Alabama Medicaid Agency

Information Security Office

PM-9 Medicaid Risk Management Strategy

07.20.20

Revision History

Date	Version	Author/Owner	Description of Changes
1.9.19	0.1	Brad Bird	Initial instantiation of document
10.21.19	0.2	Brad Bird	Added HIPAA Risk review wording
10.29.19	0.3	Brad Bird	Minor edits
07.20.20	1.0	Brad Bird	Publication of first edition. Clarification of scope – Systems that do not directly support the Medicaid Mission, integration of Risk frame from separate document.

Table of Contents

Introduction

Security capabilities are groups of functioning security controls. Since failed security controls present risk, risk management must be the new paradigm of Alabama Medicaid Agency. The Medicaid Risk Management Strategy defines the high level concepts applied to management of risk to Information Resources. The Risk frame, as it applies to Medicaid, defines assumptions, constraints, priorities, and tolerance for risk to Medicaid's information resources. The different levels of risk apply to operations and technical aspects of Medicaid.

Purpose

The purpose of this document is to establish an organizational information security Risk Management Strategy. This strategy addresses how Medicaid intends to frame, assess, respond to, and monitor information security and privacy risk.

Scope

This Risk Management Strategy applies to the Alabama Medicaid Agency, all of the Medicaid Program Areas, and all of the systems and information resources that directly support those Program Areas. This strategy also applies to entities outside of the Agency that use Alabama Medicaid information through sharing agreements such as a Business Associate Agreement, Memorandum of Understanding, or Data Sharing Agreement.

Authority & Applicability

The authority for this publication comes under the signature of the Medicaid Commissioner's Office and is applicable to all information resources owned and managed by the organization and all personnel employed by the organization, contractors or agents under the direct control of Medicaid, or any individual whose role entails access to Agency Information resources.

Also, "Agency Internal Memorandum 216: Compliance with Federal and State Legislated Security and Privacy Requirements – risk-based approach, Appendix 1" maintains an up to date list of Federal and State Legislation and other sources authoritative and applicable to the Medicaid Information Security Program.

Roles & Responsibilities

Commissioner and/or Chief Information Security Officer – define the Agency's risk management strategy and support the Agency's efforts to reach and maintain compliance with that strategy. Define the Agency's risk frame and support the Agency's efforts to reach and maintain compliance with that risk tolerance.

Chief Information Security Officer – develop, implement, and maintain the Agency's enterprise security program in alignment with this risk management strategy. Oversee the Governance, Risk, and Compliance team in risk management activities, ensuring alignment with this strategy.

System Owners – in conjunction with the Information System Security Manager (ISSM), work through the defined risk management activities to reduce risk (both overall and specific) to Agency systems. Ensure vulnerability management activities maintain patch levels of machines consistent with this risk management strategy and agency security policy.

System Administrators – maintain system configurations and patch levels consistent with this risk management strategy and agency security policy.

Information System Security Manager – manage risk management activities according to risk management policies and procedures.

PM-9: Risk Management Strategy Policy

The Agency:

a. Develops a comprehensive strategy to manage:
    1. Security risk to organizational operations and assets, individuals, other organizations, and the State associated with the operation and use of organizational systems;
    2. Privacy risk to individuals resulting from the collection, sharing, storing, transmitting, use, and disposal of personally identifiable information; and
    3. Supply chain risks associated with the development, acquisition, maintenance, and disposal of systems, system components, and system services;

b. Implements the risk management strategy consistently across the organization; and

c. Reviews and updates the Risk Management Strategy annually or as required, to address organizational changes.

Risk Management Strategy

The Alabama Medicaid Agency's Risk Management Strategy is based on the NIST Risk Management Framework (RMF), the definition of which is in NIST SP 800-39 and whose organizational implementation is described in SP 800-37.

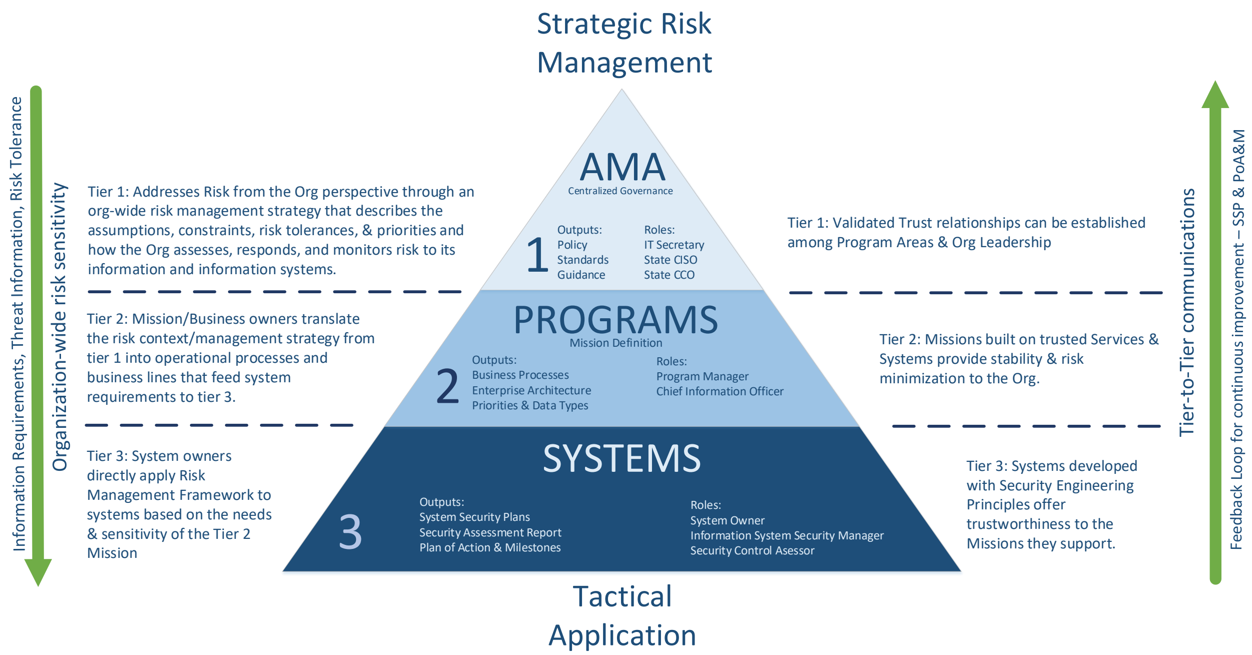
The Medicaid Risk Management Strategy intends to follow the three-tier approach in NIST SP 800-37 and 800-39:

1. Define requirements at the **Organization** level (in the form of top level policy).
2. Have requirements levied on the **Program Areas** or **Missions** within the Organization (i.e. make Program Managers responsible for protecting the information their Programs use).
3. Have those requirements implemented, assessed, responded to, and monitored at the **System** Level (in the form of procedures, standards, configurations, etc…).

This top-down approach is intended to be supported through bottom-up communications in the form of reporting back up through the three tiers:

3. System level security plans are documented depicting how each system adheres to the requirements and how each system protects the information for which the Program Managers are responsible.
2. Program Areas report high level compliance and risk mitigation plans to the top level Organization.
1. The Organization updates its Risk Management Strategy and focuses resources on areas of greatest risk.

The following pictograph illustrates this concept:


Strategic Risk Management
Information Requirements, Threat Information, Risk Tolerance
Organization-wide risk sensitivity
AMA
Centralized Governance
1
Outputs:
Policy
Standards
Guidance
Roles:
IT Secretary
State CISO
State CCO
PROGRAMS
Mission Definition
2
Outputs:
Business Processes
Enterprise Architecture
Priorities & Data Types
Roles:
Program Manager
Chief Information Officer
SYSTEMS
3
Outputs:
System Security Plans
Security Assessment Report
Plan of Action & Milestones
Roles:
System Owner
Information System Security Manager
Security Control Asessor
Tier-to-Tier communications
Feedback Loop for continuous improvement – SSP & PoA&M
Tactical Application

Tier 1: Addresses Risk from the Org perspective through an org-wide risk management strategy that describes the assumptions, constraints, risk tolerances, & priorities and how the Org assesses, responds, and monitors risk to its information and information systems.

Tier 2: Mission/Business owners translate the risk context/management strategy from tier 1 into operational processes and business lines that feed system requirements to tier 3.

Tier 3: System owners directly apply Risk Management Framework to systems based on the needs & sensitivity of the Tier 2 Mission

Tier 1: Validated Trust relationships can be established among Program Areas & Org Leadership

Tier 2: Missions built on trusted Services & Systems provide stability & risk minimization to the Org.

Tier 3: Systems developed with Security Engineering Principles offer trustworthiness to the Missions they support.

To accomplish this intent, Medicaid must Frame, Assess, Respond, and Monitor risks to information resources, both internal to and external from Medicaid (i.e. OIT's network infrastructure and contracted systems interconnected with the Medicaid Enterprise network).

Medicaid Enterprise Risk management vs HIPAA Risk management

This Risk Management strategy overarches both Medicaid Enterprise Security Risk Management Activities (for which the Chief Information Security Officer is responsible) as well as HIPAA Risk Management Activities (for which the HIPAA Security Officer is responsible). Each concept mentioned in the Risk Frame, Assessment, Response, and Monitoring sections intends to account for both Medicaid Enterprise and HIPAA Risk Management Activities.

Risk Frame

The Risk Frame is applicable to all information security risks within the Organization, whether it be risks determined through Medicaid Enterprise Security Risk Assessments, through HIPAA Risk Assessments, Federal or State audits, or any other determination of risk.

Risk Assumptions

1. Information resources (IT system components, data, etc…) are deployed in constantly contested space. Even though certain IT systems or assets do not directly support the day-to-day business of the Organization, all IT assets are known targets of attack.
2. The number and complexity of cyber-attacks increases constantly, but the scale of these attacks can grow wildly beyond what the Agency can control without understanding its threat/vulnerability landscape.
3. Information is a strategic asset, although intangible, and must be protected just like any tangible asset.

4. IT assets have vulnerabilities that present varying degrees of risk: acceptable risk will be accepted (and allowed to continue to exist); unacceptable risk will be tracked until remediated or mitigated to an acceptable level.

Risk Constraints

1. Laws and Regulations place requirements on some systems and certain types of information and must be addressed.
2. A finite amount of resources exist to meet both operational needs and to provide required security.
3. Security Professionals are an expensive resource to obtain and retain – creating a shortage of qualified individuals.

Risk Priorities

1. System criticality and information sensitivity will drive the security resource allocation and risk decisions.
2. Emphasis will be placed on system operability if limited resources prevent full security testing of IT Assets.
3. IT Assets with highest criticality and information with the highest sensitivity will have the greatest focus of security testing, assessments, and risk decisions.

Risk Tolerance

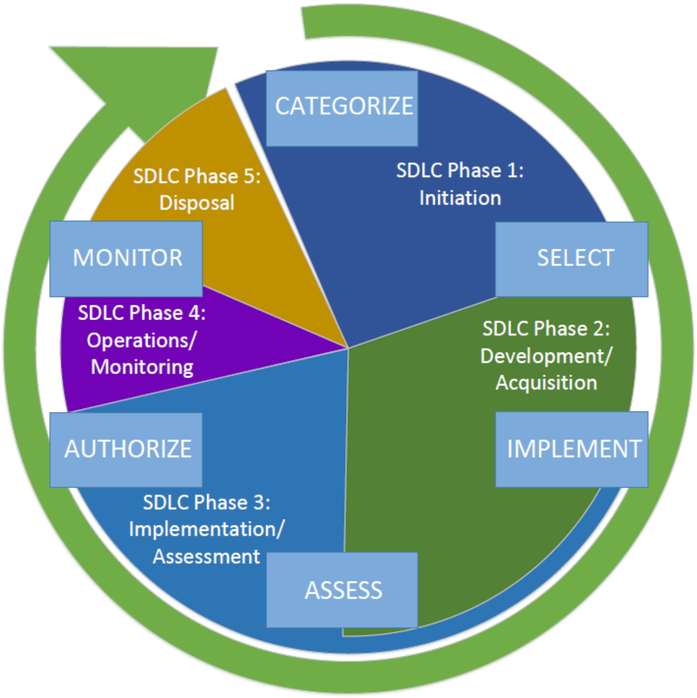
1. The MAXIMUM level of risk that will be accepted for any vulnerability or risk is **MODERATE** – this means that any risk documented in the Plan of Action and Milestones that is categorized as HIGH cannot be accepted and allowed to continue to exist without mitigation. This does NOT mean that all LOW and MODERATE vulnerabilities and risks will be accepted, only that they CAN be accepted when the resources or level of effort required to mitigate are higher than Organizational leadership can tolerate.
2. Risk to cost, schedule, performance, or security that could affect Medicaid or a line of business will be communicated to Management immediately.
3. If security or risk assessments must be conducted on short time lines, a limited subset of security controls that are agreed upon by Management will be tested – with the mindset of obtaining a minimal level of security assurance.

This Risk Frame describes management's assumptions, constraints, priorities, and tolerance of risk to the information resources of Medicaid. This explicit and transparent declaration allows for the risk assessment, risk response, and the risk monitoring methodologies to be conducted in line with Organizational risk expectations.

Risk Assessment

The Agency will perform **Security Assessments** on its systems within the development, implementation, and operations phases of each system's System Development Lifecycle (SDLC). Alabama Medicaid Agency has documented its System Development Life Cycle standards in the Organization's implementation of the NIST 800-53, SA-3: System Development Life Cycle control. Assessment reports will be added to and updated within System Security Plans or Authorization packages (as described in PM-10: Authorization Process) for each individual Medicaid System. Alabama Medicaid has documented its Security Assessment methodology in the Organization’s implementation of the NIST SP 800-53, CA-2: Security Assessment controls.

See a depiction of the Agency SDLC model (with associated RMF steps) below:


CATEGORIZE
SDLC Phase 5: Disposal
SDLC Phase 1: Initiation
MONITOR
SELECT
SDLC Phase 4: Operations/ Monitoring
SDLC Phase 2: Development/ Acquisition
AUTHORIZE
IMPLEMENT
SDLC Phase 3: Implementation/ Assessment
ASSESS

The Agency will perform **Risk Assessments** biennially and will include a HIPAA Risk Assessment as well as a full NIST 800-30r1 Assessment of Risks from adversarial and non-adversarial threats. Alabama Medicaid has documented its Risk Assessment methodology in the Organization’s implementation of the NIST SP 800-53, RA-3: Risk Assessment controls.

Risk Response

As risks are determined, Medicaid responds to those risks in several different ways:

Avoid

Risk avoidance is the elimination of hazards, activities and exposures that can negatively affect the Agency's information resources. Risk avoidance seeks to avoid compromising events entirely.

Accept

Risk acceptance occurs when the Agency acknowledges that the potential loss from a risk is not great enough to warrant spending resources to avoid it. Risks greater than the Organization's Risk Tolerance are documented in the Risk Frame.

Mitigate

Risk mitigation is a strategy to prepare for and lessen the effects of threats, vulnerabilities, and their likelihood against the Agency's information resources. Rather than planning to avoid a risk, risk mitigation deals with the steps that can be taken prior to risk realization to reduce adverse effects.

Transfer

Risk transfer is a risk management tactic that shifts risk and its bottomline effects from one party to another.

Risks are responded to by each system's Authorizing Official. Risks can be reviewed in groups or individually as the Authorizing Official deems sufficient, but **Authorizing Officials or the Agency Commissioner are the only individuals that can accept risks of any severity**.

The formal acceptance of risk occurs by a system's Authorizing Official reviewing the Authorization Package (as described in PM-10: Authorization Process), then making a determination as to whether or not the System's Security posture aligns with the Agency's Risk Management Strategy and Tolerance of Risk.

Risk Monitoring

Alabama Medicaid Agency maintains a continuous monitoring strategy that includes assessments in several events:

- Initial assessments during development and implementation of a system (prior to Authorization)
- Ongoing annual attestation of 1/3 of applicable controls
- Ongoing Configuration/Change Management events

Alabama Medicaid has documented its Risk Monitoring (or Continuous Monitoring) methodology in the Organization's implementation of the NIST SP 800-53, CA-7: Continuous Monitoring control.

Tools, Templates, and Reporting

Medicaid Systems

Systems that directly support the Alabama Medicaid Agency Mission; whether provided by in-house system development, vendor-provided system development, or commercial-off-the-shelf software or services will use the GRC Management Platform Telos Xacta instance managed by the Information

Security Office. All system security documentation and all Risk Management activities associated with Information Resources will be managed through the Information Security Office's GRC platform, whenever possible.

Non-Medicaid Systems

Systems that do not directly support the Agency's Mission, such as systems outside of the Agency that use Alabama Medicaid information through sharing agreements (Business Associated Agreement, Memorandum of Understanding, or Data Sharing Agreement) will use Agency supplied templates and adhere to the following reporting schedules:

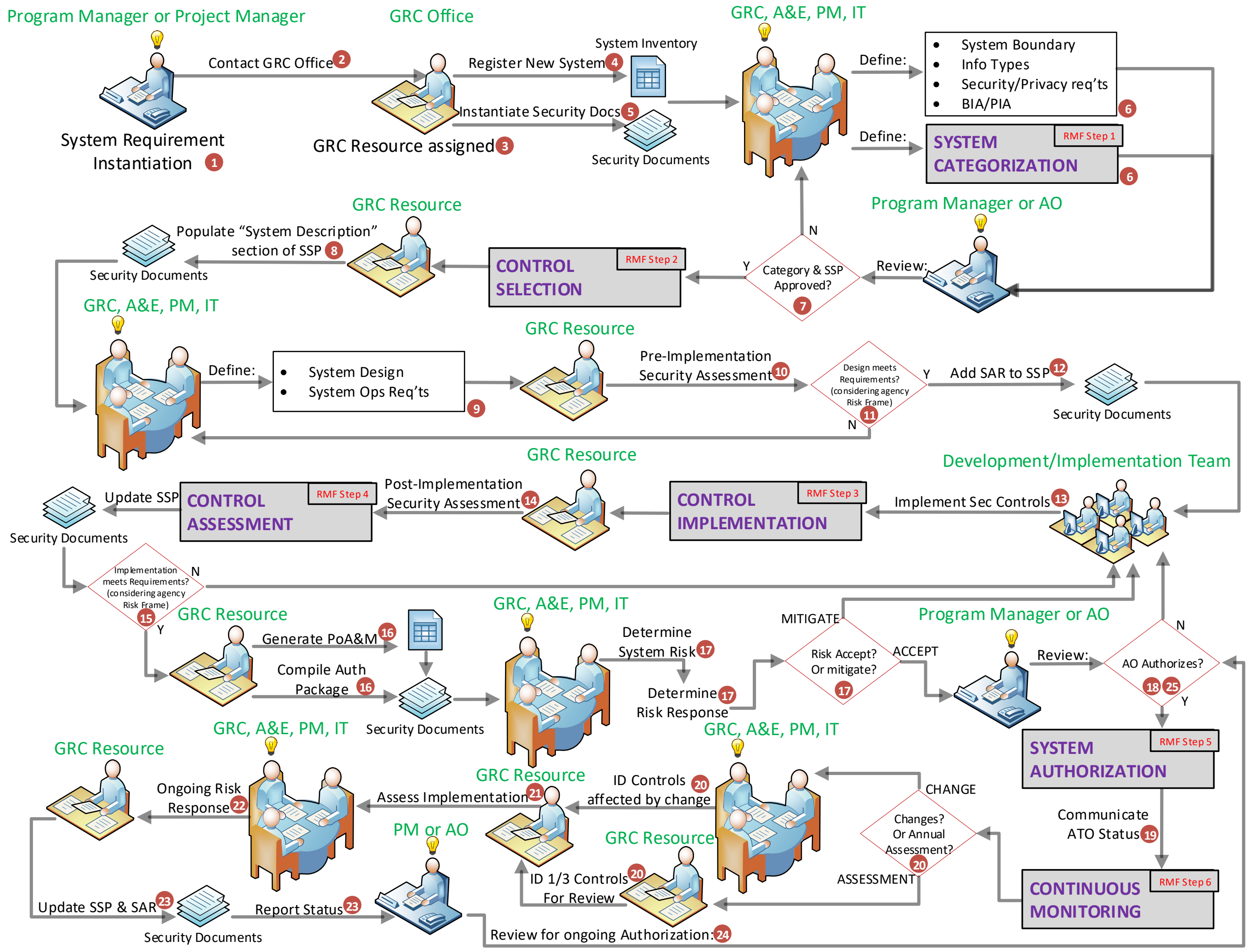
- Completed Authorization package and signed ATO – at moment of "production" status
- Updated SSP – Annually or whenever Major changes to system occur
- Updated PoAM – semi-annually (every 6 months)
- Updated SAR – every 3 years (as part of ATO re-auth)

General Practice/Workflow

Medicaid's Risk Frame sets the precedent and expectations of leadership regarding risk within the Organization. However, the Risk Assessment, Risk Response, and Risk Monitoring sections of this Risk Management Strategy are activity-based requirements that happen in the six steps of the Risk Management Framework (depicted in the SDLC model as: Categorize, Select, Implement, Assess, Authorize, and Monitor). This workflow implements the 6-step NIST Risk Management Framework for Alabama Medicaid Agency.

These activities are documented in a high level Risk Management workflow in both a visual depiction and step by step listing of the work flow illustrated below.

See the visual depiction of the workflow below:



See the step by step listing of the workflow below:

Step 1 - Categorize Information System

See RA-2: System Categorization requirements.

1. System need is determined, decision to instantiate system is made – by Authorizing Official
2. Communication is initiated with the GRC Office – by Program Manager or Project Manager
3. Assign GRC Resource to System – by GRC Team Lead
4. Register System in System Inventory – by GRC Resource
5. Instantiate System Security Documents from Template – by GRC Resource
6. Define System Boundary, Information Types, Security/Privacy Requirements; perform BIA/PIA; Categorize System – through collaboration and agreement of GRC, Security Architecture and Engineering, PM, and IST Support Teams
7. Review categorization results and System Security Plan (SSP); if approved continue to task 8, if not approved loop back to task 6 – by Authorizing Official

Step 2 - Select Security Controls

PL-10: Baseline Selection requirements scheduled to be implemented in an upcoming phase of the Security Program Plan.

8. Populate "System Description" section of SSP using information defined in task 6 – by GRC Resource
9. Select Required security controls based off of System Categorization and other requirements, according to details specified in PL-10: Baseline Selection; define System Design; define System Operational Requirements; populate "System Design" and "System Ops Requirements" sections of SSP – through collaboration and agreement of GRC, Security Architecture and Engineering, PM, and IT Support teams
10. Perform pre-implementation Security Assessment of theorized system – by GRC Resource
11. Considering the Agency Risk Frame/Tolerance, if System Design meets requirements, continue to task 12; if system design does not meet requirements loop back to task 9 – by GRC Resource
12. Add Security Assessment Report to SSP – by GRC Resource.

Step 3 - Implement Security Controls

13. Implement required Security Controls during system implementation – Development/Implementation Team.

Step 4 - Assess Security Controls

See CA-2: Assessments Requirements.

14. Perform post-implementation Security Assessment of Implemented System; update Security documents – by GRC Resource.
15. Considering the Agency Risk Frame/Tolerance, compare post-implementation assessment results with pre-implementation assessment requirements; if Implemented system meets design requirements continue to step 16; if implemented system does not meet design requirements loop back to step 13 to perform remediation actions – by GRC Resource.

Step 5 - Authorize Information System

See PM-10: Authorization Process Requirements.

16. Generate Plan of Action and Milestones based off of post-implementation Security Assessment findings, compile Authorization Package, deliver Authorization Package to Authorizing Official – by GRC Resource.
17. Review Authorization Package to determine system risk; generate Risk Assessment Report (incorporate latest Agency Risk Assessment results from RA-3: Risk Assessment); determine risk response to system risk; if risk response is “accept,” continue to step 18; if risk response is “mitigate” loop back to step 13 to perform remediation actions - through collaboration and agreement of GRC, Security Architecture and Engineering, PM, and IT Support Teams.
18. Review Authorization Package; determine System Authorization status; if Authorization Status is “yes (Authorize/ATO),” even with conditions, continue to step 19; if Authorization status is “no (Deny Authorization/DATO)” loop back to step 13 to perform remediation actions – by Authorizing Official.
19. Authorize System to Operate; notify GRC, Security Architecture and Engineering, PM, and IT Support Teams of Operational Status – by Authorizing Official.

Step 6 - Monitor Security Controls

See CA-7: Continuous Monitoring, PM-5: Plan of Action and Milestones Process, and CA-5: Plan of Action and Milestones requirements.

20. Following Authorization to Operate (ATO):
    - If changes to the system occur, identify controls affected by change – through collaboration with GRC, Security Architecture and Engineering, PM, and IT Support Teams.
    - If Annual Assessments occur, based on priority and most recent review, identify 1/3 of controls for review – by GRC Resource.
21. Assess implementation of identified controls – by GRC Resource.
22. Perform ongoing risk response to findings identified in ongoing security assessments – through collaboration with GRC, Security Architecture and Engineering, PM, and IT Support Teams
23. As findings are remediated and changes occur to the System Security Plan, update Security Documentation; report system security status and system risk to Program Manager or Authorizing Official – by GRC Resource.
24. Review system security status and system risk for ongoing authorization – by Program Manager or Authorizing Official.
25. Periodically determine system Authorization Status; If Authorization Status is “yes (Authorize/ATO),” even with conditions, loop to step 19; if Authorization Status is “no (Deny Authorization/DATO),” loop back to step 13 to perform remediation actions – by Authorizing Official

Conclusion

This Risk Management Strategy describes, at a high level, Medicaid’s Risk Frame, Risk Assessment, Risk Response, and Risk Monitoring methodologies. These requirements are met with more specific procedures, templates, authorizations, etc… within the Medicaid Enterprise Security policies and procedures. These are put into practice through the implementation of an RMF-based workflow.

Management Commitment

The undersigned, as the Chief Information Officer of Alabama Medicaid Agency, exercising the power of that office, declares this Risk Frame to be available for adoption as of the 20th day of July, 2020.

Mason L. Tanaka

Alabama Medicaid Agency, Chief Information Officer