentials and instruction to the Source Pulse Tool, FX Certification Repository
    - Resolving any issues with links to the required evidence to support the artifacts and evidence
    - Coordinating collection and delivery of additional last-minute requests for artifacts by the CMS
- Coordinating system demonstrations and live online access, as required
- Communicating with CMS SOT, CMS Certification Team, and MITRE
- Sending meeting invitations for reviews
- Preparing and distributing agendas based on information received by the CMS

4.5.2.1 Advance Requests and Questions from the CMS Certification Team

In advance of a review, the CMS CR Team will send questions and requests for additional artifacts, which will help to inform the state of the focus of discussions expected during the review. CMS does not expect, but will accept, responses ahead of the scheduled review. The Agency's participants will present and defend their responses to CMS' and MITRE's questions during the review.

4.5.2.2 Operational Readiness Review (ORR) and Certification Review (CR) Practice Sessions

Once presentation responsibilities are assigned, the responsible parties are expected to prepare their presentation and provide the completed presentations to the Certification Work Group for review according to the established deadline. The Certification Work Group will complete quality reviews of the presentations to ensure all materials are consistent and ready for presentation.

The Certification Work Group will schedule practice sessions for each presenter to present their material to the full group. This allows time for feedback and necessary modifications to the presentations to be made.

A final practice session is scheduled within five days of the actual reviews.

4.5.3 EXECUTION

The Agency will facilitate all ORR and CR Sessions, and the Certification Work Group shall support as outlined below:

- Making sure computers are displaying meeting content for participants and virtual attendees
- Providing scribes to take meeting minutes and capture action items and decisions made during each review session
- Ensuring links to the evidence and/or demonstrations are functioning for display and review
- Making sure the appropriate resources are in the room to answer questions
- The Agency, IS/IP Vendor, and the FX solution vendors will make relevant staff available to answer all questions from the CMS Certification Team and MITRE

The Certification Work Group shall manage the action items during each review and maintain the CR Action Log. Action items will be assigned throughout the process to the Agency as well as to any appropriate vendors. It is critical for any parties who are assigned an action item to resolve it while the CMS Certification Team and MITRE reviewers are still meeting with the Agency.

All action items should, at a minimum, be turned around within 24 hours. If more time is necessary, it must be discussed and approved by the Agency Certification Manager. Resolution timeframes that exceed five business days from the initial request must be updated weekly. The Certification Work Group shall support the Agency during each review with resolving and delivering any requests from the CMS Certification Team and MITRE by:

- Documenting all action items on the CR Action Log noted in **Exhibit 4-2: Florida Certification Assignment Tracker & CMS Coordination** below
- Confirming action items captured with CMS before each lunch break and before concluding each day
- Coordinating the delivery of the information from the party responsible for the action item to the CMS Certification Team and MITRE reviewers and all certification stakeholders, and agreement is reached with CMS and MITRE prior to closing the action item
- Ensuring Florida team members are informed by email of assigned action items as soon as the log entry is made
- Providing CMS Certification Team and MITRE with updates on action items status until all action items are resolved

Action items that have been resolved are all later logged into the FX Action Items Log to capture the history. Any items that are not resolved during the review will also be added and tracked accordingly until they are closed.

Exhibit 4-2: Florida Certification Assignment Tracker & CMS Coordination is an example of the information that will be captured and managed by the Agency to accomplish action item tracking and resolution during all reviews.

Project: EDW and IS/IP											
CMS AI #	Date Raised	Agenda Section	Name of CMS Requester	Action Item	Action Item OWNER	DUE DATE	STATUS (Open, In Process, Completed	STATE APPROVER	Date Approved	CMS ACCEPTED (name)	NOTES

Exhibit 4-2: Florida Certification Assignment Tracker & CMS Coordination

4.6 PROCESS OVERVIEW

The activities for the three phases in the SMC process are shown in **Exhibit 4-3: Streamlined Modular Certification Life Cycle** below.

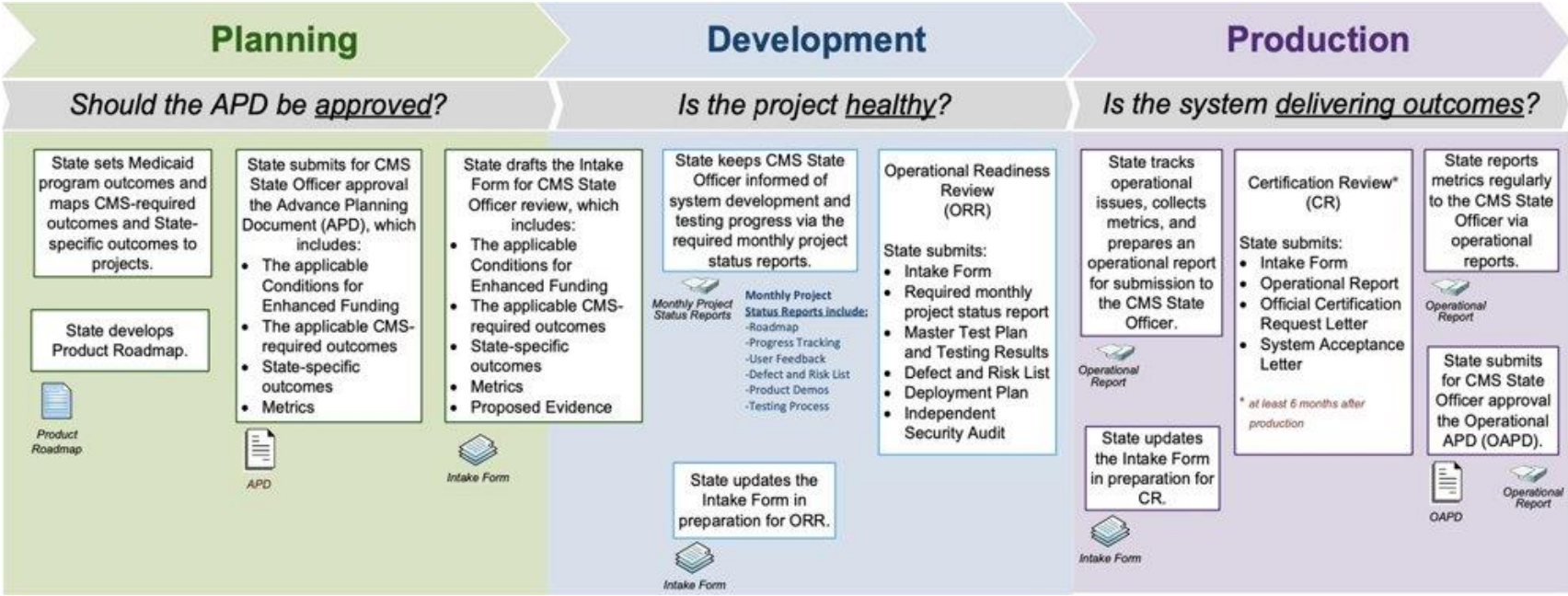

Exhibit 4-3: Streamlined Modular Certification Life Cycle

The three phases outlined in this section include:

- Planning Phase
  - CMS Collaboration
  - Outcomes and Metric Development
  - Conditions for Enhanced Funding
  - Product Roadmap
  - APD Submission
- Development Phase
  - Intake Form
  - Design, Development, and Implementation
  - Monthly Project Status Report and other artifacts required for ORR
  - ORR
- Production Phase
  - Operational Reports including artifacts required for CR
  - Update Intake Form
  - Certification Review
  - Metrics Reporting
  - Operational APD (OAPD)

4.6.1 PLANNING PHASE

This initial planning phase includes many activities and a close collaboration, with frequent conversations, between the Agency and the CMS SOT to get the project up and running. During this phase, the Agency drafts their planned program outcomes and map outcomes to projects on the FX Roadmap. The Agency articulates their planned CMS-required and state-specific outcomes, metrics, and how they propose to demonstrate achievement of those results. The planning phase ends with submission of the APD requesting funding for the DDI of a project or certifiable module. Artifacts produced in the planning phase assist CMS in determining if the APD should be approved.

Included below are high-level descriptions of activities that occur during this phase as illustrated in **Exhibit 4-3: Streamlined Modular Certification Life Cycle** above.

4.6.1.1 CONSULT WITH CMS

As explained in the guidance provided by the CMS, the Agency is encouraged to collaborate with CMS throughout the MES IT Investment Lifecycle, but especially during the initiation and planning stage, when the Agency is expected to do the following:

- Notify CMS SOT of the Agency's intent to update the MMIS/modules
- Collaborate with CMS to:
  - Develop the APD
  - Include CMS Mandated Regulatory Requirements and Outcomes
  - Design Agency specific outcomes and metrics

4.6.1.2 FX ROADMAP

As mentioned previously, the Agency developed the FX Roadmap, which is a procurement roadmap, consisting of four phases. During the planning phase, CMS requires states to articulate their roadmap and timeline for implementation when requesting FFP that will support a project. The FX Roadmap depicts the sequence and timeline of projects that will transform the existing MMIS into a modular system. The timeline presented in the FX Roadmap corresponds with the funding request in the APD by federal fiscal year.

4.6.1.3 APD DEVELOPMENT

The Agency drafts the APD to request funding for new modules or projects. The APDs are plans of action to request FFP for the DDI of technology or services. The APD provides the CMS with the information necessary to approve FFP at the appropriate match rate.

The APD must include:

- Programmatic Value Aligned to State Priorities
- Conditions for Enhanced Funding (CEF)
- CMS and State Specific Outcomes and Metrics
- Statement of need and objectives
- Requirements
- Alternative analysis
- Reuse consideration
- Project management plan
- Proposed project budget and cost distribution
- Statement of security/interface and disaster recovery requirements

- Assurances

The Agency attests in the IAPD requesting enhanced FFP for the development and implementation of MMIS systems or projects that the system will meet the Conditions for Enhanced Funding found in CFR 433.112 and that the system will remain in compliance with Medicaid program standards, laws, regulations, and industry-best practices once it is in production. The Agency's APD describes how or attests that the system will comply with the conditions. Appendix A – *Conditions for Enhanced Funding* contains the complete list of CMS conditions.

Outcomes describe the measurable improvements to a state's Medicaid program that will result from the delivery of a new module or enhancement to an existing system. Additionally, outcomes should support the priorities of the Medicaid program, be directly enabled by the state's IT project, and be stated in the APD. An outcomes statement and metrics need to be provided articulating the measurable improvements to a state's Medicaid program that will result from the delivery of a new module or enhancement to an existing system.

The Agency will reach out to their CMS SOT during the planning phase. CMS will collaborate with the Agency to support APD development, enabling inclusion of outcomes in the IAPD that align to project goals. CMS required outcomes are module-specific, focused on validating functionality, based on regulations, and provide a baseline for what is required of a MES, including the efficient, economical, and effective administration of the state's Medicaid program. CMS required outcomes are designed to be used as a starting point for aligning what the state is trying to accomplish with a project in accordance with CMS expectation. Appendix B – *CMS-Required Outcomes* provides the complete list of CMS-required outcomes specific to each individual module.

The CMS-required outcomes are distinct from (and should complement) the state-specific outcomes, which describe the specific business problem the state is trying to solve with a given project. State-specific outcomes focus on improvements to the Medicaid program not specifically addressed by the CMS-required outcomes. State-specific outcomes reflect the unique circumstances or characteristics of the state and its Medicaid program. They should be specific to the IT investment the state is making and should allow the state to demonstrate progress towards meeting its goals. A close, ongoing partnership between the CMS SOT and the Agency is essential for creating state-proposed outcomes and metrics.

In addition, the Agency's IAPD should also identify metrics, which are data providing evidence that outcomes are being met on an ongoing basis. The metrics enhance transparency and accountability of IT solutions in meeting regulatory requirements and state goals, provide insight into program evaluation, and opportunities for continuous improvement.

The Agency populates the Intake Form and Operational Report Workbook with the initial metrics definitions after the APD is approved.

4.6.1.4 DEVELOP DRAFT SOLICITATION

Note: The Agency utilizes the Invitation to Negotiate (ITN) procurement process instead of RFP for more flexibility in procuring these types of services. Throughout this document, use of the federal references to RFP also includes the ITN procurement process used in Florida.

During this phase, the Agency prepares the solicitation(s) to implement the proposed requirements and produce the desired outcomes identified in the APD.

The draft solicitation wherever enforceable under state law should include the following provisions:

- Define goals and objectives
- Environment requirements (business, architecture, data)
- Reuse, interoperability, and modularity requirements
- Conditions tying compensation to meeting or exceeding defined goals (e.g., service level agreements)
- Reservation of right for the state to approve and/or remove subcontractors
- Require contractors to cooperate with other contractors (includes IV&V Vendor)
- Require contracts to abide by all state's security and privacy policies

The state will send the draft solicitation(s) to the CMS SOT for review.

The SEAS Vendor is responsible for the development of the ITN requirements, then confirms the requirements and completes the final draft of the solicitation through a task order. All supporting activities in the development of the draft ITN are the responsibility of the SEAS Vendor. The Agency will draft the cover letter and submit the final draft of the solicitation to the CMS SOT for review and approval.

4.6.1.5 IV&V SUPPORT

Throughout the FX Program, the IV&V Vendor shall provide IV&V services for CMS and Florida in support of the MES IT Investment Lifecycle Engagement and Certification Process in accordance with the most current certification guidance from CMS. The IV&V Vendor shall participate in the review and validation of module certification materials throughout the life cycle (planning, development, and production) including all activities conducted during the requirements, DDI, testing, and implementation phase of a project.

4.6.2 THE DEVELOPMENT PHASE

In the DDI phase, the Agency will partner with their CMS SOT to keep CMS apprised of the progress a project is making toward achieving the CEF and desired program outcomes. The Agency submits the Intake Form to CMS to trigger the start of the development phase.

At the beginning of the development phase, the Agency and module vendor develops a Master Test Plan, following Appendix F – *Medicaid Enterprise Systems Testing Guidance Framework*. Throughout the development phase, the Agency provides their CMS SO with regular development and testing progress in the form of testing results, defect reports, and regular software demonstrations.

4.6.2.1 INTAKE FORM

The Intake Form Template is used to track what a state is trying to achieve with a given project, including the CMS-required outcomes, state-specific outcomes, metrics, and associated evidence. It is completed and customized for each state project and required for both ORRs and CRs. The Agency and the CMS will use the Intake Form throughout the SMC process to track the information about a project that is important for certification. The Intake Form Template is tailored for each state project. The Agency will fill out the Intake Form Template by entering the CMS-required outcomes that document compliance with regulations that are applicable to the project, state-specific outcomes, and the metrics they will use to show that the project is achieving its outcomes on a continuous basis.

The Intake Form Template information should match what is in the APD. Since the Agency will communicate these key concepts to potential vendors, the initial version of the Intake Form Template will be complete prior to the Agency's release of an ITN. As the Agency progresses with the project, the Agency and CMS SOT will work together to identify, in the Intake Form Template, the types of evidence the state should provide to demonstrate that the outcomes have been achieved.

The Intake Form Template, as shown in **Exhibit 4-4: Intake Form Template** below, includes the following two tabs:

- Tab 1: Conditions for Enhanced Funding. The Agency will provide evidence of compliance with the CEF specified in 42 CFR § 433.112 and CMS will provide an assessment of the Agency's compliance.
- Tab 2: Outcomes & Metrics. The Agency will provide evidence of compliance with CMS-required outcomes and state specific outcomes and CMS will provide an assessment of the Agency's compliance.

Metrics: The Agency will demonstrate progress on metrics, which is data that should provide evidence that outcomes are being met on an ongoing basis in production, including initially at the ORR (with test data) and the CR (with production data). These metrics should include what the state believes will allow them to know they have been successful on any given project. There are columns for the state to provide evidence for, and for CMS to provide an assessment of, the metrics at the ORR and CR.

Reference #	Outcome (Narrative Description)	Metric Description (Narrative Description)	Metric Data (Numerical)	Source(s)	State ORR Evidence
The state uses this column to provide the reference number for each CMS-required outcome in Column B. It should be the same as the matching reference number in the first column of each table in Appendix B of the SMC Guidance Document. For State-Specific outcomes just create a unique reference number for tracking purposes.	The state uses this column to provide the outcomes that are applicable to a state project that is up for certification.	The state uses this column provide the description of metrics that will be used to demonstrate the achievement of this outcome when the system is in operation. Also the metrics provided are what the state is expected to report annually in support of enhanced FFP funding requests for Operations.	The state uses this colum to provide the actual numerical data (or a link to the metric data). This metric data is what the state is expected to report annually in support of enhacned FFP funding requests for Operations.	The state uses this column to provide the statutory, regulatory, sub-regulatory, or other source which necessitated the outcome. For CMS-required outcomes this column should be populated with the regulatory references that are identified in the third column of Appendix B of the SMC Guidance Document.	The state uses this column to directly link or list the evidence the state will use to support outcomes and metrics at ORR. Examples of evidence at ORR may include, but is not limited to, testing results, demonstrations, planned operational reports, and plans for organizational change management (e.g., managing stakeholders and users, training, help desk).

Exhibit 4-4: Intake Form Template

4.6.2.2 OPERATIONAL REPORT WORKBOOK

The Agency must submit an Operational Report at multiple steps of the certification process and continue building on the document over time. The report, as shown in **Exhibit 4-5: Operational Report Workbook Template** below, will be submitted as part of the APD, ORR, and CR processes. The CMS Box Repository is the default repository for all operational reports. CMS checks and validates the data at multiple steps of the operational reporting process. Collaboration between the Agency and CMS is critical to ensure quality metrics and timely reporting. Upon approval of the CR, the Agency submits module related metrics in operational reports on a quarterly basis during the Operations and Maintenance (O&M) phase. Guidance provided by CMS to assist states in completing and submitting Operational Reports can be found in **Appendix H: Medicaid Enterprise Systems (MES) Data Submissions and Intake Process Procedures Manual, September 1, 2022.**

Metric ID	Metric Name	Outcome Reference #	Metric Description	Numerator Description	Denominator Description	Value Type	Note
The state should use this column to provide a unique identifier for the metric, following the convention of StateName-SystemType-MetricNumber. For example, the first metric for TN for Eligibility and Enrollment system should have a Metric ID of "TN-EE-1." Note Metric IDs should NOT be reused. If the state deletes an existing metric, the existing Metric ID should NOT be reused. If the state adds a new metric, use the next consecutive number.	The state should use this column to provide a title for the metric.	The state should use this column to provide the Reference # of the outcome(s) associated with the metric. It should be the same as the matching identifier defined in the Intake form (the "Reference #" column on the "Outcomes and Metrics" tab). For multiple outcomes mapped to one metric, separate the reference #s with a "|." For example, if the Metric ID "TN-EE-1" measures three outcomes (EE1, EE2, and EE4), the matching Outcome ID should be entered as "EE1|EE2|EE4". If the outcome is a state-specific outcome, and not a CMS-required outcome, use the acronym "ST" and then the appropriate numerical code.	The state should use this column to provide a description of the metric that will be used to demonstrate the achievement of outcomes when the system is in operation. Also the metrics provided are what the state is expected to report quarterly or annually in support of enhanced FFP funding requests for operations.	If the metric is a percentage or ratio, the state should use this column to provide a description of the numerator.	If the metric is a percentage or ratio, the state should use this column to provide a description of the denominator.	The state should use this column to provide a description for the value of the metric. Description options include: - "Percentage/Ratio" for example, the percentage of EVV visits automatically entered out of the total number of visits. - "Numerical", for example, the number of notifications sent on behalf of Medicaid population. - "List", for example a list of top 5 reason for helpdesk calls.	The state should use this column to provide any additional note on the metric, if applicable.
ST-EE-1	Automated ("No touch") Eligibility Determinations	EE1|EE2|EE4	Automated ("no touch") eligibility determinations are those made in real-time by the system and do not require worker touch or additional information from the applicant.	# of individuals' whose determinations made in the month were entirely automated	Total # of determinations made in the month	Percentage/Ratio	

Exhibit 4-5: Operational Report Workbook Template

4.6.2.3 MONTHLY PROJECT STATUS REPORT

In the DDI phase, the Agency completes the required monthly project status report to submit information showing that the IT projects align with Streamlined Modular Certification and appropriately demonstrates the health of a project.

The Agency must demonstrate project health focusing on the following areas:

- **Achieving targets and milestones**: The Agency should identify how their team will measure incremental progress toward intended outcomes throughout the development

phase and regularly after production. The Agency will describe, in a timeline or roadmap, how the state will achieve and implement functionality, including priorities, dependencies, and milestones.

- **Use of testing to ensure functionality is being delivered**: Agency and module vendor testing should be informed by Appendix F – *Medicaid Enterprise Systems Testing Guidance Framework***.** The Agency and module vender develops a master test plan that describes the details for how and what testing will occur and provides test results throughout the development phase and leading up to the ORR. The Agency should emphasize user engagement during the testing process and include actual users in both user acceptance and usability testing. The test results should not only validate the iterative delivery of system functionality, but also confirm that the system will produce metrics associated with approved outcomes.

The monthly project status should be submitted to their CMS SO, and either the MES mailbox (MES@cms.hhs.gov) or CMS Box Repository. The Agency will partner with their CMS SOT to keep the CMS apprised of the progress the project is making toward achieving the CEF and desired program outcomes. This report keeps the CMS SOT informed on the system development and testing progress. The report must include the following artifacts:

- Roadmap – An up-to-date product roadmap identifying current, planned, and future functionality and milestones
- Progress Tracking – A regular report measuring developmental progress and progress towards achieving outcomes
- User Feedback – A reporting showing how user feedback is regularly incorporated into development
- Defect and Risk List – Known defects and risks that may cause delays and any mitigations or workarounds
- Product Demos – Demonstrations of functionality/features, or regular report of code/feature releases
- Testing Process – A documented testing process aligned with the CMS Testing Guidance Framework

4.6.2.4 INDEPENDENT SECURITY AUDIT

The Agency's MES is the custodian of sensitive information, such as Personally Identifiable Information (PII) and Protected Health Information (PHI), for millions of individuals receiving coverage through Medicaid and the Children's Health Insurance Program. The state and its business partners share the responsibility for ensuring the protection of this sensitive information. States and their respective business partners must demonstrate continuous monitoring and regular security and privacy control testing through an independent security and privacy assessment.

Pursuant to the Health Insurance Portability and Accountability Act (HIPAA) and implementing regulations at 45 CFR §164.308(a)(1)(ii)(A), conducting a risk analysis is the first step in identifying and implementing safeguards that comply with and carry out the standards and implementation specifications of HIPAA. Therefore, a risk analysis is foundational and must be completed to assist organizations in identifying and implementing the most effective and appropriate administrative, physical, and technical safeguards of PHI/PII. Furthermore, the National Institute of Standards and Technology (NIST), Security Assessments Control, CA-2, requires an independent assessment of all applicable security and privacy controls. States should have a fully completed and implemented System Security/Privacy Plan (SSP) before starting the security and privacy assessment. CMS recommends that an independent third party assessor conduct the assessment.

45 CFR § 95.621(f) and SMDL #06-022, requires that state agencies employ assessors or assessment teams to conduct periodic security and privacy control assessments of the MES environment. The assessor's role is to provide an independent assessment of the effectiveness of implementations of security and privacy safeguards for the MES environment and to maintain the integrity of the assessment process. Alternatively, states can require vendors to have their own independent third-party assessment and provide assessment results.

The purpose of a Security Control Assessment (SCA) is to determine whether the security and privacy controls are implemented correctly, operate as intended, and produce the desired outcomes for meeting the security and privacy requirements of the application or system. The SCA also identifies areas of risk that require the state's attention and remediation. The independently conducted SCA provides an understanding of the following:

- The MES application or system's compliance with the state security and privacy control requirements
- The underlying infrastructure's security posture
- Any application and/or system security, data security, and privacy vulnerabilities to be remediated to improve the MES's security and privacy posture
- The Agency's adherence to its security and privacy program, policies, and guidance

Assessment procedures for testing each security and privacy control should be consistent with the methodology documented in the most current version of NIST SP 800-53A, *Assessing Security and Privacy Controls in Information Systems and Organizations*. The assessor prepares a detailed assessment plan using these security and privacy control assessment procedures, the main testing points for the CIS critical controls, and detailed directions for addressing the penetration testing procedures for the Open Web Application Security Project (OWASP) Top 10 vulnerabilities. The assessor modifies or supplements the procedures to evaluate the applications or system's vulnerability to different types of threats, including those from insiders, the Internet, or the network. The assessment methods should include examination of documentation, logs and configurations, interviews with personnel, and testing of technical controls.

Control assessment procedures and associated test results provide information to identify the following:

- Application or system vulnerabilities, the associated business and system risks, and potential impact
- Weaknesses in the configuration management process, such as weak system configuration settings that may compromise the confidentiality, integrity, and availability of the system
- State and/or federal policies not followed
- Major documentation omissions and/or discrepancies

4.6.3 THE OPERATIONAL READINESS REVIEW (ORR)

The Agency must undergo an ORR with CMS prior to releasing their module into production. The Agency should schedule the ORR with their CMS SO well in advance of the planned Go-Live date and together define the scope of the review. The Agency will demonstrate with appropriate evidence that the system is ready to be released, that it is likely to achieve the approved CMS-required and state-specific outcomes, and it can support the generation and reporting of metrics that were approved in the APD.

The ORR date should be scheduled to provide sufficient time to prepare for the review (approximately six months). During the ORR preparation period, CMS and the Agency will determine the minimum set of required artifacts from Appendix C – *Required Artifacts List***,** evidence needed to demonstrate the project is ready to enter production, and that outcomes are likely to be achieved. Evidence includes the required Independent Security Audit, detailed in Appendix D – *Framework for the Independent Third-Party Security and Privacy Assessment Guidelines for Medicaid Enterprise Systems*. Any required legal non-disclosure and data-sharing agreements should be prepared for the review of the relevant module.

CMS believes that proper and complete systems testing, particularly testing with users, is an important indicator of project success. Hence, testing results are a core part of what CMS and MITRE evaluate during the ORR. The evidence (e.g., testing results, demonstrations, plans for organizational change management) must clearly demonstrate that:

- The required Conditions for Enhanced Funding applicable to the project and described in the APD are met.
- The IT functionality associated with the applicable CMS-required and state-specific outcomes and described in the APD have been developed and tested in accordance with the Agency's master test plan.
- The system will support the collection and reporting of metrics described in the APD.

The ORR provides an opportunity for CMS and the Agency to review the Agency's implementation experience, confirm that a system is ready to enter production, and that the

system is likely to achieve the outcomes and metrics described in the APD. The ORR must be conducted prior to a module going into production. The Agency should be prepared to:

- Provide the evidence that they are using to determine their system is ready to go into production (e.g., test results and data illustrating that outcomes are being achieved).
- Demonstrate that their operations staff are ready for implementation and that they are compliant with applicable regulations.
- Assess the system's performance and functionality against outcomes through the submission of the Intake Form.
- Provide evidence that the system continues to comply with applicable regulations and meets programmatic outcomes once in production.

Exhibit 4-6: Operational Readiness Review Flow below depicts the activity process flow utilized to conduct the review.

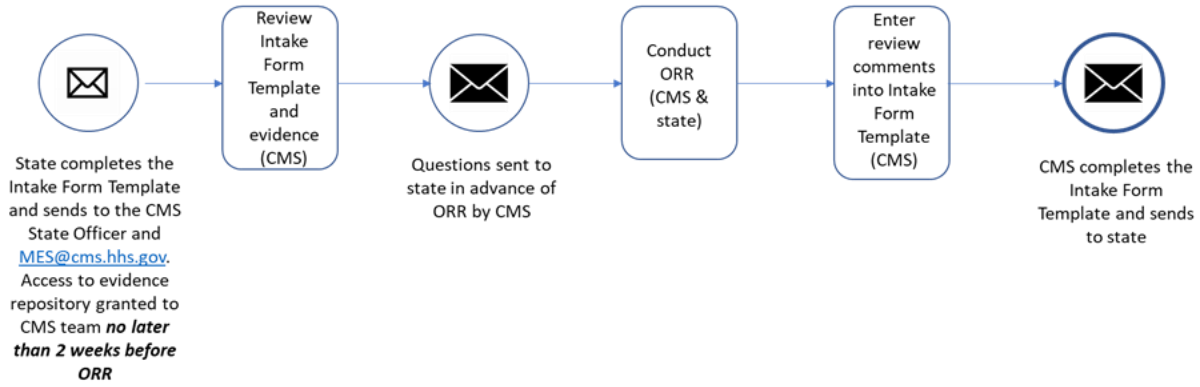

Exhibit 4-6: Operational Readiness Review Flow

The ORR process initiates with the Agency completing the Intake Form and sending it to CMS at least two weeks prior to the ORR. The Agency will populate the Intake Form with the applicable CEF, applicable CMS-required outcomes, state-specific outcomes, and metrics that will be reported. In addition, the Agency provides access to the necessary artifacts and evidence. For the ORR, the following steps are completed:

- The Agency completes the state columns of the Intake Form and Operational Report Workbook.
- The Agency populates the Intake Form and Operational Report Workbook with any updated metrics definitions.
- The Agency saves related evidence and artifacts in the FX Certification Repository for upload to the CMS Box Repository to make the evidence accessible to CMS reviewers and MITRE. The required evidence and artifacts include:

- Monthly required project status reports, which are inclusive of the indicators of project health
  - Roadmap
  - Progress Tracking
  - User Feedback
  - Defect and Risk List
  - Product Demonstrations
  - Testing Process
- Master Test Plan and Testing Results
- Deployment Plan
- Independent Security Audit

- At least three weeks before the ORR, the state sends the completed Intake Form to the CMS SO and to MES@cms.hhs.gov and uploads the evidence to the CMS Box Repository.
- Prior to the ORR, CMS will review the evidence, compile a list of any preliminary questions, and send those to the state to address during the ORR session.

The ORR review session is divided into two segments, which include an Agency presentation and a question and answer (Q&A) session. During the first segment, the Agency provides a succinct project overview and demonstration (via testing results, live demonstrations, other evidence, etc.). The Agency should indicate how the system collects the data necessary for metrics reporting to validate the continued health of the system post-production. The Q&A session provides CMS reviewers with time to ask additional questions based on information provided before and during the ORR session. Because the ORR focuses on both outcomes achievement and system deployment, the Agency's representation will include appropriate subject matter experts from program, business operations, and IT.

Upon receipt of the Intake Form, CMS and MITRE review the Intake Form and evidence. The CMS review focuses on system business outcomes and metrics, while MITRE's sole scope is security. The CMS review takes approximately two weeks, at which time CMS will provide the Agency with any comments or questions that need to be resolved for the ORR. The Agency has two weeks to remediate or resolve any questions prior to the ORR. The Agency can submit answers prior to the ORR, but it is not a CMS expectation. Agency representatives will present and defend responses to the questions during the ORR. The ORR is expected to last one full day but could be longer.

Within two weeks of the ORR, CMS will enter comments into the Intake Form and send it to the Agency. The Agency continues working with their CMS SO on addressing ORR observations and findings as the project moves into production, and in preparation for the Certification Review.

4.6.4 PRODUCTION

Once the system is in production, the Agency will regularly and consistently provide evidence that it continues to comply with applicable regulations and meets programmatic outcomes. The CMS SOs will collaborate with the Agency in conducting reviews and assessments based on metric reports to ensure continued system performance. The Agency will submit operational reports monthly, which contain data and/or evidence that demonstrates the continuous achievement of required and desired outcomes and corresponds to the agreed-upon outcomes for each applicable MES module. Operational reports should also include data and/or evidence regarding how the system is regularly incorporating user feedback on the system in production, as well as any known defects, risks, and issues that may cause delays and any associated mitigations/workarounds. The operational report should include the same level of streamlined information; confirmation of compliance with the CEF, outcomes, metrics, and the related supporting evidence. Guidance provided by CMS to assist states in completing and submitting Operational Reports can be found in **Appendix H: Medicaid Enterprise Systems (MES) Data Submissions and Intake Process Procedures Manual, September 1, 2022**.

Once the system has been in production for at least six months, and the Agency can report on approved metrics, a CR will be conducted with their CMS SO. A CR is necessary for the Agency to receive enhanced federal funding for system maintenance and operations. The Agency schedules the CR with their CMS SO well in advance to prepare for the CR and collaboratively define the scope of the review. The Agency will demonstrate with appropriate evidence that the approved CMS required outcomes, state-specific outcomes, and metrics are being achieved by the system in production.

4.6.5 CERTIFICATION REVIEW (CR)

To receive enhanced federal match for maintenance and operations, the state must request a CR for a project that has been in operation for at least six months. Because of the six-month minimum wait between production and the CR, the state must report metrics for at least six months before the CR. In contrast to the ORR, which is focused on the demonstration of functionality associated with the applicable CMS-required and state-specific outcomes in pre-production, the CR is focused on demonstrating the impact of that functionality in production, as assessed by the metrics. During the CR, the Agency demonstrates to CMS that the system in production achieves the value described in the APD. The Agency ensures that all appropriate program, business operations, and IT subject matter experts are present for the CR.

Exhibit 4-7: Certification Review Flow below depicts the activity process flow utilized to conduct the review.

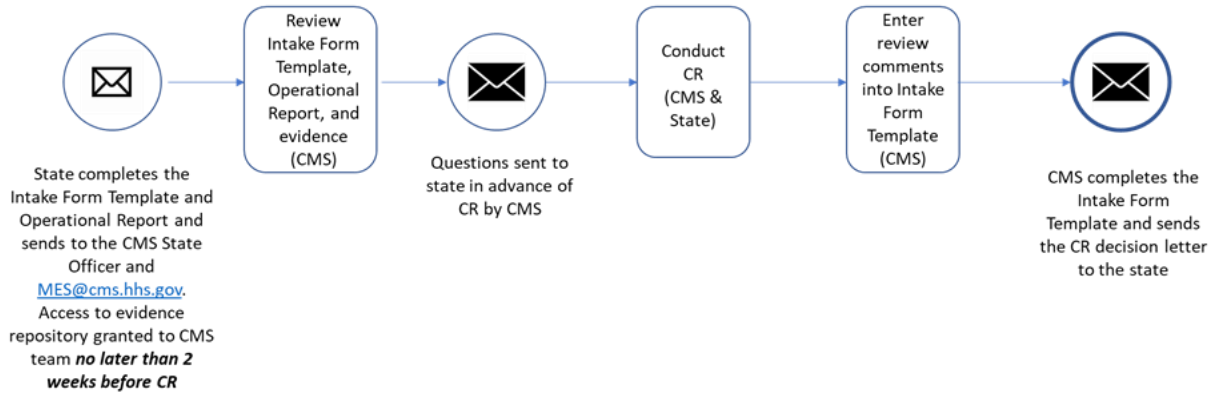

Exhibit 4-7: Certification Review Flow

To request a CR, the Agency must submit an Official Certification Request Letter that includes:

- The date at which the system became the system of record
- The date back to which the Agency is requesting the system be certified
- A proposed timeframe for the review

The letter must be accompanied by information that demonstrates the Agency is ready for the module to be certified. Readiness means that the Agency has:

- Submitted all metrics related to the project being certified, up to the most recent quarter
- Uploaded required artifacts and evidence to the CMS Box Repository)
- Submitted a copy of the System Acceptance Letter
- Submitted an operational report
- Demonstrates that the MES module requesting certification meets all applicable security controls and requirements
- Demonstrates that the MES module requesting certification complies with the Transformed Medicaid Statistical Information System (T-MSIS) requirements

The CR process initiates with the Agency completing the Intake Form and sending to CMS. The Agency will populate the Intake Form with the applicable CEF, applicable CMS-required outcomes, state-specific outcomes, and metrics that will be reported. The Agency uploads the necessary artifacts and evidence to the CMS Box Repository.

For the CR, the Agency will ensure the following steps are completed:

1. The Agency completes the state columns of the Intake Form.

2. The Agency confirms the Intake Form and Operational Report Workbook contains the latest metrics definitions, and updates if necessary.
3. The Agency populates the Operational Report Workbook with the first operational report.
4. The Agency saves related evidence and artifacts in the FX Certification Repository.
5. At least three weeks before the CR, the Agency sends the completed Intake Form to the CMS SO and to MES@cms.hhs.gov and uploads the evidence in the CMS Box Repository.
6. Prior to the CR, CMS will review the evidence, compile a list of questions, and send them to the Agency to be addressed during the CR session.

The CMS SO communicates what, if any, evidence supporting the Conditions for Enhanced Funding or outcomes that the state should upload to the CMS Box Repository prior to the CR, and work with the Agency to agree upon demonstrations of system functionality that will be provided during the CR. In addition, the Agency will clearly describe and display to CMS the metrics used to validate the continued health of the system post-production.

The required artifacts the Agency must produce for the CR include:

- Official Certification Request Letter
- System Acceptance Letter
- Monthly Project Status Reports
- Master Test Plan and Testing Results
- Defect and Risk List

In addition to the Intake Form, the Agency will submit the Operational Report Workbook to CMS at the initiation of the CR. The operational reports should include metrics data that corresponds to the agreed-upon outcomes for each applicable MES module. In addition, the reports should include data and/or evidence regarding how the system is regularly incorporating user feedback on the system in production, as well as any known defects, risks, and issues that may cause delays and any associated mitigations/workarounds. Guidance provided by CMS to assist states in completing and submitting Operational Reports can be found in **Appendix H: Medicaid Enterprise Systems (MES) Data Submissions and Intake Process Procedures Manual, September 1, 2022**.

Upon receipt of the Intake Form, the CMS and MITRE review the Intake Form, operational reports, and evidence. The CMS review takes approximately two weeks at which time CMS will provide the Agency with any comments or questions that need to be addressed during the CR. The Agency can submit answers prior to the CR, but it is not a CMS expectation. Agency representatives will present and defend responses to the questions during the CR. The CR is expected to last one full day but could be longer.

The CR includes a review of CMS findings from the ORR and identifies any operational issues experienced since entering production. Discussions will focus on how these issues have been handled or resolved, highlighting any associated work-arounds, as well as demonstrating the state's measured progress to resolve them (including live demonstrations of functionality, as needed).

As with the ORR, the CR is divided into two segments, an Agency presentation and Q&A session. During the first segment, the Agency concisely demonstrates or otherwise provides evidence of functionality related to the outcomes and their aligned programmatic value. The Agency will discuss ORR findings and operational issues that surfaced since the ORR, as well as discuss how the respective metrics demonstrate that the project is achieving outcomes. During the Q&A segment, the Agency responds to CMS' questions and discusses how successfully the system is supporting the Agency's operational needs and goals.

CMS will follow up with the Agency shortly after the CR to discuss any findings, as applicable. Additionally, CMS will comment about the review in the final CR report returned to the Agency along with a formal CR Decision Letter.

4.6.6 Operational Reporting Phase

To efficiently demonstrate ongoing, successful system operations, the Agency must submit the Operational Report Workbook containing data and/or other evidence that modules are meeting all applicable requirements for the Agency's claimed federal matching funds. These reports should be submitted annually in support of the OAPD request; however, more frequent reporting on key operational metrics may be necessary.

The Operational Report Workbook includes metric data corresponding to the agreed-upon intended outcomes for each applicable MES module. In addition to operational reports, the Agency must submit an OAPD per 45 C.F.R. §95.611, for enhanced funding authorized through certification at 42 C.F.R. §433.116 for any module or system for which the state requests enhanced federal matching funds for the state's expenditures on operations of an existing system. The Agency coordinates with their CMS SO to determine which modules and metrics may need more frequent reporting.

Guidance provided by CMS to assist states in completing and submitting Operational Reports can be found in **Appendix H: Medicaid Enterprise Systems (MES) Data Submissions and Intake Process Procedures Manual, September 1, 2022**.

SECTION 5 REQUIRED PROJECT ARTIFACTS AND REPORTING

Throughout the SMC for each FX module there will be various needs for tracking and reporting to ensure successful Certification. Many of the example reports in this section will need collaboration with the Agency and other vendors to finalize and implement. Several of the examples provided in this section are proposed reports that can be generated from the Source Pulse Certification Tracking Tool once reporting capabilities are implemented. **Exhibit 5-1: Summary of Project Artifacts and Reporting** below summarizes each report, the responsible party, and frequency that is reviewed in this section.

REPORT NAME	RESPONSIBLE PARTY	FREQUENCY
Agency Source Pulse Certification Dashboard	▪ Certification Work Group	▪ Weekly
Agency SMC Workflow Report	▪ Certification Work Group	▪ Weekly
Integrated Certification Project Schedule	▪ FX Vendor Responsible for the Integrated Master Program Schedule	▪ Quarterly
Stoplight Enterprise Certification Artifact Status	▪ Certification Work Group	▪ Weekly
MITA Maturity Level Tracking	▪ Agency	▪ After each update

Exhibit 5-1: Summary of Project Artifacts and Reporting

5.1 AGENCY CERTIFICATION TRACKING AND REPORTING

Exhibit 5-2: Sample Agency Source Pulse Certification Dashboard below provides a high-level view of the overall certification status.

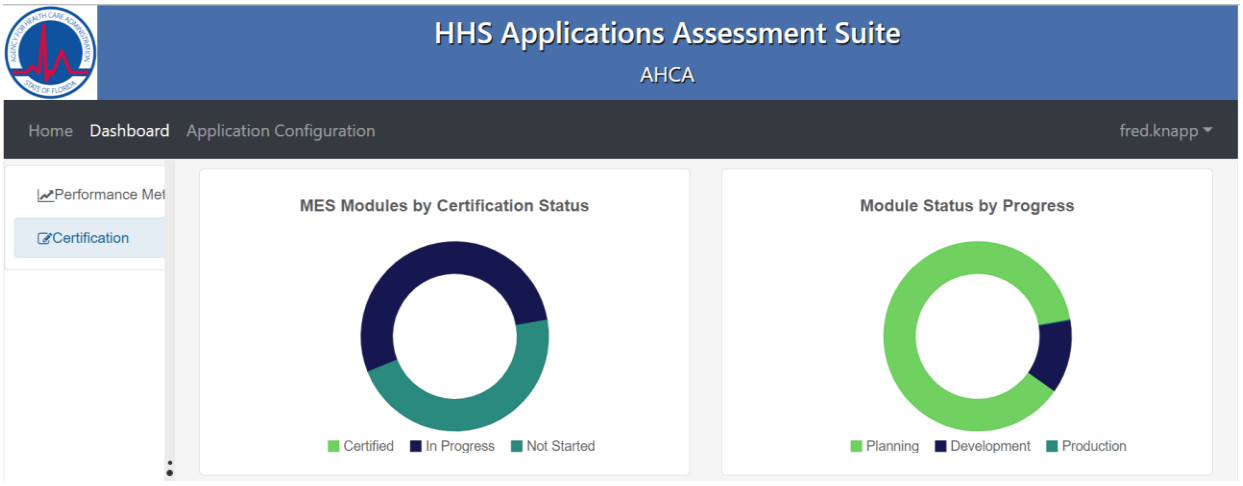

Exhibit 5-2: Sample Agency Source Pulse Certification Dashboard

Exhibit 5-3: Agency Source Pulse SMC Workflow Report below provides the status on steps and artifacts throughout the SMC life cycle. The report visual provides a simple way to track the progression of critical success factors through the certification planning, development, and production phases. The Certification Work Group will utilize Source Pulse workflow capabilities to monitor tasks assigned to individual users to ensure timely compliance and appropriate actions are taken to complete the task.

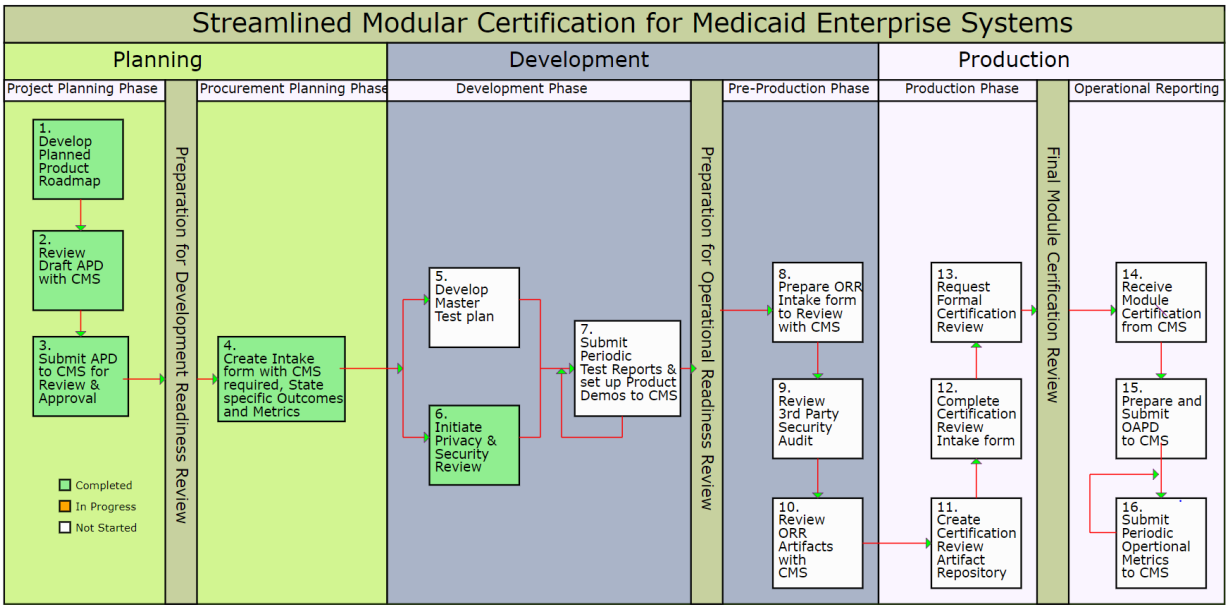

Exhibit 5-3: Agency Source Pulse SMC Workflow Report

5.2 Tracking and Reporting

5.2.1 Certification Related Risks, Issues, Action Items, and Decisions Tracking

Throughout the SMC, it is critical to track any related risks, issues, action items, and decisions related to a project. It is equally as critical to be able to track it for certification. The Agency Certification Lead uses the Agency-approved methods documented in Section 6 – *FX Project Planning Stage* and Section 8 – *Monitoring and Controlling* of the *P-2: FX Project Management Standards* to manage and track risks, issues, action items, and decisions for certification.

Certification related risks, issues, action items, and decisions will be visible to all project stakeholders and will help to ensure that items will be escalated when necessary. This will be critical especially for producing the CMS Monthly Reports, deciding when to schedule reviews with CMS, or when the Agency must respond to follow up requests from the CMS CR Team after reviews.

Action items that come out of the ORR and CR reviews will be logged and managed in a separate action log due as described in Section 4.5.3 – *Execution* due to the quick turnaround time, they will be entered into the global list after the review is complete. Any open items will be logged and tracked in the Action Items Log. Depending on the criticality it can also be elevated to a risk as described in the *P-2: FX Project Management Standards*.

The Certification Work Group tasks will not be logged as action items unless they are not acted upon within a reasonable amount of time or due to unresponsiveness. If this occurs, they will be elevated to the Action Item Log to get visibility and closure. If not addressed as an action item, it will be escalated to a risk as described in the *O-1: SEAS Management Plan*.

5.2.2 Integrated Certification Project Schedule

The IS/IP Vendor is responsible for managing the integrated schedule. This includes monitoring all certification schedules that are developed by all FX vendors including the Agency and Certification Work Group owned Certification activities and tasks throughout the SMC of each FX solution. Tasks will need to be detailed to the level necessary to track Certification progress of each artifact and evidence collection. It is imperative for all FX vendors to collaborate to develop a detailed schedule to allow the Agency to be able to track Certification progress.

With the large number of artifacts required for the two reviews, it is critical that the Certification Work Group and the Agency have a way to track who is responsible for the development of artifacts, evidence identification, metrics, and collection in addition to the numerous other tasks associated with planning for the execution of the reviews with the CMS. This will be a critical area that will help achieve these monitoring goals especially when more than one FX module is in development at the same time. Understanding and knowing the progress being made toward the development, and the completion of various required reviews, also helps to track contractual requirements and overall Certification readiness.

5.2.3 Stoplight Reports

Stoplight reports are a quick and effortless way to communicate the status of artifact collection at an enterprise level. This information, which contains high-level information, helps the Agency identify potential delays in the schedule. The Source Pulse certification tool procured by the Agency will track certification activities and notify appropriate staff when an activity is complete. The tool includes dashboards to reflect the status and the progress of work tasks related to certification artifacts. The Certification Work Group shall work with the Agency and Source Pulse to refine reports.

5.2.4 MITA Maturity Monitoring for FX Modules

Each FX solution is monitored closely to understand the changes that will result in MITA Maturity to the Medicaid enterprise. Monitoring the advancements throughout the SMC helps with updating the MITA State Self-Assessment (SS-A).

Under current regulations at 42 C.F.R. §433.112(b)(11) and §433.116(b), (c), and (i), and guidance issued by CMS in 2014, states are required to submit a MITA SS-A in support of their request for enhanced federal matching for their MES expenditures. As part of CMS' focus on outcomes and reducing administrative burden, CMS will accept an alternative format for the MITA SS-A, if preferred by the Agency. In place of focusing on rating the maturity level of a state's MES across each MITA business area, the SS-A could include the following information:

- Current operational problems and risks, challenges, and limitations of the existing system or module
- Which Medicaid program goals are impacted by the existing system or module limitations and the nature of the impact
- Definition of what success looks like in the To-Be state and how it will be measured

The Agency contracted with Source Pulse's nonproprietary MITA tracking tool and implemented it with the functionality to automatically pull reports of the data collected during the SS-A before and after the implementation of each FX module. **Exhibit 5-4: Example MITA Maturity Level Tracking** below is a sample report that can be developed using the SS-A data. This example is for the Operations Management MITA Business Area, which illustrates the maturity level changes over three SS-As conducted over the course of six years. In this example, four processes in the Operations Management MITA business area advanced.

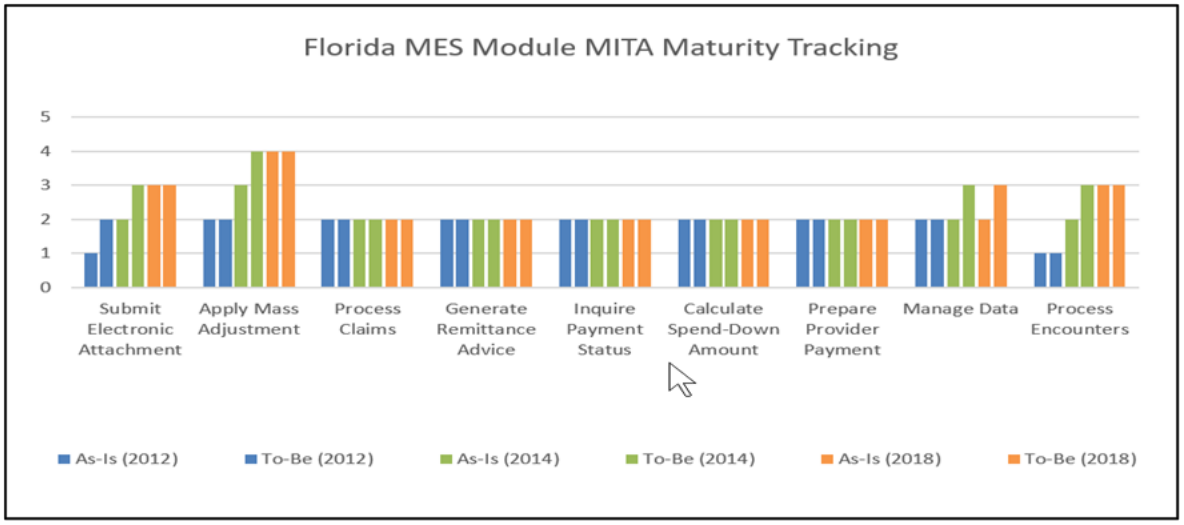

Exhibit 5-4: Example MITA Maturity Level Tracking

Considering the new guidance issued by CMS, the Agency will need to decide to continue to monitor MITA maturity using the traditional MITA SS-A process or align to simplified outcomes-based method proposed as an alternative by CMS to track MITA business process improvements.

SECTION 6 UPDATES AND IMPACT ANALYSIS

6.1 OUTCOMES-BASED AND SMC UPDATE PROCESS

The Agency, with support from the SEAS Vendor, is responsible for monitoring federal publications, notices, and websites for Medicaid Certification guidance and certification updates. Should there be any updates throughout the life of the FX Project, the SEAS Vendor will support the Agency in analyzing the information and conducting a gap analysis of the change impacts.

Intended outcomes and metrics are likely to evolve over time. CMS launched a Certification Repository on GitHub8 for additional materials, including identifying the specific outcomes derived from regulatory requirements, state-proposed outcomes, and metrics. The CMS Certification Repository on GitHub provides a collaborative space where states can learn, share, and contribute information about the MES Certification process and its related documentation. CMS created this repository for CMS, states, and vendors to:

- Access current information about CMS-required outcomes and recommended metrics
- Create and contribute to a community of state-specific outcomes and metrics
- Access examples of well-defined outcomes and metrics

The Certification Repository on GitHub provides access to resources such as certification guidance, information about the regulatory conditions for enhanced funding, outcomes, metrics, and related supporting evidence/examples to help inform how states approach their IT investment planning, development, operations, and certification. From this site the Agency, with support from the Certification Work Group, will access the latest-and-greatest information about CMS-required outcomes and recommended metrics as well as view CMS approved state-specific outcomes and metrics.

There are occasions when the changes have little to no impact and other times when there are large impacts that may require changes in vendor scope and request for additional federal funding. Once the gap analysis is completed, the Certification Work Group prepares a Certification Analysis Summary document and delivers it to the Agency who is responsible for reviewing the analysis and providing feedback to the work group. In addition to providing feedback, the Agency is also responsible for assessing if any changes to the Certification Training Curriculum are warranted.

Once the Certification Work Group receives feedback from the Agency, the Certification Work Group is responsible for assessing certification tasks, scope changes, and potential changes for other vendors and tools that support certification and then present the recommendations to the Agency for action. When a decision is made on the change by the Agency, the Certification Lead follows the Agency-approved process for monitoring and controlling change and monitoring and controlling decisions outlined in Section 8 – *Monitoring and Controlling* of the *P-2: FX Project Management Standards*. The Agency works with the SEAS Vendor, IV&V

Vendor, IS/IP Vendor, and FX solution vendors to distribute any updates and communicate outcomes to all stakeholders.

APPENDICES

APPENDIX A – CONDITIONS FOR ENHANCED FUNDING

The information in the following table contains the Conditions for Enhanced Funding (CEF) described in 42 C.F.R. §433.112 that are applicable for all MES modules.

This table, combined with the applicable table(s) in Appendix B – *CMS-Required Outcomes* for Specific MES Modules, are a starting point for aligning the state's goals for a project with applicable CMS required outcomes.

Conditions for Enhanced Funding (CEF) Outcomes

REF #	CONDITION
1	▪ CMS determines the system is likely to provide more efficient, economical, and effective administration of the State plan.
2	▪ The system meets the system requirements, standards and conditions, and performance standards in Part 11 of the State Medicaid Manual, as periodically amended.
3	▪ The system is compatible with the claims processing and information retrieval systems used in the administration of Medicare for prompt eligibility verification and for processing claims for persons eligible for both programs.
4	▪ The system supports the data requirements of quality improvement organizations established under Part B of title XI of the Act.
5	▪ The State owns any software that is designed, developed, installed, or improved with 90 percent FFP.
6	▪ The Department has a royalty free, non-exclusive, and irrevocable license to reproduce, publish, or otherwise use and authorize others to use, for Federal Government purposes, software, modifications to software, and documentation that is designed, developed, installed, or enhanced with 90 percent FFP.
7	▪ The costs of the system are determined in accordance with 45 CFR 75, subpart E.
8	▪ The Medicaid agency agrees in writing to use the system for the period specified in the advance planning document approved by CMS or for any shorter period that CMS determines justifies the Federal funds invested.
9	▪ The agency agrees in writing that the information in the system will be safeguarded in accordance with subpart F, part 431 of this subchapter.
10	▪ Use a modular, flexible approach to systems development, including the use of open interfaces and exposed application programming interfaces; the separation of business rules from core programming, available in both human and machine-readable formats.
11	▪ Align to, and advance increasingly, in maturity for business, architecture, and data.

REF #	CONDITION
12	▪ The agency ensures alignment with, and incorporation of, industry standards adopted by the Office of the National Coordinator for Health IT in accordance with 45 CFR part 170, subpart B: The HIPAA privacy, security and transaction standards; accessibility standards established under section 508 of the Rehabilitation Act, or standards that provide greater accessibility for individuals with disabilities, and compliance with Federal civil rights laws; standards adopted by the Secretary under section 1104 of the Affordable Care Act; and standards and protocols adopted by the Secretary under section 1561 of the Affordable Care Act.
13	▪ Promote sharing, leverage, and reuse of Medicaid technologies and systems within and among States.
14	▪ Support accurate and timely processing and adjudications/eligibility determinations and effective communications with providers, beneficiaries, and the public.
15	▪ Produce transaction data, reports, and performance information that would contribute to program evaluation, continuous improvement in business operations, and transparency and accountability.
16	▪ The system supports seamless coordination and integration with the Marketplace, the Federal Data Services Hub, and allows interoperability with health information exchanges, public health agencies, human services programs, and community organizations providing outreach and enrollment assistance services as applicable.
17	▪ For E&E systems, the State must have delivered acceptable MAGI-based system functionality, demonstrated by performance testing and results based on critical success factors, with limited mitigations and workarounds.
18	▪ The State must submit plans that contain strategies for reducing the operational consequences of failure to meet applicable requirements for all major milestones and functionality. This should include, but not be limited to, the Disaster Recovery Plan and related Disaster Recovery Test results.
19	▪ The agency, in writing through the APD, must identify key state personnel by name, type and time commitment assigned to each project.
20	▪ Systems and modules developed, installed, or improved with 90 percent match must include documentation of components and procedures such that the systems could be operated by a variety of contractors or other users.
21	▪ For software systems and modules developed, installed, or improved with 90 percent match, the State must consider strategies to minimize the costs and difficulty of operating the software on alternate hardware or operating systems.
22	▪ Other conditions for compliance with existing statutory and regulatory requirements, issued through formal guidance procedures, determined by the Secretary to be necessary to update and ensure proper implementation of those existing requirements.

APPENDIX B – CMS-REQUIRED OUTCOMES

The following tables contain the CMS-required outcomes for specific MES modules. These outcomes are aligned with statutory, regulatory and policy requirements that states must follow when implementing modules or capabilities. These are a starting point for aligning the state's project goals with applicable CMS outcomes. The list should be adjusted if any outcomes are deemed not applicable for a state project or if the state proposes other outcomes that are not covered in the applicable table(s) below.

Eligibility and Enrollment (E&E) Outcomes

REFERENCE #	OUTCOME	SOURCE(S)
EE1	The eligibility system receives, ingests, and processes the single-streamlined applications, change of circumstances, renewal forms, and any supporting documentation requested by the state (including telephonic signatures) from individuals, for all Medicaid eligibility groups and CHIP through online via multiple browsers, mail (paper), phone, and in-person (e.g., via kiosk) applications to support eligibility determination for all Insurance Affordability Programs (Federal Health Insurance Exchange), state Medicaid or CHIP, State-Based Marketplace (SBM), Basic Health Program (BHP).	42 CFR 435.907 42 CFR §435.916 42 CFR §436.901 (for Guam, Puerto Rico, and the Virgin Islands)
EE2	Individuals experience a user-friendly, dynamic, online application, such that subsequent questions are based on prior answers.	42 CFR 435.907 42 CFR §436.901 (for Guam, Puerto Rico, and the Virgin Islands)
EE3	Individuals eligible for automatic Medicaid eligibility are promptly enrolled (e.g., SSI recipients in 1634 states, individuals receiving a mandatory state supplement under a federally- or state-administered program, individuals receiving an optional State supplement per 42 CFR 435.230 and deemed newborns). (Automatic enrollment in Guam, Puerto Rico, and the U.S. Virgin Islands is required only for individuals receiving cash assistance under a state plan for OAA, AFDC, AB, APTD, or AABD, and deemed newborns.)	42 CFR 435.117 42 CFR 435.909 42 CFR 436.909 and 42 CFR 436.124 (for Guam, Puerto Rico, and the Virgin Islands)
EE4	The state correctly calculates income and household composition based on Modified Adjusted Gross Income (MAGI) and non-MAGI methodologies at application and renewal. Example business rules include subtracting five percentage points off FPL for applicable family size	42 CFR 435.603 42 CFR 436.601 and 42 CFR 436.811-814 (for Guam, Puerto Rico, and the Virgin Islands)

REFERENCE #	OUTCOME	SOURCE(S)
EE5	The eligibility system uses automated interfaces with electronic data sources to enable real-time or near real-time, no manual touch eligibility determinations. The data sources include (but are not limited to) SSA and the Department of Homeland Security (DHS) (directly or via the Federal Data Services Hub (FDSH)), state quarterly wage data, data from financial institutions for asset verification, Renewal and Redetermination Verification service through the FDSH, Public Assistance Reporting Information System (PARIS) to verify Medicaid coverage in other states.	42 CFR 435.940-965 42 CFR 435.945(d) 42 CFR 436.901 (for Guam, Puerto Rico, and the Virgin Islands)
EE6	Individuals who apply for Medicaid based on disability receive an eligibility determination within 90 days and all other applicants receive an eligibility determination within 45 days.	42 CFR 435.911-912 42 CFR 436.901 (for Guam, Puerto Rico, and the Virgin Islands)
EE7	Individuals are enrolled for up to 90 days if pending verification of citizenship or immigration status.	42 CFR 435.407 42 CFR 435.956 42 CFR 436.407 and 436.901 (for Guam, Puerto Rico, and the Virgin Islands)
EE8	Individuals are enrolled pending verification of SSN.	42 CFR 435.910 42 CFR 435.956(d) 42 CFR 436.901 (for Guam, Puerto Rico, and the Virgin Islands)
EE9	Individuals receive system-generated timely automated (versus manual) eligibility notices and request for additional information for eligibility determination, as necessary.	42 CFR 431.210-214 42 CFR 435.917-918 42 CFR 436.901 (for Guam, Puerto Rico, and the Virgin Islands)
EE10	Individuals receive electronic notices and alerts as applicable via their preferred mode of communication (e.g., email, text that notice is available in online account).	42 CFR 431.210-214 42 CFR 435.917-918 42 CFR 436.901 (for Guam, Puerto Rico, and the Virgin Islands)
EE11	Following an eligibility determination, the system promptly sends the beneficiary information to MMIS to complete enrollment into the appropriate delivery system (e.g., FFS, managed care).	42 CFR 435.914 42 CFR 436.901 (for Guam, Puerto Rico, and the Virgin Islands)
EE12	The system receives Presumptive Eligibility (PE) applications from all approved entities in an automated manner and facilitates eligibility termination if no full Medicaid application is received by the end of the month following the month of PE determination.	42 CFR Parts 435.1110
EE13	The system uses electronic data sources to confirm eligibility, wherever possible, to facilitate ex-parte renewals.	42 CFR 435.916 42 CFR 436.901 (for Guam, Puerto Rico, and the Virgin Islands)
EE14	If ex-parte renewal cannot be completed, the system can automatically generate pre-populated renewal forms and distribute those forms via individuals' preferred communication mode.	42 CFR 435.916 42 CFR 436.901 (for Guam, Puerto Rico, and the Virgin Islands)

REFERENCE #	OUTCOME	SOURCE(S)
EE15	The system applies an automated eligibility hierarchy that places an individual in the most advantageous group for which they are eligible at initial application and renewal.	42 CFR 435.404 42 CFR 436.404 (for Guam, Puerto Rico, and the Virgin Islands)
EE16	The system uses automated business rules to assign accurate eligibility categories for all the mandatory and relevant optional eligibility groups at initial application and renewal. Example business rules include: ▪ Correct identification of individuals aged 19-64 at or below 133 percent FPL (VIII group) ▪ Correct alignment of eligibility categories to FMAP rate	42 CFR 435.404 42 CFR 436.404 (for Guam, Puerto Rico, and the Virgin Islands)
EE17	Incarcerated individuals receive timely access to inpatient services and receive a timely and accurate eligibility determination upon release.	42 CFR 435.1009 42 CFR 436.1005 (for Guam, Puerto Rico, and the Virgin Islands)
EE18	Individuals whose coverage is limited to emergency services due to immigration status receive timely and accurate eligibility determination.	42 CFR 435.139 42 CFR 440.255(c) 42 CFR 436.128 (for Guam, Puerto Rico, and the Virgin Islands)
EE19	Individuals receive timely and accurate determinations of eligibility for the three months prior to the date of application if the individual would have been eligible and received Medicaid covered services.	42 CFR 435.915 42 CFR 436.901 (for Guam, Puerto Rico, and the Virgin Islands)
EE20	Individuals are promptly enrolled with the accurate effective date of eligibility in accordance with the approved State Plan.	42 CFR 435.915 42 CFR 436.901 (for Guam, Puerto Rico, and the Virgin Islands)
EE21	In states that have an integrated eligibility system with human services programs, the system is able to pend application for one program without having to do so for Medicaid or CHIP programs, if needed.	June 18, 2013, CMS Guidance on State Alternative Applications for Health Coverage
EE22	The state maintains a coordinated eligibility and enrollment process with all insurance affordability programs by supporting bi-directional data-sharing for application- related data and adjudication status with all relevant insurance affordability programs (FFE, CHIP, SBE if applicable, BHP if applicable).	42 CFR 435.1200
EE23	Account Transfer information for individuals applying at the FFE from a determination state is automatically ingested and the state promptly enrolls individuals determined eligible by the FFE.	42 CFR 435.1200
EE24	Account Transfer information for individuals applying at the FFE from an assessment state is automatically ingested and the state conducts only the remaining verifications necessary to complete the determination process for individuals assessed as potential eligible by the FFE.	42 CFR 435.1200
EE25	The system receives and responds to requests from the FFE in real-time to confirm whether an individual applying for coverage through the FFE currently has Minimum Essential Coverage through Medicaid or CHIP.	42 CFR 435.1200

Reference #	Outcome	Source(s)
EE26	Persons with disabilities or with Limited English Proficiency (LEP) can submit a single streamlined application with any necessary assistance (e.g., TTY for the hearing impaired for phone applications, and language assistance for persons with LEP).	42 CFR 435.905 42 CFR 435.908 42 CFR 436.901 (for Guam, Puerto Rico, and the Virgin Islands)
EE27	Beneficiaries and applicants can submit an appeal against an adverse action via multiple channels (e.g., online, phone, mail, in person) and the status and adjudication of an appeal can easily be accessed by necessary state staff and appellants.	42 CFR 431.221

Claims Processing Outcomes

Reference #	Outcome	Source(s)
CP1	The system receives, ingests, and retains claims, claims adjustments, and supporting documentation submitted both electronically and by paper in standard formats.	45 CFR 162.1102
CP2	The system performs comprehensive validation of claims and claims adjustments, including validity of services.	42 CFR 431.052 42 CFR 431.055 42 CFR 447.26 42 CFR 447.45(f) 45 CFR 162.1002 SMD Letter 10-017 SMM Part 11 Section 11300
CP3	The system confirms authorization for services that require prior approval to manage costs or ensure patient safety, and that the services provided are consistent with the authorization. The system accepts use of the authorization by multiple sequential providers during the period as allowed by state rules. Prior-authorization records stored by the system are correctly associated with the relevant claim(s).	SSA 1927(d)(5) 42 CFR 431.630 42 CFR 431.960 45 CFR 162.1302 SMM Part 4 SMM Part 11 Section 11325
CP4	The system correctly calculates payable amounts in accordance with the State Plan and logs accounts payable amounts for payment processing. The system accepts, adjusts, or denies claim line items and amounts and captures the applicable reason codes.	42 CFR 431.052

Reference #	Outcome	Source(s)
CP5	The state communicates claims status throughout the submission and payment processes and in response to inquiry. If there are correctable errors in a claims submission, the system suspends the claims, attaches pre-defined reason code(s) to suspended claims, and communicates those errors to the provider for correction. The system associates applicable error or reason code(s) for all statuses (e.g., rejected, suspended, denied, approved for payment, paid) and communicates those to the submitter. The system shows providers, case managers and members current submission status through one or more of the following: ▪ Automatic notices as appropriate based on claims decision or suspension. ▪ Explanation of Benefits (EOB). ▪ Providing prompt response to inquiries regarding the status of any claim through a variety of appropriate technologies, and tracking and monitoring responses to the inquiries. ▪ Application programming interface (API)	45 CFR Part 162.1402 (c) 45 CFR Part 162.1403 (a) & (b) 42 CFR 431.60 (a) & (b) SMM Part 11 Section 11325
CP6	The system tracks each claim throughout the adjudication process (including logging edits made to the claim) and retains transaction history to support claims processing, reporting, appeals, audits, and other uses.	42 CFR 447.45 42 CFR 431.17 SMM Part 11 Section 11325

Financial Management Outcomes

Reference #	Outcome	Source(s)
FM1	The system calculates FFS provider payment or recoupment amounts, as well as value-based and alternative payment models (APM), correctly and initiates payment or recoupment action as appropriate.	Section 1902(a)(37) of the Act 42 CFR 433.139 42 CFR 447.20 42 CFR 447.45 42 CFR 447.56 42 CFR 447.272
FM2	The system pays providers promptly via direct transfer and electronic remittance advice or by paper check and remittance advice if electronic means are not available.	42 CFR 447.45 42 CFR 447.46
FM3	The system supports the provider appeals by providing a financial history of the claim along with any adjustments to the provider's account resulting from an appeal.	42 CFR 431.152
FM4	The system accurately pays per member/per month capitation payments electronically in a timely fashion. Payments account for reconciliation of withholds, incentives, payment errors, beneficiary cost sharing, and any other term laid out in an MCO contract.	42 CFR 438 42 CFR 447.56(d)
FM5	The system accurately tallies recoupments by tracking repayments and amounts outstanding for individual transactions and in aggregate for a provider.	42 CFR 447

REFERENCE #	OUTCOME	SOURCE(S)
FM6	The state recovers third party liability (TPL) payments by: ▪ Tracking individual TPL transactions, repayments, outstanding amounts due, ▪ Aggregating by member, member type, provider, third party, and time period, ▪ Alerting state recovery units when appropriate, and ▪ Electronically transferring payments to the state.	42 CFR 433.139
FM7	The system processes drug rebates accurately and quickly.	42 CFR 447.509
FM8	State and federal entities receive timely and accurate financial reports (cost reporting, financial monitoring, and regulatory reporting), and record of all transactions according to state and federal accounting, transaction retention, and audit standards.	42 CFR 431.428 42 CFR 433.32
FM9	The system tracks that Medicaid premiums and cost sharing incurred by all individuals in the Medicaid household does not exceed an aggregate limit of five percent of the family's income. If the beneficiaries at risk of reaching the aggregate family limit, the system tracks each family's incurred premiums and cost sharing without relying on beneficiary documentation.	42 CFR 447.56(f)

Decision Support System (DSS)/Data Warehouse (DW) Outcomes

REFERENCE #	OUTCOME	SOURCE(S)
DSS/DW1	The system supports various business processes' reporting requirements	42 CFR 431.428
DSS/DW2	The solution includes analytical and reporting capabilities to support key policy decision making	42 CFR 433.112

Encounter Processing System (EPS) Outcomes

REFERENCE #	OUTCOME	SOURCE(S)
EPS1	The system ingests encounter data (submissions and re-submissions) from MCOs and sends quality transaction feedback back to the plans to ensure appropriate industry standard format. (Quality transaction checks include, but are not limited to completeness, missing information, formatting, and the TR3 implementation guide business rules validations).	42 CFR 438.242

REFERENCE #	OUTCOME	SOURCE(S)
EPS2	The system ingests encounter data (submissions and re-submissions) from managed care entities in compliance with HIPAA security and privacy standards and performing quality checks for completeness and accuracy before submitting to CMS using standardized formatting, such as ASC X12N 837, NCPDP and the ASC X12N 835, as appropriate. (Quality checks include, but are not limited to completeness, character types, missing information, formatting, duplicates, and business rules validations, such as payment to dis-enrolled providers, etc.).	42 CFR 438.604 42 CFR 438.818 42 CFR438.242
EPS3	The state includes submission requirements (timeliness, re-submissions, etc.), definitions, data specifications and standards, and consequences for non-compliance in its managed care contracts. The state enforces consequences for non-compliance.	42 CFR Part 438.3
EPS4	The state uses encounter data to calculate capitation rates and performs payment comparisons with FFS claims data.	42 CFR Part 438
EPS5	The state complies with federal reporting requirements.	42 CFR 438.818 42 CFR 438.242

Long Term Services & Supports (LTSS) Outcomes

REFERENCE #	OUTCOME	SOURCE(S)
LTSS1	LTSS system generates notifications including eligibility determination; termination of state waiver (30 days in advance); and inspections taking place in a beneficiary's home when a beneficiary receives services in his/her own home or the home of a relative (HCBS waiver for individuals sixty-five and older) (48 hours in advance).	42 CFR 441.307 42 CFR 441.356 42 CFR 441.365 42 CFR 431.206 42 CFR 431.210 42 CFR 433.112
LTSS2	LTSS systems stores proof of beneficiary consent to enroll in HCBS state plan or waiver-based programs.	42 CFR 441.301
LTSS3	LTSS system assigns, tracks, and changes beneficiary prioritization and waiver waitlist status.	42 CFR 433.112
LTSS4	LTSS system maintains a record of beneficiaries who have left the waiver program due to death or loss of eligibility for Medicaid under the State Plan to replace those beneficiaries with others on the waitlist.	42 CFR 441.305
LTSS5	LTSS system stores the person-centered plan, including any updates or changes containing all required information and consent signatures.	42 CFR 441.302
LTSS6	LTSS system supports conflict-free case management via role-based access, proper firewalls, and mitigation strategies that provide beneficiaries appropriate access to records.	HIPAA 42 CFR 441.301
LTSS7	LTSS System supports completion of CMS Form 372.	42 CFR 433.112 42 CFR 441.302

REFERENCE #	OUTCOME	SOURCE(S)
LTSS8	LTSS system collects and saves prior authorizations to exchange with MMIS as needed to prevent the provision of unnecessary or inappropriate services and supports.	42 CFR 441.301
LTSS9	LTSS system documents and tracks reportable events related but not limited to instances of abuse, neglect, exploitation, and unexplained death from case initiation to case closeout.	42 CFR 441.404 42 CFR 441.585 42 CFR Part 438 CMS Bulletin, Modifications to Quality Measures and Reporting in §1915(c) Home and Community-Based Waivers, March 12, 2014
LTSS10	LTSS system collects grievances related but not limited to instances of abuse, neglect, exploitation, and unexplained death from case initiation to case closeout.	42 CFR 441.464 42 CFR 441.555
LTSS11	LTSS system creates trend reports of critical incident causes and tracks trends of critical incidents after operational implementation of interventions/mitigations/corrective actions.	Application for a §1915(c) Home and Community- Based Waiver [Version 3.6, January 2019] Instructions, Technical Guide and Review Criteria p.242-243 (Appendix G-1-e) Modifications to Quality Measures and Reporting in §1915(c) Home and Community-Based Waivers, Page 10

Member Management Outcomes

REFERENCE #	OUTCOME	SOURCE(S)
MM1	The system auto-assigns managed care enrollees to appropriate managed care organizations, per state and federal regulations.	42 CFR 438.54
MM2	The system sends notice, or facilitates, to the enrolled member with an initial assignment, a reasonable period to change the selection, and appropriate information needed to make an informed choice. If no selection is made, the system either confirms the original assignment, or assigns the member to FFS.	42 CFR 438.10 42 CFR 438.54
MM3	The system disenrolls members at the request of the plan and in accordance with state procedures.	42 CFR 438.56(b) (c), and (d)
MM4	Disenrollments are effective in the system the first day of the second month following the request for disenrollment.	42 CFR 438.56(e)

REFERENCE #	OUTCOME	SOURCE(S)
MM5	The system notifies enrollees of their disenrollment rights at least 60 days before the start of each enrollment period. This notification is in writing.	42 CFR 438.56(f)
MM6	To prevent duplication of activities, enrollee's needs are captured by the system so that MCOs, PIHPs, and PAHPs can see and share the information (in accordance with privacy controls).	42 CFR 438.208(b)
MM7	The system allows beneficiaries or their representative to receive information through multiple channels including phone, Internet, in-person, and via auxiliary aids and services.	42 CFR 438.71
MM8	The state provides content required by 42 CFR 438.10, including but not limited to definitions for managed care and enrollee handbook, through a website maintained by the state.	42 CFR 438.10(c)
MM9	Potential enrollees are provided information about the state's managed care program when the individual become eligible or is required to enroll in a managed care program. The information includes, but is not limited to the right to disenroll, basic features of managed care, service area coverage, covered benefits, and provider directory and formulary information.	42 CFR 438.10(e)
MM10	The system maintains an up to date (updated at least annually) fee-for-service (FFS) or primary care case-management (PCCM) provider directory containing the following: ▪ Physician/provider ▪ Specialty ▪ Address and telephone number ▪ Whether the physician/provider is accepting new Medicaid patients (for PCCM providers), and ▪ The physician/provider's cultural capabilities and a list of languages supported (for PCCM providers).	Section 1902(a)(83) Section 1902(mm) SMD # 18-007
MM11	The system captures enough information such that the state can evaluate whether members have access to adequate networks. (Adequacy is based on the state's plan and federal regulations).	42 CFR 438.68

Prescription Drug Monitoring Program (PDMP) Outcomes

REFERENCE #	OUTCOME	SOURCE(S)
PDMP 1	Covered providers have near real-time access to: a. Information regarding Medicaid beneficiary's prescription drug history. b. The number and type of controlled substances prescribed to and filled for the covered individual during at least the most recent 12-month period. c. The name, location, and contact information (or other identifying number selected by the state, such as a national provider identifier issued by the CMS National Plan and Provider Enumeration System) of each covered provider who prescribed a controlled substance to the covered individual during at least the most recent 12-month period.	Section 1944(b) of the Act Section 5042 – Medicaid PARTNERSHIP Act CMS FAQs-SUPPORT for Patients and Communities Act
PDMP 2	Providers can easily use the PDMP information though workflow integration, which may include electronic prescribing system for controlled substances.	Section 1944(b) of the Act Section 5042 – Medicaid PARTNERSHIP Act CMS FAQs-SUPPORT for Patients and Communities Act
PDMP 3	The state has data-sharing agreements with all contiguous states to track patients, prescribers, and prescriptions across state lines.	Section 1944(f) of the Act Section 5042 – Medicaid PARTNERSHIP Act CMS FAQs-SUPPORT for Patients and Communities Act
PDMP 4	The state medical and pharmacy directors and any designee has access to the PDMP information in an electronic format based on data-sharing agreements in place (subject to state law).	Section 1944(b) of the Act Section 5042 – Medicaid PARTNERSHIP Act CMS FAQs-SUPPORT for Patients and Communities Act
PDMP 5	The state produces data for the reports that are required to be submitted in the Annual Report to HHS.	Section 1944(e) of the Act Section 5042 – Medicaid PARTNERSHIP Act 42 CFR 433.112(b)(15) CMS FAQs-SUPPORT for Patients and Communities Act
PDMP 6	The system produces reports to contribute to reports to HHS by the State Drug Utilization Review (DUR) Board and for program evaluation, continuous improvement in business operations, transparency, and accountability, as well as identify patterns of fraud, abuse, gross overuse, excessive utilization related to limitations identified by the state, inappropriate or medically unnecessary care, or prescribing or billing practices that indicate abuse or excessive utilization among Medicaid physicians, pharmacists and enrollees associated with specific drugs or groups of drugs.	Section 1944 (e)(1) of the Act Section 1927(g)(2)(B) and (g)(3)(D) of the Act Section 1004 of the SUPPORT Act 42 CFR 433.112(b)(15) CMS FAQs-SUPPORT for Patients and Communities Act Centers for Disease Control

Pharmacy Benefit Management (PBM) Outcomes

REFERENCE #	OUTCOME	SOURCE(S)
PBM1	The system adjudicates claims within established time parameters to ensure timely pharmacy claims payments.	Section 1927(h) of the SSA 42 CFR 456.722
PBM2	The system adjudicates claims accurately within established parameters. The module can be configured to provide authority/ability to override a reject/edit/denied claim and then resubmit to ensure timely provider claims payments.	42 CFR 456.722
PBM3	The system captures the necessary data to ensure timely processing of manufacturer rebates as well as the capability to track rebates to promote beneficiary cost savings.	Section 1927 of the SSA 42 CFR 447.509
PBM4	The system has the capability to support cost savings by capturing, storing, and transferring data to the payment process system to generate invoices of participating drug manufacturers within 60 days of the end of each quarter.	Section 1927(b)(2) of the SSA 42 CFR 447.520 42 CFR 447.511
PBM5	The system supports cost savings by enabling the tracking, monitoring, and reporting of manufacturer's pharmacy drugs and rebate savings.	Section 1927(b)(2) of the SSA 42 CFR 447.520 42 CFR 447.511
PBM6	The system enables the beneficiary to have timely access to medication if the system has the capability to perform prior authorization and provide a response by telephone or other telecommunication devices within 24 hours of a request and provides for the dispensing of at least 72-hour supply of a covered outpatient prescription drug in an emergency situation (unless excluded under the SSA).	Section 1927(d)(5) of the SSA
PBM7	The system supports CMS oversight of the safe, effective, and appropriate dispensing of medications by enabling the capability to provide data to support the creation of the CMS annual report on the operation and status of the state's DUR program.	Section 1927(g)(3)(D) of the SSA Section 1944(e)(1) of the SSA 42 CFR 456.712
PBM8	The system supports the safe, effective, and appropriate dispensing of medications by enabling the capability to provide point-of-sale or point of distribution prospective review of drug therapy based upon predetermined standards, including standards for counseling.	Section 1927 (g) of the SSA 42 CFR 456.703, 42 CFR 456.705(b) 42 CFR 456.709
PBM9	The system supports the identification of patterns of fraud, abuse, gross overuse, or inappropriate or medically unnecessary care, or prescribing or billing practices indicating abuse or excessive utilization among physicians, pharmacists and individuals receiving benefits by enabling the collection of pharmacy data to be used in retrospective drug utilization reviews.	Section 1927 (g) of the SSA 42 CFR 456.703, 42 CFR 456.705(b) 42 CFR 456.709

Provider Management Outcomes

REFERENCE #	OUTCOME	SOURCE(S)
PM1	A provider can initiate, save, and apply to be a Medicaid provider.	42 CFR 455.410(a)
PM2	A state user can view screening results from other authorized agencies (Medicare, CHIP, other related agencies) to approve provider if applicable.	42 CFR 455.410(c)
PM3	A state user can verify that any provider purporting to be licensed in a state is licensed by such state and confirm that the provider's license has not expired and that there are no current limitations on the provider's license ensure valid licenses for a provider.	42 CFR 455.412
PM4	The system tracks the provider enrollment period to ensure that the state initiates provider revalidation at least every five years.	42 CFR 455.414
PM5	A state user (or the system, based on automated business rules) must terminate or deny a provider's enrollment upon certain conditions (refer to the specific regulatory requirements conditions in 42CFR455.416).	42 CFR 455.416
PM6	After deactivation, a provider seeking reactivation must be re-screened by the state and submit payment of associated application fees before their enrollment is reactivated.	42 CFR 455.420
PM7	A provider can appeal a termination or denial decision, and a state user can monitor the appeal process and resolution including nursing homes and ICFs/IID.	42 CFR 455.422
PM8	A state user can manage information for mandatory pre-enrollment and post-enrollment site visits conducted on a provider in a moderate or high-risk category.	42 CFR 455.432(a)
PM9	A state user can view the status of criminal background checks, fingerprinting, and site visits for a provider as required based on their risk level and state law.	42 CFR 455.434
PM10	The system checks appropriate databases to confirm a provider's identity and exclusion status for enrollment and reenrollment and conducts routine checks using federal databases including Social Security Administration's Death Master File, the National Plan and Provider Enumeration System (NPPES), the List of Excluded Individuals/Entities (LEIE), and the Excluded Parties List System (EPLS). Authorized users can view the results of the data matches as needed.	42 CFR 455.436
PM 11	A state user can assign and screen all applications by a risk categorization of limited, moderate, or high for a provider at the time of new application, re- enrollment, or re-validation of enrollment. A state user can adjust a provider's risk level due to payment suspension or moratorium.	42 CFR 455.450

REFERENCE #	OUTCOME	SOURCE(S)
PM 12	The system can collect application fees. A state user ensures any applicable application fee is collected before executing a provider agreement.	42 CFR 455.460
PM 13	A state user can set CMS and state-imposed temporary moratoria on new providers or provider types in six-month increments.	42 CFR 455.470
PM 14	A state user can determine network adequacy based upon federal regulations and state plan.	42 CFR 438.68
PM 15	A state user, and/or the system, can send and receive provider sanction and termination information shared from other states and Medicare to determine continued enrollment for providers.	42 CFR 455.416(c)
PM 16	The system can generate relevant notices or communications to providers to include, but not limited to, application status, requests for additional information, re-enrollment termination, investigations of fraud, suspension of payment in cases of fraud.	42 CFR 455.23
PM 17	A state user can report required information about fraud and abuse to the appropriate officials.	42 CFR 455.17
PM 18	The system, or a state user, can suspend payment to providers in cases of fraud.	42 CFR 455.23
PM 19	A state user can view provider agreements and disclosures as required by federal and state regulations.	42 CFR 455.104 42 CFR 455.105 42 CFR 455.106 42 CFR 455.107
PM 20	A state user can view information from a managed care plan describing changes in a network provider's circumstances that may affect the provider's eligibility to participate in Medicaid, including termination of the provider agreement.	42 CFR 438.608(a)
PM 21	A beneficiary can view and search a provider directory.	42 CFR 438.10(h)

Third Party Liability (TPL) Outcomes

REFERENCE #	OUTCOME	SOURCE(S)
TPL1	The system does the following: ▪ Records third parties, ▪ Determines the liability of third parties, ▪ Avoids payment of third-party claims, ▪ Recovers reimbursement from third parties after Medicaid claims payment, and ▪ Records information and actions related to the plan.	42 CFR 433.138(k)(2)(i)
TPL2	The system records other health insurance information at the time of application or renewal for Medicaid eligibility that would be useful in identifying legally liable third-party resources.	Section 1902(a)(25) of the Act 42 CFR 433.136 42 CFR 433.137 42 CFR 433.138

REFERENCE #	OUTCOME	SOURCE(S)
TPL3	The system uses electronic exchange state wage information collection agency The system(s) regularly updates the member file with any third-party liability information, how long it is valid, and for what services, through regular automated checks with these databases.	42 CFR 433.138(d) and (f) 42 CFR 435.4 State Plan
TPL4	The system rejects and returns to the provider for a determination of the amount of liability for all claims for which the probable existence of third-party liability is established at the time the claim is filed.	42 CFR 433.139(b)
TPL5	For claims identified with a third-party liability and designated as “mandatory pay and chase,” the system makes appropriate payments and identifies such claims for future recovery. (Examples include preventive pediatric services provided to children, or medical child support from an absent parent.)	Section 1902(a)(25) of the Act 42 CFR 433.139(b)(3)(ii)
TPL6	The system(s) supports providing up to one hundred days to pay claims related to medical support enforcement, preventive pediatric services, labor and delivery, and postpartum care that are subject to "pay and chase." If a state cannot differentiate the costs for prenatal services from labor and delivery on the claim, it will have to cost avoid the entire claim.	Bipartisan Budget Act of 2018, Sec. 53102 Section 1902(a)(25) of the Act CMCS Informational Bulleting (CIB) November 14, 2019 (pg. 2)
TPL7	The system identifies paid claims that contain diagnosis codes indicative of trauma, injury, poisoning, and other consequences of external causes on a routine and timely basis for the purposes of determining legal liability of third parties.	42 CFR 433.138(e) and (f)
TPL8	The system identifies probable TPL within 60 days after the end of the month in which payment has been made (unless there is an approved waiver to not recoup funds).	42 CFR 433.139(d)
TPL9	The system can generate reports on data exchanges and trauma codes so that the state can evaluate its TPL identification process.	42 CFR 433.138(j)
TPL10	The system enables the agency to seek reimbursement from a liable third party on all claims for which it is cost effective.	42 CFR 433.139(f)
TPL11	As determined by the state policies, system(s) enables the state to manage and oversee TPL recoveries made by its MCOs.	COB/TPL Training and Handbook- 2020 (pg. 53-55)
TPL12	Appropriate privacy and security controls are in place so that information exchanged with other agencies is safeguarded.	42 CFR 433.138(h)
TPL13	The system tracks TPL reimbursements received so that the state can reimburse the federal government in accordance with the state's FMAP.	42 CFR 433.140 (c)

Program Integrity (PI)

REFERENCE #	OUTCOME	SOURCE(S)
CP2	The system performs comprehensive validation of claims and claims adjustments, including validity of services.	42 CFR 431.052 42 CFR 431.055 42 CFR 447.26 42 CFR 447.45(f) 45 CFR 162.1002 SMD Letter 10-017 SMM Part 11 Section 11300
FM5	The system accurately tallies recoupments by tracking repayments and amounts outstanding for individual transactions and in aggregate for a provider.	42 CFR 447
PBM9	The system supports the identification of patterns of fraud, abuse, gross overuse, or inappropriate or medically unnecessary care, or prescribing or billing practices indicating abuse or excessive utilization among physicians, pharmacists and individuals receiving benefits by enabling the collection of pharmacy data to be used in retrospective drug utilization reviews.	Section 1927 (g) of the SSA 42 CFR 456.703 42 CFR 456.705(b) 42 CFR 456.709
PI1	The system can check member record to ensure the member on the claim was enrolled in the Medicaid program and the benefit was covered at the time of service. Membership enrollment records the system is checking against are updated daily. **Applicable to CP*	42 CFR 455.1(a)
PI2	System provides a method for identifying suspected inappropriate services and incorrect billing. **Applicable to CP, E&E, MM*	42 CFR 455.13
PI3	System can verify with beneficiaries whether services billed by providers were received.	42 CFR 455.20
PI4	System can suspend Medicaid payments in whole or in part to providers for whom the agency has determined there is a credible allegation of fraud and is conducting an investigation and other activities, including provide notice of suspension; referrals to MFCU; and documentation and record retention.	42 CFR 455.23(a-g)
PI5	System can perform provider lock-in for identified members responsible for fraudulent activity, or that have utilized services in excess of what is medically necessary (as defined by state guidelines) and can send notice to the impacted member and the appropriate provider. **Applicable to PM*	42 CFR 431.54(f)
PI6	System can recover improper payments by: (a) Tracking repayments and outstanding amounts due at an individual transaction level as well as aggregating by provider, time period (b) Supporting electronic transfer back to the state (c) Temporarily limiting future payments to provider(s) who have an outstanding recovery balance.	42 CFR 447 42 CFR 431.1002 42 CFR 433.300-322

REFERENCE #	OUTCOME	SOURCE(S)
PI7	System can complete the required independent certified audit of Disproportionate Share Hospital (DSH) payments for each Medicaid State Plan rate year using payment and utilization information.	42 CFR 455.304(d)
PI8	System can reject claims for items or services that were ordered or referred that do not contain a National Provider Identifier. **Applicable to CP*	42 CFR 455.440
PI9	System can support activities conducted by Medicaid RACs can including review all claims submitted by providers of items or services for which payment has been made to identify underpayments and overpayments and recoup overpayments, as necessary.	42 CFR 455.506
PI10	System can refer all cases of suspected provider fraud to the state's Medicaid Fraud Unit and provide access to Case Tracking as applicable.	42 CFR 455.21(a)
PI11	System can sample and review active cases, including negative cases, to determine eligibility errors in accordance with the state's MEQC pilot planning document.	42 CFR 431.814(b)
PI12	System can submit following information to CMS for among other purposes, estimating improper payments in Medicaid and CHIP, that include, but are not limited to— (1) Adjudicated fee-for-service or managed care claims information, or both, on a quarterly basis, from the review year; (2) Upon request from CMS, provider contact information that has been verified by the State as current; (3) All medical, eligibility, and other related policies in effect, and any quarterly policy updates; (4) Current managed care contracts, rate information, and any quarterly updates applicable to the review year; (5) Data processing systems manuals; (6) Repricing information for claims that are determined during the review to have been improperly paid; (7) Information on claims that were selected as part of the sample, but changed in substance after selection, for example, successful provider appeals; (8) Adjustments made within 60 days of the adjudication dates for the original claims or line items, with sufficient information to indicate the nature of the adjustments and to match the adjustments to the original claims or line items; (9) Case documentation to support the eligibility review, as requested by CMS; (10) A corrective action plan for purposes of reducing erroneous payments in FFS, managed care, and eligibility; and (11) Other information that the Secretary determines is necessary for these purposes.	42 CFR 431.970

Reference #	Outcome	Source(s)
PM11	System can assign and screen all applications by a risk categorization of limited, moderate, or high for a provider at the time of new application, re- enrollment, or re-validation of enrollment. A state user can adjust a provider's risk level due to payment suspension or moratorium.	42 CFR 455.450
PM17	A state user can report required information about fraud and abuse to the appropriate officials.	42 CFR 455.17
PM18	The system can suspend payment to providers in cases of fraud.	42 CFR 455.23

Health Information Exchange (HIE)

Please note that, although there are not CMS-required outcomes for Health Information Exchange (HIE) modules, all other Streamlined Modular Certification requirements apply (e.g., the CEF, state-specific outcomes).

APPENDIX C – REQUIRED ARTIFACTS LIST

The following table contains the list of artifacts required for an Operational Readiness Review (ORR) and Certification Review (CR). Minimum requirements for each document are given, but this is not an exhaustive list of what is typically included in each artifact. States are encouraged to add elements, as appropriate.

DOCUMENT/ARTIFACT	MINIMUM REQUIRED CONTENT AND NOTES	REQUIRED AT ORR, CR, OR BOTH
	Entry Criteria for CR	
Official Certification Request Letter	▪ The date at which the system became the system of record ▪ A copy of the state's letter to the vendor contractor or state development team accepting the system/modules(s) ▪ The effective date for which the state is requesting certification approval ▪ A proposed timeframe for the CR ▪ A declaration that the state's system meets all the requirements of law and regulation including 42 CFR 433.117 for all periods for which the 75 percent FFP is being claimed ▪ The state maintains monthly production submissions of T-MSIS files. (States will be deemed out of compliance with timeliness requirements if T-MSIS files are submitted later than one month after the T- MSIS reporting period.) ▪ The state maintains complete and accurate historical T-MSIS data for program evaluation and the continuous improvement in business operations. ▪ The state can demonstrate that data quality issues are meeting the targets for Outcomes Based Assessment (OBA) critical priority data quality checks, high priority data quality checks, and the expenditure data content category. The state should also demonstrate they are working in good faith to resolve such issues. CMS will consider the state out of compliance with TMSIS requirements if it is not meeting the targets for OBA criteria in critical priority data quality checks, high priority data quality checks, and the expenditure data content category and/or the state is not working in good faith to resolve any identified data quality issues. ▪ The state meets all requirements outlined in the T-MSIS Reporting - Standard Operating Procedures (SOP) for any Large System Enhancements (LSEs) affecting T-MSIS reporting ▪ Is ready for CMS certification, based on the system's performance in demonstrating achievement of outcomes	Submitted to begin the CR process
System Acceptance Letter	▪ A copy of the state's acceptance letter addressed to the system developer indicating that the system or module was accepted as fully operational at least six months prior to the requested certification review date	Submitted to begin the CR process

DOCUMENT/ARTIFACT	MINIMUM REQUIRED CONTENT AND NOTES	REQUIRED AT ORR, CR, OR BOTH
Project Management		
Monthly Project Status Reports	Indicators of Project Health, which are: ▪ **Roadmap** - A product roadmap identifying current, planned, and future functionality and milestones ▪ **Progress Tracking** - A regular report measuring developmental progress and progress towards achieving outcomes. ▪ **User Feedback** - A reporting showing how user feedback is regularly incorporated into development ▪ **Defect and Risk List** - Known defects and risks that may cause delays and any mitigations or workarounds ▪ **Product Demos** - Demo of functionality/features, or regular report of code/feature releases ▪ **Testing Process** - A documented testing process aligned with CMS ***Testing Guidance Framework***	Both
Technical		
Master Test Plan and Testing Results	▪ State testing should be informed by the ***Testing Guidance Framework*** document, which offers MES testing expectations and recommendations ▪ Test results should not only validate the iterative delivery of system functionality, but also confirm that the system will produce metrics associated with outcomes ▪ Testing should be as automated and self-documenting as possible (e.g., continuous unit testing) ▪ Test results should be mapped to functionality, with an acceptance testing report for each user story/use ▪ case	Both
Deployment Plan	▪ Description of the release and deployment of a new/updated module agreed upon by all stakeholders ▪ Compatibility between all the related assets and service components within each release package is verified ▪ Via the configuration management process in place, verify that the integrity of release packages and their constituent components are maintained throughout the transition activities ▪ Define how release and deployment packages can be tracked, installed, tested, verified, and/or uninstalled or backed out, if appropriate ▪ Define how deviations, risks, and issues related to the new or updated module are recorded and how corrective actions are ensured ▪ Define how the transfer of knowledge will occur to enable end users to optimize their use of the new/updated module to support their business activities ▪ Define the transfer of skills and knowledge to operations staff to enable them to effectively and efficiently deliver, support and maintain the new/updated module according to the ▪ documented Service Level Agreements (SLAs)	ORR

DOCUMENT/ARTIFACT	MINIMUM REQUIRED CONTENT AND NOTES	REQUIRED AT ORR, CR, OR BOTH
Defect and Risk List	▪ Current defect list, with frequency, severity (inclusive of all critical and high defects), and associated implementation timelines ▪ Defect entries should include information about the operational impact ▪ Risks should be accompanied by a mitigation/resolution or a risk acceptance statement	Both
Independent Security Audit	Independent, third-party security and privacy controls assessment report that covers compliance with the following: ▪ NIST SP 800-171 and/or NIST SP 800-53 standards and all relevant controls in HIPAA; ▪ aligning Health Care Industry Security Approaches pursuant to Cybersecurity Act of 2015, Section 405(d); and ▪ the Open Web Application Security Project Top 10. Privacy and Security related risks should be identified using NIST SP 800-30 Revision 1. The third-party audit should include, but need not be limited to, a penetration test, a review of all HIPAA compliance areas: user access control; information disclosure; audit trail; data transfers; and information on correct data use (role-based testing of use). The audit should cover adequate audit trails and logs (e.g., ID, access level, action performed, etc.). The audit should also cover encryption of data at rest, in audit logs, and in transit between workstations and mobile devices (where applicable), to external locations and to offline storage.	ORR

APPENDIX D – FRAMEWORK FOR THE INDEPENDENT THIRD-PARTY SECURITY AND PRIVACY ASSESSMENT GUIDELINES FOR MEDICAID ENTERPRISE SYSTEMS

1. Introduction

The state Medicaid Enterprise System (MES) is the custodian of sensitive information, such as Personally Identifiable Information (PII) and Protected Health Information (PHI), for millions of individuals receiving coverage through Medicaid and the Children's Health Insurance Program. The state and its business partners share the responsibility for ensuring the protection of this sensitive information. States and their respective business partners must demonstrate continuous monitoring and regular security and privacy control testing through an independent security and privacy assessment.

This guidance document provides an overview of the independent security and privacy assessment requirements. It contains guidelines for both cloud-based and non-cloud-based environments. The state can tailor guidelines based on the solution implementation. This guidance is applicable for the states that work directly with a third-party assessment vendor or a MES solution vendor working with a third- party assessment vendor.

1.1 Requirements Background

Pursuant to the Health Insurance Portability and Accountability Act (HIPAA) and implementing regulations at 45 Code of Federal Regulations (CFR) §164.308(a)(1)(ii)(A), conducting a risk analysis is the first step in identifying and implementing safeguards that comply with and carry out the standards and implementation specifications of HIPAA. Therefore, a risk analysis is foundational, and must be completed to assist organizations in identifying and implementing the most effective and appropriate administrative, physical, and technical safeguards of PHI/PII. Furthermore, the National Institute of Standards and Technology (NIST), Security Assessments Control, CA-2, requires an independent assessment of all applicable security and privacy controls. States should have a fully completed and implemented System Security/Privacy Plan (SSP) before starting the security and privacy assessment. The Centers for Medicare & Medicaid Services (CMS) highly recommends that an independent third- party assessor conduct the assessment.

If the state has adopted a framework similar or complementary to NIST that supports the HIPAA requirements, then the state may use that framework to do risk analysis.

If NIST is not the core framework of the third-party assessor, then the third-party assessor needs to provide a translation or crosswalk of the supported framework to the NIST controls.

1.2 Purpose

This guidance document provides an overview of the independent security and privacy assessment requirements through the following objectives:

- Define the independent third-party assessor (Section 2).
- Explain the scope of the security and privacy control assessment and provide assessment planning considerations (Section 3).
- Provide a basic security and privacy control assessment methodology (Section 4).
- Summarize security and privacy assessment reporting (Section 5).

This document is not intended to provide detailed guidance for assessment planning and performance, nor for state planning and action to address assessment findings.

2. Independent Third-Party Security and Privacy Assessor

Pursuant to 45 CFR § 95.621(f) and consistent with State Medicaid Director Letter #06-022, CMS requires that state agencies employ assessors or assessment teams to conduct periodic security and privacy control assessments of the MES environment. The assessor's role is to provide an independent assessment of the effectiveness of implementations of security and privacy safeguards for the MES environment and to maintain the integrity of the assessment process. Alternatively, states can require vendors to have their own independent third-party assessment and provide assessment results.

2.1 Assessor Independence and Objectivity

An assessor must be free from any real or perceived conflicts of interest, including being free from personal, external, and organizational impairments to independence, or the appearance of such impairments to independence. An assessor is considered independent if there is no perceived or actual conflict of interest involving the developmental, operational, financial, and/or management chain associated with the system and the determination of security and privacy control effectiveness.

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-39, *Managing Information Security Risk*, states that:

> "Assessor independence is an important factor in: (i) preserving the impartial and unbiased nature of the assessment process; (ii) determining the credibility of the security assessment results; and (iii) ensuring that the authorizing official receives the most objective information possible in order to make an informed, risk-based, authorization decision."

2.2 Assessor Qualifications

Experience and competencies are important factors in selecting an assessor. CMS recommends that the MES assessor possess a combination of privacy and security experience and relevant assessment certifications. Examples of acceptable privacy and security experience may include, but are not limited to:

- Reviewing compliance with HIPAA security standards
- Reviewing compliance with the most current NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, or the most current NIST SP 800-171, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations
- Reviewing compliance with the Minimal Acceptable Risk Standards for Exchange
- Reviewing compliance with the Federal Information Security Management Act
- Participating in the Federal Risk and Authorization Management Program (FedRAMP)-certified third-party assessment organization
- Reviewing compliance with the Statement on Standards for Attestation Engagements 16
- Experience assessing the implementation of the Center for Internet Security (CIS) benchmarks
- Reviewing compliance with the Open Web Application Security Project (OWASP).

The assessor organizations should have relevant security and privacy accreditations, and the assessor's team leads should have relevant security and privacy certifications. Examples of relevant auditing certifications are:

- Certified Information Privacy Professional
- Certified Information Privacy Manager
- Certified Information Systems Security Professional
- Fellow of Information Privacy
- HealthCare Information Security and Privacy Practitioner
- Certified Internal Auditor
- Certified Risk Management Professional
- Certified Information Systems Auditor
- Certified Government Auditing Professional
- Certified Expert HIPAA Professional

2.3 Assessor Options

CMS strongly recommends the use of an experienced third-party security and privacy assessor. However, internal state staff may be leveraged, provided they have appropriate qualifications to evaluate the implementation of security and privacy controls. The internal state staff must be familiar with HIPAA regulations, NIST standards, and other applicable federal privacy and cybersecurity regulations and guidance. They must also meet the assessor's independence, objectivity, and qualifications documented in Sections 2.1 and 2.2. Furthermore, they must be capable of performing penetration testing and vulnerability scans.

3. Assessment Scope and Planning

3.1 Scope of the Independent Security and Privacy Control Assessment

The purpose of a Security Control Assessment (SCA) is to determine whether the security and privacy controls are implemented correctly, operate as intended, and produce the desired outcomes for meeting the security and privacy requirements of the application or system. The SCA also identifies areas of risk that require the state's attention and remediation. The independently conducted SCA provides an understanding of the following:

- The MES application or system's compliance with the state security and privacy control requirements
- The underlying infrastructure's security posture
- Any application and/or system security, data security, and privacy vulnerabilities to be remediated to improve the MES's security and privacy posture
- The state's adherence to its security and privacy program, policies, and guidance

3.2 Vulnerabilities and Testing Scenarios

Given the sensitivity of data processed in the MES and the high threat of the web environment, it is critically important that the security of web applications deployed meet the present-day known security attack vectors and situations. OWASP keeps an up-to-date list that identifies such attacks and situations. In addition to the mandated security and privacy controls, the independent SCA requires vulnerability assessments to determine vulnerabilities associated with known attacks and situations obtained from the current OWASP Top 10 – *The Ten Most Critical Web Application Security Risks*. The assessment should adjust the SCA scope to address the current OWASP list of vulnerabilities. The state should regularly review the following list to determine the current vulnerabilities in the OWASP Top 10, including, but not limited to:

- Broken Access Control
- Cryptographic Failures
- Injection
- Insecure Design
- Security Misconfiguration
- Vulnerable and Outdated Components
- Identification and Authentication Failures
- Security Logging and Monitoring Failures
- Server-Side Request Forgery

3.3 Assessment of Critical Security Controls

Test scenarios should assess the implementation status of critical security controls identified by the Center for Internet Security (CIS). The CIS controls are mapped to the NIST controls. The testing scenario information for each CIS control is available at the CIS site. The main testing points identified by the CIS are incorporated into the SCA scope, corresponding Security and Privacy Controls Assessment Test Plan (SAP), and testing criteria.

CIS benchmarks are specific to environmental components such as server operating system hardening, networking configurations, or cloud service implementations. Where benchmarks exist, they should be applied to the system configurations.

3.4 Assessment Planning

The state is encouraged to develop an assessment strategy and procedure that provides a standardized approach for planning and resourcing the SCA of its applications, systems, and underlying components. The state is responsible for ensuring that each SCA has:

- Budget and assigned resources suitable for completing the assessment
- Clear objectives and constraints
- Well-defined roles and responsibilities
- Scheduling that includes defined events and deliverables

During planning for the SCA, the state develops a scope statement that is dependent on, but not limited to, the following factors:

- Application or system boundaries
- Known business and system risks associated with the application or system
- Dependence of the application or system on any hierarchical structure
- Current application or system development phase
- Documented security and privacy control requirements

The assessor's SCA contract statement of work should include requirements to provide support to clarify findings and make corrective action recommendations after the assessment. The contract terms should also specify that all assessor staff must execute appropriate agreements such as Non-Disclosure Agreement, Memorandum of Understanding, or HIPAA Business Associate Agreement for the protection of sensitive data before accessing any information related to the security and privacy of the application or system. Requests to access information should only be considered based on a demonstration of a valid need to know, ***not*** a position, title, level of investigation, or position sensitivity level.

4. Security and Privacy Control Assessment Methodology

The SCA methodology described in this guidance originates from the standard CMS methodology used in the assessment of all CMS internal and business partner applications or systems.

Assessment procedures for testing each security and privacy control should be consistent with the methodology documented in the most current version of NIST SP 800-53A, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations*. The assessor should prepare a detailed assessment plan using these security and privacy control assessment procedures, the main testing points for the CIS critical controls, and detailed directions for addressing the penetration testing procedures for the OWASP Top 10 vulnerabilities. The assessor should modify or supplement the procedures to evaluate the applications or system's vulnerability to distinct types of threats, including those from insiders, the internet, or the network. The assessment methods should include examination of documentation, logs and configurations, interviews with personnel, and testing of technical controls.

Control assessment procedures and associated test results provide information to identify the following:

- Application or system vulnerabilities, the associated business and system risks, and potential impact
- Weaknesses in the configuration management process, such as weak system configuration settings that may compromise the confidentiality, integrity, and availability of the system
- State and/or federal policies not followed
- Major documentation omissions and/or discrepancies

4.1 Security and Privacy Control Technical Testing

To conduct security technical testing, the state grants assessor staff user access to the application or system. The state system administrator establishes application-specific user accounts for the assessor that reflect the different user types and roles. Through this access and these accounts, the assessor can perform a thorough assessment of the application or system and test application and system security controls that might otherwise not be tested. The assessor should not be given a user account with a role that would allow access to PHI/PII in any application or database.

The assessor should attempt to expose vulnerabilities associated with gaining unauthorized access to the application or system resources by selecting and employing tools and techniques that simulate vulnerabilities, such as buffer overflows and password compromises. The assessor must use caution to ensure against any inadvertent alteration of important settings that may disable or degrade essential security or business functions. Because many automated testing utilities mimic signs of attack and/or exploit vulnerabilities, the assessor must identify in the SAP all proposed tools that pose a risk to the computing environment.

The MES solution can be tested in a test environment, or a pre-production environment provided these environments host an instance of the production operational environment. The testing or pre- production environments should mirror the production environment to generate an accurate response. Any deviations in these environments used for testing should be properly documented. States or vendors should certify and attest that all system vulnerabilities found because of security and privacy assessment performed in a test or a pre-production environment will also be mitigated in the production environment.

4.2 Network and Component Scanning

To gain an understanding of a network and component infrastructure security posture, the SCA includes network-based infrastructure scans, database scans, web application scans, and penetration tests for all in-scope components, applications, and systems. This scope provides a basis for determining the extent to which the security controls implemented within the network meet security control requirements. The assessor evaluates the results of these scans in conjunction with the configuration assessment.

4.3 Configuration Assessment

The configuration assessment provides the assessor with another mechanism for determining if the state's security requirements are implemented correctly in the application or system, or if the system environmental components are implemented correctly within the boundary of the application or system. Performing the configuration assessment requires the assessor to:

- Review the implemented configurations for each component against the state's security and privacy requirements
- Review access to the system and databases for default user accounts
- Test firewalls, routers, systems, and databases for default configurations and user accounts
- Review firewall access control rules against the state's security requirements
- Determine consistency of system configuration with the state's documented configuration standards

4.4 Documentation Review

The assessor should review all security and privacy documentation for completeness and accuracy and gain the necessary understanding to determine the security and privacy posture of the application or system. Through this process, the assessor develops insight into the documented security and privacy controls in place to effectively assess whether all controls are implemented as described. The documentation review augments all testing: it is an essential element for evaluating compliance of the documented controls versus the actual implementation as revealed during technical testing, scanning, configuration assessment, and personnel interviews.

For example, if the specified control stipulates that the password length for the system must be eight characters, the assessor must review the state's password policy or the SSP to verify compliance with this requirement. During the technical configuration assessment, the assessor confirms that passwords are configured as stated in the state's documentation. Table 1 identifies examples of core security documentation for review.

Core Security and Privacy Documentation

NIST/STATE CONTROL FAMILY	NIST/STATE CONTROL NUMBER	DOCUMENT NAME
Planning (PL)	PL-2: System Security and Privacy Plan (SSP)	System Security and Privacy Plan (SSP)
Configuration Management (CM)	CM-9: Configuration Management Plan	Configuration Management Plan (CMP)
Contingency Planning (CP)	CP-2: Contingency Plan	Contingency Plan (CP)
Contingency Planning (CP)	CP-4: Contingency Plan Testing and Exercises	CP Test Plan and Results
Incident Response (IR)	IR-8: Incident Response Plan	Incident Response Plan (IRP)
Incident Response (IR)	IR-3: Incident Response Testing and Exercises	IRP Test Plan
Awareness and Training (AT)	AT-3: Security Training	Security Awareness Training Plan
Awareness and Training (AT)	AT-4: Security Training	Training Records
Security and Assessment Authorization (CA)	CA-3: System Interconnections	Interconnection Security Agreements (ISA)
Risk Assessment (RA)	RA-3: Risk Assessment	Information Security Risk Assessment (ISRA)
Authority and Purpose (AP)	AP-1: Authority to Collect	Privacy Impact Assessment (PIA) or other privacy documents
Authority and Purpose (AP)	AP-2: Purpose Specification	Privacy documents and notices including, but not limited to, PIAs and agreements to collect, use, and disclose PHI/PII and Privacy Act Statements
Accountability, Audit, and Risk Management (AR)	AR-1: Governance and Privacy Program	Governance documents and privacy policy
Accountability, Audit, and Risk Management (AR)	AR-2: Privacy Impact and Risk Assessment	Documentation describing the organization's privacy risk assessment process, documentation of privacy risk assessments performed by the organization

4.5 Personnel Interviews

The assessor conducts personnel interviews to validate the implementation of security and privacy controls, confirm that state and/or MES solution vendor staff understand and follow documented control implementations, and verify the appropriate distribution of updated documentation to staff. The assessor interviews business, information technology (IT), and support personnel to ensure effective implementation of operational and managerial security and privacy controls across all support areas. The assessor will customize interview questions to focus on control assessment procedures applicable to individual roles and responsibilities and ensure that state staff are properly implementing and/or executing security and privacy controls.

The SCA test plan identifies the designated state and/or MES solution vendor subject matter experts (SMEs) to interview. These SMEs should have specific knowledge of overall security and privacy requirements and a detailed understanding of the application or system operational functions. The staff selected for conducting interviews may have the following roles:

- Business Owner(s)
- Application Developer
- Configuration Manager
- Contingency Planning Manager
- Database Administrator
- Data Center Manager
- Facilities Manager
- Firewall Administrator
- Human Resources Manager
- Information System Security Officer
- Privacy Program Manager
- Privacy Officer
- Media Custodian
- Network Administrator
- Program Manager
- System Administrator(s)
- System Owner
- Training Manager

Although the initial identification of interviewees is determined when the SAP is prepared, additional staff may be identified for interviewing during the SCA process.

4.6 Penetration Testing

At a minimum, penetration testing includes the tests found in Section 3.2 (based on the OWASP Top 10). The Security and Privacy Controls Assessment Test Plan should document the tools, methods, and processes for penetration testing. The test plan should clearly account for and coordinate any special requirements or permissions for penetration testing during the SCA.

A penetration test is a comprehensive way of testing an organization's cybersecurity vulnerabilities and compliance with the adopted security and privacy standards. Penetration testing views the network, application, device, and physical security through the eyes of both a malicious actor and an experienced cybersecurity expert to discover weaknesses and identify areas where the security posture needs improvement, and subsequently, ways to remediate the discovered vulnerabilities.

5. Security and Privacy Assessment Reporting

At the completion of the assessment, the assessor provides a Security and Privacy Assessment Report (SAR) to the state's Business Owner, who is then responsible for providing the report to CMS. The SAR's structure and content (as described in the following subsection) must be consistent with the assessment objectives. The SAR allows the assessor to communicate the assessment results to several audience levels, ranging from executives to technical staff.

The SAR is not a living document; findings should not be added to or removed from the SAR.

5.1 SAR Content

The SAR content may include, but is not limited to, the following information:

- System Overview
- Executive Summary Report
- Detailed Findings Report
- Scan Results
  - Infrastructure Scan
  - Database Scan
  - Web Applications Scan
- Penetration Test Report
- Penetration Test and Scan Results Summary

The SAR presents the results of all testing performed, including technical testing, scans, configuration assessment, documentation review, personnel interviews, and penetration

testing. Results from multiple testing sources may be consolidated in one finding if results are closely related. The findings of the assessment should be annotated in detail with the remediation recommendations for the weaknesses and deficiencies found in the system security and privacy controls implementation. To reduce the risks posed to this important healthcare service and to protect the sensitive information of the citizens who use this service, the assessment team must assign business and system risk levels to each specific finding. The assignment of these risk levels should follow the methodology outlined in NIST SP 800-30 Rev. 1, Appendices G, H, and I.

The SAR structure should allow the independent third-party assessor to communicate the security and privacy assessment results to several targeted audience levels, ranging from executives to technical staff. A sample SAR can be modeled after one used by FedRAMP.

6. Incident and Breach Reporting Procedures

CMS considers a security or privacy incident14 or breach15 of beneficiary PHI/ PII to be a serious matter. Therefore, state agencies which are found to be out of compliance with the privacy or security requirements outlined in this guidance can expect suspension or denial of FFP for their information systems and may be subject to other penalties under federal and state laws and regulations.

Under HIPAA standards, states must require that contractors and other entities performing claims processing, third-party (or other payment or reimbursement) services on their behalf protect PHI/PII privacy and security through business associate agreements. In so doing, states should ensure that their business associates update their procedures as necessitated by environmental or operational changes affecting security and privacy safeguards. The HIPAA Breach Notification Rule, 45 C.F.R. §164.400-414, requires HIPAA covered entities and their business associates to provide notification following a breach of unsecured protected health information. Similar breach notification provisions implemented and enforced by the Federal Trade Commission (FTC) apply to vendors of personal health records and their third-party service providers, pursuant to Section 13407 of the HITECH Act.

Visit the HHS HIPAA Breach Notification Rule website for more information and guidance on the breach reporting requirements.16 In addition to the above HIPAA requirements, the state, in turn, should immediately report a security or privacy incident or breach, whether discovered by its own staff or reported by a contractor, to the CMS State Officer and CMS IT Service Desk at cms_it_service_desk@cms.hhs.gov. If a state is unable to report breaches to the CMS IT Service Desk via email, the state can contact the CMS IT Service Desk by phone at (800) 562-1963 or (410) 786-2580.

7. Summary

All organizations should either perform an internal state risk assessment or engage an industry- recognized security and privacy assessment organization to conduct an external third-party risk assessment (CMS preferred method) of the MES implementation to identify and address security and privacy vulnerabilities. Information security and privacy safeguards and

continuous monitoring are dynamic processes that must be managed effectively and proactively to support organizational risk management decisions. Independent security and privacy assessment provides a mechanism for the organization to identify and respond to new vulnerabilities, evolving threats, and a constantly changing enterprise architecture and operational environment, which can feature changes in hardware or software, as well as risks from the creation, collection, disclosure, access, maintenance, storage, and use of data. Through ongoing assessment and authorization, organizations can detect changes to the security and privacy posture of an IT system, which is essential to making well-informed, risk-based decisions about the system within the MES.

APPENDIX E – INTAKE FORM TEMPLATE

The Intake Form Template is used throughout the Streamlined Modular Certification process to track information about a state MES project for certification. It is tailored for each state project. States will fill out the Intake Form Template by entering the CMS-required outcomes that document compliance with regulations applicable to their project, their state-specific outcomes, and the metrics used to show that the project is achieving its outcomes on a continuous basis. The outcomes and metrics included in Intake Form Template information should match what is included in the APD. As the state progresses with the project, the state along with their CMS State Officer will identify and document in the Intake Form Template, the evidence to be provided to demonstrate that outcomes have been achieved. As the ORR approaches, CMS and the state will finalize the specific evidence to be provided by the state. The detailed results of the ORR evaluation and the CR are also documented in the Intake Form Template. Using a single Intake Form Template to record information for the ORR and CR allows CMS to maintain an audit record for all certification activities.

Please see the CMS Certification GitHub Repository for the Intake Form Template.

APPENDIX F – MEDICAID ENTERPRISE SYSTEMS TESTING GUIDANCE FRAMEWORK

Comprehensive and thorough testing of enterprise software throughout the MES IT Investment Lifecycle leads to higher quality software products and increased levels of user satisfaction. CMS expects states to effectively test applications and services so that issues are identified and remediated early in the MES IT Investment Lifecycle. Early detection of systems issues reduces the number of errors embedded in the software and the cost of rework later in the development cycle, thereby increasing the overall quality of the delivered system and user satisfaction.

This document lists a set of expectations and recommendations for testing which are defined as follows:

- Expectations describe actions and deliverables that states are required to demonstrate and/or provide as evidence.
- Recommendations denote industry best practices that have been shown to increase the efficiency and quality of products. CMS encourages states to adopt and follow these recommendations to enhance the quality and reduce risk for MES implementations.

Expectations The expectations are broken down by major project stages: test planning, test execution, and operational monitoring.

Test Planning

Test planning starts with the acquisition process by including testing expectations in Requests for Proposals (RFPs) and contracts and it continues into the early phases of project planning to organize the testing process. Specifying testing requirements in the contract should leave no ambiguity regarding the role of the state and vendors in the testing process. Including testing-related expectations in the contract also ensures that the vendor's test planning processes and level of rigor are documented and available for CMS review.

Expectation 1: CMS expects state contracts to include requirements for system testing. Further, in accordance with 42 CFR 433.112, states must share the contracts with, and obtain prior approval from CMS, to be eligible for Federal Financial Participation (FFP). Depending on the nature of the procured system (e.g., custom developed, Commercial off-the-shelf (COTS), Software as a Service (SaaS)), the following are examples of testing-related requirements that CMS expects states to include in relevant contracts:

- Ensure that test teams have appropriate skills and are independent of the development teams. For example, the use of automated software testing requires the testing team members to have programming experience to develop the automated tests and validate the test results.
- Define the various testing environments (e.g., integration environment, user acceptance environment), the process of managing testing environments, and conditions for promoting software builds from one environment to another. Test environment

configuration should be automated to increase efficiency and protect against test environment misconfiguration.

- Define defect severity levels (i.e., what qualifies as a defect for each severity level, and expectations about the turnaround time for fixing defects of different severity).
- Define expectations regarding detailed test cases development for each system requirement.
- Define expectations regarding load and performance testing, and the role of automated testing in these types of tests.
- Describe the process for resolving defects when the system is in production, including replicating the defects in non-production environments and conducting root cause analyses (RCAs).
- Describe the process for loading new software builds in the production environment.
- Describe the process for continuously monitoring the production environment's performance and taking the appropriate actions to proactively deal with potential issues. Examples of monitoring include CPU, memory and disk usage, system response time, event logs, and health of processes and services.
- Define expectations regarding measuring and reporting metrics defined in Service Level Agreements (SLA). Examples of SLA metrics include system availability, system recovery objectives in case of system crashes or natural disasters, and system response time.

Expectation 2: CMS expects states or their vendors to develop and share a master test plan that describes the details for how and what testing will occur. The master test plan should cover elements such as:

- List of stakeholders who need to review and approve the master test plans.
- Project scope and summary, which includes a list of features that will be tested in order to remove ambiguity about the testing scope.
- Types of testing, such as integration testing, user acceptance testing, load testing, etc.
- Test entry criteria, which include information such as description of the test environment, specific setup of required test data, review, and approval of test cases, etc.
- Test exit criteria, which specify the quality gates that need to be met before a project can be rolled into production. Most projects have minimum quality gates that are 100% execution of all test cases, no outstanding critical or high severity defects, etc.
- Test data requirements, (e.g., requirement for the generation of vast amounts of random data). In addition, it is sometimes more beneficial to use production data in test environments to test issues found in the production system. The master test plan should describe the method to remove Personally Identifiable Information (PII) and Protected Health Information (PHI) (i.e., data de-identification) when used in lower test environments.
- Testing tools that will be used in various environments.
- The process for identifying risks, developing mitigations, and tracking the risks.
- Testing schedule.
- Defect management process, which describes the stages a defect will go through before it is closed.

- Test metrics that are used to get reports on the progress of testing. Examples of test metrics include number of test cases executed, defects logged, features with the most bugs, requirements coverage, how long it takes defects before they are closed, etc.

Expectation 3: CMS expects states to develop and share an incident response handling plan and a contingency plan for sustaining operation of the legacy system if the testing process demonstrates that the new system exhibits untenable performance behaviors either during the system development phase or after production. The plans should include elements such as:

- A process for conducting quality audits during system development to examine qualitative and quantitative metrics that assess the system health and quality and to assess risks of missing important milestones.
- A process for conducting quality audits during system operation to examine qualitative and quantitative metrics to assess the operational system health and quality and to assess risks of continued quality issues.
- A process for triggering an escalation procedure to make decisions to either sustain or revert to a legacy system if issues cannot be fixed or addressed with appropriate workarounds.

Test Execution

Regardless of the software development methodology used (e.g., agile, waterfall), the type of system (e.g., custom development, COTS, SaaS), or the responsibilities of the state and vendor, the state is responsible for ensuring that robust testing has been performed and the delivered system is of high quality. Disconnects between activities executed by different stakeholders can create schedule, cost, quality, and maintenance problems.

Expectation 1: CMS expects states to exercise their responsibility to assess the system functionality via testing and to develop and share clear documentation of state and vendor responsibilities regarding testing and quality. The documented process is expected to also include processes and remedies to address system defects. To meet the expectations, states should ensure certain steps are performed, such as:

- System requirements are documented in sufficient detail to allow the development and/or use of test scenarios and for the testing team to develop comprehensive test cases that handle normal and exception data, (e.g., data incorrectly formatted), or data that falls outside specified ranges.
- Test cases are linked to, and provide full coverage of, functional system requirements, including testing across multiple browsers and devices.
- Every step in a test case should have a clear indication of the expected results and pass/fail conditions.
- A thorough independent state review of the test results is performed at various stages in the development cycle.
- Pre-production system builds are available to system and business users to conduct frequent user acceptance testing.
- RCAs are conducted for defects, promoting effective re-use of lessons learned.

- Defects are consistently tracked and reported, using defined defect severity levels.
- Appropriate turnaround times for error/defect resolution are maintained.
- Test cases should include non-functional requirements, such as conducting test cases to test high availability, failover, disaster recovery, response time, data migration, and system performance under simulated peak load.
- The testing team has a clear escalation path to the appropriate stakeholders if high-severity defects are not fixed within a reasonable timeframe or if system quality issues persist throughout system development.

Expectation 2: CMS expects states to ensure the testing team includes experienced testing and quality assurance team members:

- The state and vendor test assessment team should include team members who understand the nature and purpose of the system and the kind of software involved.
- The state testing team should include members with appropriate experience and expertise to review test plans and procedures and to evaluate the functionality.
- The quality assurance team members should ensure correct system quality procedures are followed, (e.g., entry and exit criteria are followed for code to be promoted from the development environment to the system testing environment).

Expectation 3: CMS expects states to provide evidence and test results to CMS for different types of tests. Different types of testing include:

- Unit Testing: The developer conducts the unit test, typically on the individual modules under development. The unit test often requires simulating interfaces to other modules or systems which are the source of input data or receive the output of the module being tested but that are not yet ready to test.
- System Integration Testing: When a new module or a significant new layer of functionality is added to the system, a series of tests are performed to ensure that the new module or functionality operates correctly in conjunction with all pre-existing modules/functions. This type of testing is most prevalent when a new function is developed, or an application programming interface (API) has been added or modified. In addition, states should include testing federal reporting requirements, such as T-MSIS, as part of this type of testing.
- Regression Testing: Once changes are made to a system, such as new functionality or significant modifications due to defect resolution, a series of tests must be performed to ensure that all pre-existing functionality is still operational and still passes previously executed tests.
- User Acceptance Testing: Once development and system testing have been completed, a “final” series of tests must be performed to ensure that the new/updated system functionality satisfies the needs of the business and system users and helps them perform their daily activities in a more streamlined manner. Accessibility testing (i.e., 508 compliance) could be incorporated as a form of end-user testing. In addition, states should include testing federal reporting requirements, such as Transformed Medicaid Statistical Information System (T-MSIS), as part of this type of testing.

- Performance Testing: The system must be subjected to tests that ensure that SLAs are attainable and sustainable. These tests primarily focus on ensuring that system response times and infrastructure parameters (e.g., CPU, storage, network) are within acceptable tolerances.
- Load Testing: These tests include employing specific tools and techniques (often automated) to apply simulated high – yet realistic – volumes of user traffic and thus stress the underlying infrastructure components. The primary goal of this type of testing is to determine at what point the system "breaks" or response times are degraded to a point where they become intolerable. These tests provide an insight into the scalability of the system.
- Parallel Testing: This important type of testing is typically used when transitioning from a legacy system to a new system and it aims to find out whether the legacy system and the new system are behaving the same or differently and to ensure that the two systems produce consistent results. This type of testing should include testing of federal reporting requirements, such as T-MSIS.
- Data Migration Testing: Migration Testing is a verification process of migration of the legacy system to the new system with minimal disruption/downtime, with data integrity, and no loss of data, while ensuring that all the specified functional and non-functional aspects of the application are met post-migration. Migrating data from legacy systems is often difficult and risky as it requires combining data from multiple sources and databases and handling data quality and inconsistency from disparate sources.
- Security Testing: Security testing ensures that sensitive information, such as PII and PHI, is protected. Security testing should be performed prior to production and on an ongoing basis when the system is operational. For more details on the scope and requirements of security and privacy testing, please refer to the Streamlined Modular Certification for Medicaid Electronic Systems Guidance Document, Appendix D – *Framework for the Independent Third-Party Security and Privacy Assessment Guidelines for Medicaid Enterprise Systems*.
- Usability Testing: Usability testing is a method of testing the functionality of a system and involves observing real users as they attempt to complete tasks in the system. The goal is to reveal areas of confusion and uncover opportunities to improve the overall user experience. Conducting usability testing helps improve the user experience.

Expectation 4: CMS expects states to share testing and quality metrics with CMS. Metrics include, but are not limited to:

- Percentage of requirements covered by and traced to test cases.
- Percentage of software code covered by test cases.
- Current list of defects with data, such as defect title, description, test case reference, requirements reference, severity, open date, status, etc.
- Charts or graphs showing the distribution of defects by severity level.
- Graphs showing the rate of opening and closing defects.
- Statistics showing defect age.
- Statistics for defect reopening.

Expectation 5: CMS expects states to develop a thorough deployment plan. The deployment plan should include, but not be limited to, the following components. In addition, some components below may not be needed for SaaS solutions:

- A release plan that describes the activities for a phased implementation or roll-out. The release plan may include the following activities as appropriate: preparation of the environment, conversion information, product installation information, and data migration.
- Production readiness checklist that describes a list of steps necessary to ensure the product deployment requirements are met.
- Communication plan to ensure that everyone who needs to be informed about deployment activities and results gets the needed information in a timely manner.
- Issue/change request tracking method that will be used to record project issues and decisions.
- Business continuity and disaster recovery plan that describes a business resumption plan when a catastrophic event occurs.

Expectation 6: CMS expects states to use, and share collected data in an actionable manner and to hold vendors accountable for unacceptable system quality that jeopardizes important milestones and/or system users buy-in:

- A triage process to understand and analyze data collected, (e.g., defect statistics), to properly assess system quality issues.
- A process for developing RCAs with a plan to resolve severe issues.
- A process for officially informing vendors of unacceptable quality issues and requesting a plan to remedy such issues, (e.g., a cure notice).
- A process for escalating consistent issues to an identified body of decision-makers and CMS to determine the future of the system and the system development with the current vendor(s).

Operational Monitoring

Once a system goes into production, operational monitoring tracks the system “health” on an ongoing basis. Monitoring the production environment ensures that the system responds well to peak loads, users are satisfied with the system response, the system is intuitive and well-liked by users, and the system handles component failure in a graceful manner.

Expectation 1: CMS expects states to perform ongoing testing after production to validate changes to the system and to share the testing results with CMS. This is effectively a form of regression testing. Testing may include:

- A set of tests to ensure that newly added functionality works as expected.
- A process for initiating and monitoring RCAs for production defects, and for using the RCA results to enhance the quality of the software and the quality of testing to avoid detecting defects witnessed only in the production environment.

- A suite of regression tests to ensure newly added functionality does not break existing functionality that was already working in the production system.
- A signoff process to allow the new software to be loaded in the production system.
- A documented process to back out certain changes to the production code, if necessary.

Expectation 2: CMS expects states to develop and share a set of metrics to monitor the health of the system and escalation procedures to notify the appropriate stakeholders for certain detected conditions. Metrics may include, but are not limited to, the following items:

- Statistics regarding usage of important computing capacity, such as CPU, memory, and storage.
- System availability.
- Statistics regarding system response time for various user transactions.
- Statistics regarding a help desk or call center, if applicable.
- Statistics regarding corrective action plans and RCAs.
- Statistics regarding turnaround times to resolve production defects.

Expectation 3: CMS expects states to use, and share collected data in an actionable manner and to hold vendors accountable for unacceptable system quality that jeopardizes important milestones and/or system users buy-in:

- A triage process to understand and analyze data collected from the operational system, (e.g., SLAs and defect statistics), to properly assess system quality issues.
- A process for developing RCA with a plan to resolve severe issues.
- A process for informing vendors officially of unacceptable quality issues and request for a plan to remedy such issues, (e.g., a cure notice).
- A process for escalating consistent issues to an identified body of decision-makers and CMS to determine the future of the system and make decisions regarding the operational system and the current vendor(s).

List of Recommendations

CMS recommends states also adopt the following best practices to assist in meeting CMS MES testing expectations in an efficient and effective manner.

Recommendation 1: States should define formal testing team structures that may include a combination of state and vendor staff.

- If the first level of testing is performed by the vendor testing team and the state team functions more as user acceptance and oversight team, the state should produce clear documentation of the division of responsibility and the handoff procedures between the state and vendor testing teams.

Recommendation 2: States should consider pooling test resources and knowledge with other states to increase efficiency. This may take several forms, such as:

- Making test scenarios and test cases available for sharing between cooperating states allows states to learn new practices that enable them to become better generators of their own new test cases.
- Making testing tool licenses available for sharing between cooperating states whenever possible to allow greater access to valuable tools that might otherwise be too expensive for them to acquire individually.
- Launching and actively participating in a states' learning consortium that consolidates lessons learned, serves as a central knowledge custodian, and provides a forum for iterative self-improvement. CMS could work with states, if interested, to test the effectiveness of this recommendation and to develop a mechanism to operationalize it.
- Exploring the use of a common testing environment to enhance states' overall testing regimens.

Recommendation 3: States should use synthetic datasets whenever possible and to the extent practical. Synthetic data is artificially generated to replicate real-world data but does not contain any identifiable information. This lowers the barrier to deploy data by removing the need for vast volumes of real data and adds security by eliminating PII/PHI.

Recommendation 4: CMS recommends the use of automated testing tools. The recommended breadth and depth of unit, functional, and regression testing cannot be effectively performed solely by manual testing. Automated testing should be implemented in a cost-effective manner, and both states and their vendor(s) should be participants in this effort. Iterative development and regression testing benefit from the speed and consistency provided by automation tools.

APPENDIX G – OPERATIONAL REPORT WORKBOOK

Operational Report Workbook

APPENDIX H – MEDICAID ENTERPRISE SYSTEMS (MES) DATA SUBMISSIONS AND INTAKE PROCESS PROCEDURES MANUAL, SEPTEMBER 1, 2022

MES Data Submissions and Intake Process Procedure Manual

APPENDIX I – FXPA CERTIFICATION RACI – DATED FEBRUARY 7, 2023

FX RACI Matrix										
Role / **Project Deliverable**	**Agency**	**SEAS**	**ISIP**	**EDW**	**UOC**	**Core**	**PSM**	**IV&V**	**Existing System Owner**	**External Organizations**
8.13 Certification										
Planning Phase										
Project Planning										
Engage Agency SME Ownership of Program Outcomes & Metrics	R/A	C						I		
Identify Program Business Processes	R/A	C						I		
Prioritize Program Business Processes by Agency Benefit Needs	R/A	C						I		
Map Prioritized Program Business Processes to Projects	A/C	R						I		
Articulate FX Program Outcomes and Benefits	A/C	R						I		
Articulate Project Outcomes and Benefits	A/C	R	C	C	C	C	C	I		
Articulate Plan Project (Product) Roadmap	A/C	R	C	C	C	C	C	I		
Align Project (Product) Roadmap to FX Roadmap	A/C	C	R	R	R	R	R	I		
Draft Metrics, and Evidence for Each Outcome	A/R	C	C	C	C	C	C	C		
Coordinate with CMS SO on Outcome Metrics and Evidence Development	A/R	C	I	I	I	I	I	C		C
Configure MITA Pulse Certification Workflow	A/C	R	I	I	I	I	I	I		
Validate CMS Outcomes and CEFs in MITA Pulse	A	R	I	I	I	I	I	C		
Populate State-specific Outcomes in MITA Pulse	A	R	I	I	I	I	I	C		
Populate Proposed Metrics and Evidence in MITA Pulse	A	R	I	I	I	I	I	C		
Generate Intake Form in MITA Pulse	A	C	I	I	I	I	I	R		
Submit Intake Form to CMS SO for Review and Feedback	A/R	C	I	I	I	I	I	C		
Review and Incorporate CMS SO Intake Form Response	A/R	C	C	C	C	C	C	C		

FX RACI Matrix										
	Agency	**SEAS**	**ISIP**	**EDW**	**UOC**	**Core**	**PSM**	**IV&V**	**Existing System Owner**	**External Organizations**
Procurement Planning										
Incorporate Outcomes in APD	A/R	C						I		
Review APD with CMS SO	A/R	C						I		
Update APD (as needed)	A/R	C						I		
Submit the APD for CMS Review and Approval	A/R	C						I		
Review CMS APD Response and Mitigate Comments (as needed)	A/R	C						I		
Map Outcomes to Business and Technical Requirements in Draft Procurement Document	A/C	R						I		
Development										
Develop Master Test Plan	A	C	R	I	I	I	I	I		
Develop Master Deployment Plan	A	C	R	I	I	I	I	I		
Validate Draft Evidence Against Design	A	C	R	R	R	R	R	I		
Validate Draft Metrics Against Design	A	C	R	R	R	R	R	I		
Validate and Update MITA Pulse Workflow	A/C	R	I	I	I	I	I	I		
Develop CMS Monthly Project Status Reports	A	R	C	C	C	C	C	I		
Track and Compile User Feedback	A	C	R	R	R	R	R	I		
Monitor Defect and Risk Lists	A	R/C	R	R	R	R	R	I		
Track Project Progress	A	C	R	R	R	R	R	I		
Project Progress Product Demos (for phased implementations)	A	C	R	R	R	R	R	I		
Track Testing Progress	A	C	R	R	R	R	R	I		
Conduct Independent Third-party Security and Privacy Assessment	A/C	I	R	R	R	R	R	C		R
Develop Evidence to Demonstrate Project Health	A	C	R	R	R	R	R	I		
Maintain Workflow and Evidence in MITA Pulse SMC Tool	A/C	R	I	I	I	I	I	I		
Create and Submit CMS Monthly Project Status Reports	A	R	C	C	C	C	C	I		
Pre-Production: Operational Readiness Review										
Schedule ORR with CMS SO	A/R	C	C	C	C	C	C	I		
Validate Required Artifacts and Evidence	A	C	C	C	C	C	C	R		
Develop Presentation and Demonstration for ORR	A/R	C	R/C	R/C	R/C	R/C	R/C	C		
Complete Non-Disclosure and Data-Sharing Agreements with CMS and MITRE	A/R	I	I	I	I	I	I	I		

FX RACI Matrix										
	Agency	**SEAS**	**ISIP**	**EDW**	**UOC**	**Core**	**PSM**	**IV&V**	**Existing System Owner**	**External Organizations**
Upload Evidence and Artifacts to the CMS Box Repository for Review	A/R	I	I	I	I	I	I	I		
Complete State Columns of the Intake Form	A	C	I	I	I	I	I	R		
Submit Intake Form to CMS	A/R	I	I	I	I	I	I	I		
Receive CMS Questions and Prepare Responses	A/R	R/C	R/C	R/C	R/C	R/C	R/C	C		
Support ORR	A/R	R/C	R/C	R/C	R/C	R/C	R/C	C		
Conduct ORR	A/R	C	C	C	C	C	C	C		
Receive CMS Completed Intake Form	A/R	I	I	I	I	I	I	I		
Respond to CMS Comments in the Intake Form	A/R	C	C	C	C	C	C	C		
Production										
Operational Activities										
Resolve Action Items from CMS ORR Response	A/R	C	R/C	R/C	R/C	R/C	R/C	I		
Create and Submit CMS Monthly Project Status Reports and Operational Reports	A/R	C	R/C	R/C	R/C	R/C	R/C	I		
Requesting Certification Review										
Send Certification Request Letter to CMS with Evidence of Readiness	A/R	I	I	I	I	I	I	I		
Send System Acceptance Letter to CMS	A/R	I	I	I	I	I	I	I		
Review and Refresh Required Artifacts and Evidence	A/R	C	R/C	R/C	R/C	R/C	R/C	I		
Report Metrics	A/R	C	R/C	R/C	R/C	R/C	R/C	I		
Develop Presentation and Demonstration for CR	A/R	C	R/C	R/C	R/C	R/C	R/C	C		
Upload Evidence and Artifacts to the CMS Repository for Review	A/R	I	I	I	I	I	I	I		
Complete State Columns of the Intake Form and Submit to CMS	A	C	I	I	I	I	I	R		
Receive CMS Questions and Prepare Responses	A/R	C	R/C	R/C	R/C	R/C	R/C	C		
Certification Review										
Conduct CR	A/R	C	C	C	C	C	C	C		
Support CR	A/R	R/C	R/C	R/C	R/C	R/C	R/C	C		
Receive CMS Completed Intake Form with Observations and Findings	A/R	I	I	I	I	I	I	I		

FX RACI Matrix										
	Agency	**SEAS**	**ISIP**	**EDW**	**UOC**	**Core**	**PSM**	**IV&V**	**Existing System Owner**	**External Organizations**
Operational Reporting Phase										
Operational Activities										
Respond to Action Items and Findings from CMS if Recommendations are made or Conditional Approval is Granted	A/R	C	R/C	R/C	R/C	R/C	R/C	I		
Create and Submit CMS Operational Project Status Reports	A/R	C	R/C	R/C	R/C	R/C	R/C	I		
Key										
Lifecycle Phase										
Service Management Category										
Process										
Function										
R - Responsible										
A - Accountable										
C - Consulted										
I - Informed										