Division of Enterprise Technology Strategy and Services

ETSS Policy 300.6

Assessment, Authorization, and Continuous Monitoring (CA)

Publish Date: 15 July 2026
Effective Date: 15 July 2026
Last Review: 14 July 2026

doa.entsec@doit.ri.gov

1. Purpose

Establish policy for implementing a comprehensive continuous monitoring program that ensures ongoing visibility into the security posture of State of Rhode Island information systems. The program provides real-time and periodic monitoring of security controls, vulnerabilities, threats, and incidents, enabling proactive risk management and timely response to adverse events. Continuous monitoring activities—such as vulnerability scanning, log analysis, control assessments, and automated security alerts—equip enterprise and agency personnel with the situational awareness necessary to safeguard the confidentiality, integrity, and availability of State information systems and data.

This policy directly supports the Govern and Detect functions of the NIST Cybersecurity Framework (CSF) 2.0 by embedding monitoring responsibilities into daily operations and ensuring risks are identified and addressed before they escalate into significant incidents. Additionally, this policy incorporates Complementary User Entity Controls (CUECs) by explicitly recognizing the shared responsibility between the enterprise security teams, agency personnel, and third-party service providers in maintaining continuous oversight of security controls. The policy also aligns with the State's ETSS Security and Risk Program (PM-1), which establishes a statewide risk management framework based on the NIST Risk Management Framework (RMF) and NIST SP 800-53 moderate baseline, by ensuring that assessment, authorization, and monitoring controls (CA family) are consistently implemented, maintained, and measured across all agencies under the coverage of Enterprise Technology Strategy and Services (ETSS) technology outlined in the applicability section.

2. Applicability

This policy is applicable to all State of Rhode Island Executive Branch Departments1 (including agencies, boards and commissions), and their employees (including permanent, non-permanent, full-time, and part-time) and interns, consultants, contractors, vendors, contracted individuals, and any entity having access to state information systems and data, whether operated or maintained by the state or on behalf of the state. For this policy, the term "Agency" is used to refer to any department, agency, division, or unit of the Executive branch of the State of Rhode Island.

3. Definitions

NIST Cybersecurity Framework (CSF)

A voluntary, risk-based framework developed by the National Institute of Standards and Technology (NIST) that provides common standards, guidelines, and best practices to help organizations identify, protect, detect, respond to, and recover from cybersecurity risks. The CSF 2.0 expands these activities into the Govern, Identify, Protect, Detect, Respond, and Recover functions, establishing a flexible model for managing enterprise cybersecurity risk.

NIST SP 800-53

A catalog of security and privacy controls maintained by NIST that provides a structured baseline for protecting federal information systems and organizations. The controls are organized into control families (e.g., Access Control, Awareness and Training, Incident Response) and are tailored based on impact level (Low, Moderate, High). The State of Rhode Island applies the Moderate baseline (Rev. 5) as its primary control standard across managed systems, supplemented by overlays as required.

NIST Risk Management Framework (RMF)

A structured process defined in NIST SP 800-37 that integrates information security, privacy, and risk management into the system development life cycle. The RMF provides steps for categorizing systems, selecting controls, implementing safeguards, assessing effectiveness, authorizing operations, and continuously monitoring security posture.

Complementary User Entity Controls (CUECs)

Controls that users are required to perform to support the effectiveness of enterprise or vendor-provided security controls. CUECs typically arise from third-party assurance frameworks but are applied in State policy to emphasize shared responsibility. For example, while ETSS may provide enterprise annual training, agency users are responsible for completing the security training, and following rules of behavior, and reporting incidents promptly.

Information Assurance Level (IAL)

Categorization used by the State of Rhode Island to determine the security requirements of an information system, based on the sensitivity of the data it processes, stores, or transmits.

Continuous Monitoring

An ongoing process of collecting, analyzing, and reporting information on the security state of information systems to maintain situational awareness of risks, threats, and vulnerabilities, and to enable timely risk-based decisions.

Security Information and Event Management (SIEM)

A platform that aggregates and correlates security-related events and logs across enterprise and agency systems for analysis, alerting, and reporting.

Vulnerability Scanning

Automated or manual scanning of information systems to identify known security weaknesses or misconfigurations that could be exploited.

Security Control Assessment (SCA)

The evaluation of the effectiveness of specific security controls to determine if they are implemented correctly, operating as intended, and producing the desired outcome.

4. Procedures for Compliance

Security controls in this policy will be implemented in accordance with the security categorization of the information system. The security categorization is based on the Information Assurance Level (IAL) requirements of the information system.

Low Risk Systems (IAL1)

Information systems that only contain data that is public by law or directly available to the public via mechanisms such as the internet. In addition, desktops, laptops, and supporting systems used by agencies are Low Risk unless they store, process, transfer, or communicate

private or sensitive data.

Moderate Risk Systems (IAL2)

Information systems that store, process, transfer, or communicate private or sensitive data or have a direct dependency on a Moderate system. At a minimum, any information system that stores, processes, transfers, or communicates PII or other sensitive data types is classified as a Moderate system.

4.1. [IAL1, IAL2] Continuous Monitoring Policy and Procedures (CA-7) ETSS will develop, document, disseminate to designated personnel defined in the applicable system security plan, review, and annually update a continuous monitoring policy and procedures.

a. Continuous monitoring responsibilities apply at both the enterprise and agency levels:
    i. Enterprise Responsibilities: ETSS is responsible for establishing statewide continuous monitoring standards, tools, and reporting mechanisms; aggregating and analyzing monitoring data; and coordinating enterprise-wide risk response activities.
    ii. Agency Responsibilities: Agencies are responsible for implementing continuous monitoring processes within their systems, reporting results to ETSS, and ensuring monitoring activities are integrated with agency risk management, incident response, and contingency planning efforts.
    iii. Third-Party and Shared Services: Contractors, vendors, cloud providers, and other third parties with access to State information systems must comply with ETSS continuous monitoring requirements as documented in contracts or Service Level Agreements (SLAs).

4.2. [IAL1, IAL2] Continuous Monitoring Strategy

ETSS will:

a. Establish and implement a strategy for monitoring security controls, including the frequency of monitoring, assessment methods, and reporting mechanisms.
b. Identify security controls to be monitored continuously, such as access control, configuration management, vulnerability management, and incident response.
c. Define roles and responsibilities for personnel with continuous monitoring duties.
d. Ensure that monitoring results inform risk assessments, authorization decisions, and system security plan updates

4.3. [IAL1, IAL2] Vulnerability Scanning

ETSS will:

a. Perform automated vulnerability scans of information systems no less than quarterly, and after significant changes, using enterprise-approved tools.
b. Document scanning results and provide dashboards and reporting to enterprise support teams, system owners, and agency support teams for resolution.

System Owners and/or Agency Support Teams will:

a. Remediate or mitigate identified vulnerabilities based on risk, with high-risk vulnerabilities addressed within agency-defined timelines.
b. Document scanning results and report findings to ETSS and agency information security managers.

4.4. [IAL1, IAL2] Security Event Monitoring

ETSS will:

a. Monitor for anomalous or suspicious activity, including unauthorized access attempts, changes to critical configurations, and signs of insider or external threats.
b. Retain monitoring records in accordance with State General Records Retention Schedules and compliance requirements.

System Owners and/or Agency Support Teams

a. Forward applicable security logs to the Enterprise SIEM for analysis and correlation.

4.5. [IAL1, IAL2] Ongoing Assessment and Reporting

ETSS will:

a. Assess the effectiveness of selected controls at least annually, and more frequently for controls deemed critical or high-risk.
b. Produce security status reports that summarize continuous monitoring results and share with agency teams, ETSS, and stakeholders.
c. Assess the effectiveness of system controls at least annually, and during major changes.
d. Update Plans of Action and Milestones (POAMs) within timelines outlined within ETSS Risk Assessment policy for identifying deficiencies through continuous monitoring activities.

4.6. [IAL1, IAL2] Integration with Risk Management

ETSS will:

a. Integrate continuous monitoring results into security reviews, incident response activities, contingency planning, and governance actions.

5. Approval / Review Signature:

Digitally signed by Nathan Loura
Date: 2026.07.29 13:41:45 -04'00'

Chief Information Security Officer (CISO)
Division of Enterprise Technology Strategy and Services

Brian Tardiff
Digitally signed by Brian Tardiff
Date: 2026.07.29 13:54:37 -04'00'

Chief Digital Officer (CDO)
Division of Enterprise Technology Strategy and Services