
	Assessment, Authorization and Monitoring Policy		
ID-IM-P1			
Effective Date: 01/31/2025	Date Approved: 01/15/2025	Version: 1	Page #: 1 of 8

GOVERNANCE

This document is governed by the IT Governance policy which provides the following guidance:

- a. Roles and Responsibilities;
- b. Policy Control Application;
- c. Policy Compliance Requirements;
- d. Policy Exemptions or Exceptions; and
- e. Policy Reviews and Updates.

SCOPE

This policy covers all State information and information systems to include those used, managed, or operated by a contractor, an agency, or other organization on behalf of the State. This policy applies to all State employees, contractors, and all other users of State information and information systems that support the operation and assets of the State.

CA-1 – Policy and Procedures

This document addresses the requirements set forth by the State to implement the family of Assessment, Authorization and Monitoring security controls at the organization, process, and/or system level for all information assets.

The Assessment, Authorization and Monitoring process is implemented to ensure compliance with State information security policies and is critical to minimizing the threat of breaches. Security assessments are conducted to ensure correct controls are implemented, operating as intended, and meeting the information security requirements for the system.



Authorization is the process of accepting the residual risks associated with the continued operation of a system and granting authorization to operate for a specified time.

Authorizations to Operate (ATOs) information technology assets shall be controlled and managed to ensure that only authorized systems including workstations, servers, cloud computing applications, software applications, mobile devices, networks, and data repositories are implemented for business needs.

The State has adopted the Assessment, Authorization and Monitoring principles established in the NIST SP 800-53 “Assessment, Authorization and Monitoring,” control guidelines, as the official policy for this security domain. The “CA” designator identified in each control represents the NIST-specified identifier for the Assessment, Authorization and Monitoring control family. A designator followed by a number in parenthesis indicates a control enhancement that provides statements of security and privacy capability that augment a base control. Only those control enhancements associated with the moderate level controls are listed. Should an Executive Branch agency be required to address other control enhancements for a control item, the organization will be responsible for writing an additional policy to meet that requirement.

The following subsections in this document outline the Security Assessment and Authorization requirements each State information system must implement and maintain to be compliant with this policy.

This policy and associated procedures shall be reviewed and updated at least every three years, unless Federal, State, or agency defined events require a more frequent review.

	Assessment, Authorization and Monitoring Policy		
ID-IM-P1			
Effective Date: 01/31/2025	Date Approved: 01/15/2025	Version: 1	Page #: 2 of 8



CA-2 - Control Assessments

Risk associated with each business system shall be assessed to determine applicable security requirements. Organizations shall select the appropriate assessor or team for the type of assessment to be conducted.

Control assessments determine the appropriate placement of each system and application within the security framework and evaluate the network resources, systems, data, and applications based on criticality.

Security measures protecting data and applications shall increase commensurately with their criticality. Control assessments shall:

- a. Be performed under a Continuous Monitoring Plan supporting a frequency defined by OIT at least annually or when significant changes occur to the system or supported environment; until system decommissioning. The Continuous Monitoring plan shall be reviewed and approved by the agency head or designated representative prior to conducting the assessment.
- b. Agencies shall provide evidence of their annual compliance and assessments to OIT through the ServiceNow Audit workflow. This certification includes compliance of cloud service providers.
- c. Deficiencies identified within the agency shall be addressed. Reports must be submitted using approved secure methods.
- d. Annual reports shall ensure the agency identifies its security deficiencies and estimated cost for remediation. The report shall include, but is not limited to, the following:
 - i. Security boundary devices, e.g., firewalls, Intrusion Detection/Prevention Systems (IDS/IPS);
 - ii. Vulnerability management, e.g., scanning, and patching systems;
 - iii. Resource constraints;
 - iv. Cybersecurity training deficiencies; and
 - v. System development lifecycle (SDLC) deficiencies.
- e. Before significant changes are made to an information system, a Security Impact Analysis (SIA) shall be conducted to determine how the changes will affect system security. These analyses are conducted as part of the System Development Lifecycle (SDLC) to ensure security and privacy requirements are identified and addressed during system development and testing.
- f. Agencies shall follow the procedures below when significant changes are made to the information system:
 - i. Document assessment results and include correction or mitigation recommendations to enable risk management and oversight activities;
 - ii. Provide the results to OIT within thirty (30) days of assessment completion;
 - iii. The controls in the information system shall be assessed at least annually to ensure the controls are implemented correctly, operating as intended, and meeting system security and privacy requirements; and
 - iv. Cloud vendors must provide an attestation of compliance via an independent third-party assessment report. Executive Branch agencies may include more restrictive requirements than the State's, such as agency defined policies, standards, and other additional controls.

	Assessment, Authorization and Monitoring Policy		
ID-IM-P1			
Effective Date: 01/31/2025	Date Approved: 01/15/2025	Version: 1	Page #: 3 of 8

CA-2 (1) - Control Assessments | Independent Assessors

Third-party assessors or assessment teams may be employed to conduct control assessments. Independent assessors or assessment teams are individuals or groups who conduct impartial assessments of information systems. Assessor independence provides a degree of impartiality to the process. To achieve impartiality, assessors should not:

- a. Create a mutual or conflicting interest with the organizations where the assessments are being conducted;
- b. Assess their own work;
- c. Act as management or employees of the organizations they are serving; or
- d. Place themselves in positions of advocacy for the organizations acquiring their services.



Independent assessments are typically contracted from public or private sector entities outside of the organization. These independent assessments may be conducted by OIT personnel or contracted for with a third-party vendor. In either situation, each agency will be financially responsible for the assessment.

CA-3 - Information Exchange

Note: This control applies only to dedicated connections between information systems.

All information systems must use approved and managed information exchange agreements for each information system connecting to other information systems (external to the agency). These agreements may include but are not limited to: Interconnection Security Agreements (ISAs), Business Associate Agreements (BAAs), Memorandums of Understanding (MOUs), or Memorandums of Agreement (MOAs). For all information exchange agreements, each agency must ensure the following items are included with detail:

- a. As part of each exchange agreement, document:
 - i. All interface characteristics;
 - ii. Security and privacy requirements, controls, and responsibilities for each system;
 - iii. Costs incurred under the agreement; and
 - iv. The nature of the information communicated.
- b. Employ a deny-all and allow-by-exception policy for allowing systems that receive, process, store, or transmit data to connect to external information systems.
- c. Follow the procedures below for connections to systems outside of the State Network:
 - i. Establish an approved agreement signed by the Secretary of Alabama Office of Information Technology or other State-defined designee or Agency head;
 - ii. Submit a connection request to the OIT Service Desk (service.desk@oit.alabama.gov). The request must include the following:
 1. Type of connection to be established;
 2. Type connection requirements;
 3. Key personnel to coordinate the planning efforts of the system interconnection;
 4. Duration of the interconnection; and
 5. Point of contact for the external organization requesting the interconnection of data and level of sensitivity of the data being exchanged.
 - iii. Prior to system interconnection, system owners must complete a security impact analysis. The results must be provided to the Agency head for risk determination and approval.

	Assessment, Authorization and Monitoring Policy		
ID-IM-P1			
Effective Date: 01/31/2025	Date Approved: 01/15/2025	Version: 1	Page #: 4 of 8

- iv. Review and update ISAs at least annually or whenever there is a significant change to any of the interconnected systems.
- v. Terminate all interconnections when any of the following conditions exist:
 - i. The ISA, MOU, or MOA has expired or is withdrawn;
 - ii. The business requirement for the interconnection no longer exists; and
 - iii. A significant change in the environment increases the risk to an unacceptable level of operations.



CA-5 – PLAN OF ACTION AND MILESTONES

When deficiencies are discovered in the security posture of systems, a Plan of Action and Milestones (POAM) shall be developed for each system and shall:

- a. Document planned remedial actions to correct weaknesses or deficiencies noted during the controls assessment and to reduce or eliminate known vulnerabilities in the system.
- b. Update existing action plans and milestones based on the findings from controls assessments, independent audit reviews, and continuous monitoring activities.
- c. The following information shall be included in each POAM:
 - i. Type of weakness;
 - ii. Identity of the Agency, Office, or organization responsible for resolving the weakness;
 - iii. Estimated funding required for resolving the weakness;
 - iv. Scheduled completion date for weakness remediation or mitigation;
 - v. Key milestones with completion dates;
 - vi. Source of weakness discovery;
 - vii. Status of the corrective action; and
 - viii. Security Incidents.

CA-6 – Authorization

- a. All information systems must have a senior-level executive responsible for the information asset and who shall ensure:
 - i. The responsible individual accepts the use of common controls inherited by the system and authorizes the information asset for processing, e.g., Authority to Operate (ATO), before the system commences operations.
 - ii. The information system meets State, Federal and other mandates for compliance at least annually.
 - iii. Authorization levels shall be reviewed and updated regularly to prevent disclosure of information through unauthorized access.
- b. All responsible parties shall consider if granting authorization to use a system utility could violate segregation controls, and the State shall enact precautions to ensure that this violation does not occur.
- c. System documentation and user procedures shall be updated to reflect changes based on the modification of applications, data structures and/or authorization processes.
- d. Access shall require authentication and authorization to access needed resources, and access rights shall be regularly reviewed.

	Assessment, Authorization and Monitoring Policy		
ID-IM-P1			
Effective Date: 01/31/2025	Date Approved: 01/15/2025	Version: 1	Page #: 5 of 8



CA-7 – CONTINUOUS MONITORING

A program for system-level continuous monitoring and auditing shall be implemented to detect unauthorized activity and should support the organization-level continuous monitoring strategy to include cloud environments, whether hosted by contracted vendors or State managed.

All hardware connected to the State information network or cloud hosted shall be configured to support State/agency management and monitoring standards.

All organizations shall complete an annual risk and security assessment of their critical systems and infrastructure to ensure ongoing processes are assessing the current posture of the environment. Continuous Monitoring ensures all agencies are assessed at least annually and includes the following:

- a. A configuration management process for the information system and its constituent components.
- b. A determination of the security impact of changes to the information system and operating environment.
- c. Ongoing control assessments must include the following:
 - a. Performance metrics concerning the status of control compliance and corrective actions required for identified control gaps.
 - b. Development of a process to evaluate supporting documentation.
 - c. The time required to monitor assessment recommendations.
 - d. A schedule for assessing critical systems on an annual basis.
 - e. Security and Privacy status results reporting to be provided to the agency AO at least annually or upon any significant system changes.
 - f. Coordination between the agencies and OIT to address residual risks for those controls that cannot be implemented.
- d. Business Owners and System Owners, in coordination with Agency CIOs, CISOs and stakeholders for State data residing in non-state locations (e.g., cloud or off-site hosted systems) shall ensure the following:
 - a. Agencies shall ensure vendor compliance with State, and if applicable, Federal, security policies by obtaining a vendor agreement prior to contract approval;
 - b. Implement the Continuous Monitoring Plan; and
 - c. For vendor hosted systems/solutions that will have Sensitive or Confidential data, the State shall obtain at least one of the following independent third-party certifications from the vendor before contract award and one annually thereafter:
 - i. Federal Risk and Authorization Management Program (FedRAMP) authorization certificate (or equivalent);
 - ii. State Risk and Authorization Management Program (StateRAMP) authorization certificate (or equivalent);
 - iii. Service Organization Controls (SOC) 2 Type 2;
 - iv. International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27001 Information Security Management Standard; or
 - v. HITRUST Common Security Framework (HCSF).
 - vi. SaaS vendors cannot use IaaS/PaaS certifications unless the application is explicitly covered as part of those assessments.

	Assessment, Authorization and Monitoring Policy		
ID-IM-P1			
Effective Date: 01/31/2025	Date Approved: 01/15/2025	Version: 1	Page #: 6 of 8

- d. Correlate and analyze system level security-related information generated by assessments and monitoring to identify weaknesses and develop corrective actions;
- e. Report system level security and privacy status to the OIT Director of Security Operations; and
- f. Demonstrate to the State that ongoing continuous monitoring activities are in place and compliance is being met for:
 - i. Security
 - ii. Privacy and Confidentiality
 - iii. Availability (Business Continuity Management)
 - iv. Processing integrity

CA-7 (1) – Continuous Monitoring | Independent Assessment

Third-party independent assessors or assessment teams shall be employed to provide continuous monitoring of the controls in information systems. An independent third-party assessor is an entity separate from the agency and/or vendor being accessed and can provide an objective opinion on an information system.

CA-7 (4) Continuous Monitoring | Risk Monitoring

Risk monitoring shall be an integral part of the continuous monitoring strategy / plan and shall include:

- a. Effectiveness monitoring;
- b. Compliance monitoring; and
- c. Change monitoring.

CA-8 – PENETRATION TESTING

All systems containing Sensitive or Confidential data shall have a penetration test performed by an independent third-party assessor at least tri-annually unless exigent circumstances require a more frequent review. This may be part of a third-party assessment/certification, e.g., SOC 2 Type 2.

Endpoint threat monitoring of all devices shall be required including services within the cloud.



CA-9 – INTERNAL SYSTEM CONNECTIONS

Security compliance checks must be performed between information systems and (separate) system components (e.g., intra-system connections) including but not limited to: system connections with mobile devices, notebook/desktop computers, printers, copiers, scanners, sensors, and servers.

Instead of authorizing each individual internal connection, internal connections for a class of components with common characteristics and/or configurations may be authorized.

For enterprise solutions, the State shall:

- a. Establish classes and subclasses of components permitted for internal system connections.
- b. Develop baseline configurations for each component class and subclass.
- c. Define interface characteristics and security and privacy standards for each component class and subclass connection type by State-defined categorization standard – Moderate or Low.
- d. Terminate internal system connections after agency-defined conditions.

	Assessment, Authorization and Monitoring Policy		
ID-IM-P1			
Effective Date: 01/31/2025	Date Approved: 01/15/2025	Version: 1	Page #: 7 of 8

e. Review the continued need for each internal connection on an agency-defined frequency.

Agency Business/System Owners shall only implement the established classes and sub-classes of components according to baseline configurations and security and privacy requirements. Any deviations must be submitted through the State's Exception Process.

POLICY OWNER

Secretary of Office of Information Technology (OIT)

MATERIAL SUPERSEDED

This current policy supersedes all previous versions of the policy. All State agencies and vendors of the State are expected to comply with the current implemented version of this policy.



Assessment, Authorization and Monitoring Policy



ID-IM-P1

Effective Date:
01/31/2025

Date Approved:
01/15/2025

Version:
1

Page #:
8 of 8

REVISION HISTORY

Revision Date	Summary of Change
12/31/2024	Policy Update

REMAINDER OF PAGE LEFT INTENTIONALLY BLANK



Assessment, Authorization and Monitoring Policy



ID-IM-P1

Effective Date:
01/31/2025

Date Approved:
01/15/2025

Version:
1

Page #:
9 of 8

APPROVED BY

Signature	<i>Daniel Urquhart</i>
Approved by	Daniel Urquhart
Title	Secretary of Office of Information Technology (OIT)
Date Approved	01/15/2025

REMAINDER OF PAGE LEFT INTENTIONALLY BLANK