Division of Enterprise Technology Strategy and Services

ETSS Policy 300.13

Cybersecurity and Risk Program Management (PM-1)

Publish Date: 7/29/2026
Effective Date: 7/29/2026
Last Revision Date: 07/29/2026

doa.entsec@doit.ri.gov

1. Purpose

To establish a statewide Cybersecurity & Risk Management Program that embeds confidentiality, integrity, and availability into the design, implementation, and maintenance of Rhode Island's information systems and network infrastructure. The program protects constituent data across State-managed and third-party environments; provides a consistent, repeatable governance framework to assess, authorize, and connect IT assets; and supports enterprise standards that manage technology risk, improve consistency, and increase accessibility.

This policy supports the NIST Cybersecurity Framework (CSF) 2.0—primarily the GOVERN and PROTECT functions and, through continuous monitoring and incident response, the DETECT, RESPOND, and RECOVER functions. It also incorporates Complementary User Entity Controls (CUECs) by recognizing the shared-responsibility model between enterprise services and agency personnel. The program is implemented via the NIST Risk Management Framework (RMF) and uses NIST SP 800-53 Rev.5 Moderate as the statewide control baseline unless otherwise required by law or federal partner overlays.

2. Applicability

This policy is applicable to all State of Rhode Island Executive Branch Departments[1] (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

a. 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.

b. 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.

c. 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.

d. 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, following rules of behavior, and reporting incidents promptly.

e. Information Assurance Level (IAL) - A 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.

f. Assessment - The process of identifying the risks to system security and determining the probability of occurrence, the resulting impact, and additional safeguards that would mitigate this impact.

g. Audit - The review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures.

h. Breach - An incident where information is stolen or taken from a system without the knowledge or authorization of the system's owner.

i. Control - A safeguard or countermeasure prescribed for an information system or an organization designed to protect the confidentiality, integrity, and availability of its information and to meet a set of defined security requirements.

j. Federal Tax Information (FTI) - FTI includes return or return information received directly from the IRS or obtained through an authorized secondary source, as well as any information derived from federal returns or return information.

k. Information Technology (IT) Governance
A defined, integrated, and sequenced set of processes and workflows that establishes authority, management, and decision-making parameters to ensure Network Resources and related services

are well architected, procured, deployed, managed, monitored, and secured throughout the enterprise in a standardized manner

l. Payment Card Industry (PCI) - PCI Data Security Standard protects cardholder data, which includes sensitive data that is printed on a card or stored on a card's magnetic stripe or chip – and personal identification numbers entered by the cardholder.

m. Personally Identifiable Information (PII) - is information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual.

n. Plan of Action and Milestones (POAMs) - A formal management document used to track identified security weaknesses, the corrective actions to remediate them, assigned responsibilities, and target completion dates. POAMs provide accountability, support continuous monitoring, and demonstrate compliance with NIST SP 800-53 CA-5 and State ETSS requirements.

o. Risk - A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of the adverse impacts that would arise if the circumstance or event occurs, and the likelihood of occurrence.

p. System - Any organized assembly of resources and procedures united and regulated by interaction or interdependence to accomplish a set of specific functions. Systems also include specialized systems such as industrial/process controls systems, telephone switching and private branch exchange (PBX) systems, and environmental control systems.

4. Roles & Responsibilities

4.1. Program Ownership – Chief Digital Officer (CDO). Approves frameworks, support models, technologies, processes, and staffing necessary for program execution.

4.2. Program Execution, Oversight & Maintenance – Chief Information Security Officer (CISO). The CISO and enterprise security teams will:

- Publish policies/standards; selects statewide baselines (NIST SP 800-53 Rev.5 Moderate by default).
- Run the RMF at enterprise scale (categorize, select, implement, assess, authorize, and monitor).
- Operate the statewide audit, assessment, and continuous monitoring program (dashboards, Plans of Actions and Milestones (POAMs), reporting).
- Designate common/inheritable controls and maintain Appendix A – Control Baselines.
- Coordinate overlays (IRS 1075, CJIS, HIPAA/MARS-E/ARC-AMPE, PCI, FedRAMP) and Zero Trust Architecture alignment

4.3. Enterprise Control Compliance – Chief Technology Officer (CTO) The CTO and enterprise technology teams will:

- Ensure enterprise platforms implement inheritable controls at the "low" default for all connected endpoints, with elevation for moderate systems as required (defined in Appendix B).
- Track exceptions centrally with enterprise POAMs; enforce configuration baselines, patch/vulnerability windows, logging, and endpoint protections.

4.4. Agency Systems Owner; Agency IT Manager (AIM) The system or data owner with the ETSS AIM supporting the agency will:

- Protect agency data; accept or mitigate residual risks identified.
- Advise non-technology system users and ensures local implementation of required controls for IAL1/IAL2 systems; maintains system risk artifacts, assessments/audits, and POAMs; coordinates exception requests with CISO.

4.5. Agency Technical Support Manager (TSM) The ETSS TSM supporting the agency will:

- Implements and validates local/system-specific and hybrid controls; supports audits/assessments; escalates exception needs to AIM/Owners

5. Procedures for compliance

5.1. Adoption of NIST RMF and Control Frameworks. The State adopts NIST SP 800-37 RMF and utilizes NIST SP 800-53 Rev.5 controls (Moderate baseline as default). Control implementation shall follow the principles of least privilege, zero trust, defense-in-depth, and secure-by-design.

5.2. Security Categorization & Baseline Tailoring. Systems shall be categorized as IAL1 (Low) or IAL2 (Moderate) based on data sensitivity and mission impact. Baselines may be tailored to add/strengthen controls, apply overlays, or remove controls only where justified by documented risk decisions and approved by the CISO. The statewide control baseline and tailoring guidance are maintained in Appendix A

5.3. Control Inheritance & CUECs. Enterprise common controls (e.g., identity, endpoint protection, email security, logging) are inheritable when the system is managed by ETSS or approved third party outside the agency boundary and has been designated as inherited in system security plan (SSP) or another security configuration artifact.

5.3.1. Hybrid and system-specific responsibilities must be documented in the System Security Plan (SSP) or another security configuration artifact.

5.4. System Security Plans (SSPs) & Authorization. All IAL2 systems—and IAL1 systems where required by regulation or business risk—must maintain an SSP or control implementation evidence and authorization artifacts (Security Assessment Reports or POAMs).

5.5. Continuous Monitoring (ConMon). Agencies and enterprise providers must participate in statewide ConMon including endpoint/host sensors, vulnerability scanning, configuration/state compliance, log collection/retention, alerting, and reporting.

5.5.1. The CDO and CISO will require installation of monitoring/auditing agents on any device connected to State networks or processing State data.

5.5.2. Findings feed enterprise and agency POAMs with tracked remediation timelines and risk acceptance where applicable.

5.6. Information Protection & Data Handling. Agencies shall implement safeguards commensurate with data classification, including identity proofing (where required), MFA, encryption in transit/at rest, data loss prevention, least privilege, and secure collaboration controls.

5.6.1. Sensitive data (e.g., PII, FTI, PCI, CJIS, HIPAA/MARS-E/ARC-AMPE) must be handled by controlling statutes/agreements, applicable overlays, and ETSS policy.

5.6.2. Breaches or suspected compromises must be reported and handled IAW *ETSS Policy 300.8, Cybersecurity Incident Handling and Response* and applicable law.

5.7. Supply Chain Risk Management (SCRM). Technology acquisitions and external services must meet SCRM policy requirements, including supplier due diligence, secure development expectations, support lifecycles, SBOMs (when applicable), and component authenticity.

5.8. Configuration & Vulnerability Management. Systems must implement and adhere to ETSS secure configurations, standard images, change control, and timely patching aligned to risk. Unsupported components require CISO-approved exceptions and mitigation in alignment with SA family controls.

5.9. Training & Awareness. All users will complete security awareness training; personnel with security-significant roles complete role-based training as defined by the ETSS Awareness and Training policy.

5.10. Exceptions and Risk Acceptance. Where compliance is infeasible, an exception request with compensating controls and time-bound POAM must be submitted to the CISO. Risk acceptance requires Systems & Data Owner ownership, CTO and CISO approval, and CDO concurrence (for higher severity risks).

6. Related Policies and Frameworks

6.5. All ETSS published policies

6.6. NIST SP 800-37 Risk Management Framework https://csrc.nist.gov/projects/risk-management/risk-management-framework-(RMF)-Overview

6.7. NIST SP 800-53 Rev5 Security and Privacy Controls for Information Systems and Organizations https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

7. Approval / Review Signature:

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

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

Appendix A – Control Baselines & Mappings

CONTROL NO.	CONTROL NAME	INITIAL CONTROL BASELINES	
		LOW (IAL1)	MODERATE (IAL2)
ACCESS CONTROL			
AC-1	Access Control Policy and Procedures	AC-1	AC-1
AC-2	Account Management	AC-2	AC-2 (1) (2) (3) (4) (5) (13)
AC-3	Access Enforcement	AC-3	AC-3
AC-4	Information Flow Enforcement	OPTIONAL	AC-4
AC-5	Separation of Duties	OPTIONAL	AC-5
AC-6	Least Privilege	OPTIONAL	AC-6 (1) (2) (5) (7) (9) (10)
AC-7	Unsuccessful Logon Attempts	AC-7	AC-7
AC-8	System Use Notification	AC-8	AC-8
AC-9	Previous Logon Notification	OPTIONAL	OPTIONAL
AC-10	Concurrent Session Control	OPTIONAL	OPTIONAL
AC-11	Device Lock	OPTIONAL	AC-11 (1)
AC-12	Session Termination	OPTIONAL	AC-12
AC-14	Permitted Actions without Identification or Authentication	AC-14	AC-14
AC-16	Security and Privacy Attributes	OPTIONAL	OPTIONAL
AC-17	Remote Access	AC-17	AC-17 (1) (2) (3) (4)
AC-18	Wireless Access	AC-18	AC-18 (1) (3)
AC-19	Access Control for Mobile Devices	AC-19	AC-19 (5)
AC-20	Use of External Systems	AC-20	AC-20 (1) (2)
AC-21	Information Sharing	OPTIONAL	AC-21
AC-22	Publicly Accessible Content	AC-22	AC-22
AC-23	Data Mining Protection	OPTIONAL	OPTIONAL
AC-24	Access Control Decisions	OPTIONAL	OPTIONAL
AC-25	Reference Monitor	OPTIONAL	OPTIONAL
AWARENESS AND TRAINING			
AT-1	Awareness and Training Policy and Procedures	AT-1	AT-1
AT-2	Literacy Training and Awareness	AT-2 (2)	AT-2 (2) (3)
AT-3	Role-Based Training	AT-3	AT-3
AT-4	Training Records	AT-4	AT-4
AT-6	Training Feedback	OPTIONAL	OPTIONAL
AUDIT AND ACCOUNTABILITY			
AU-1	Audit and Accountability Policy and Procedures	AU-1	AU-1
AU-2	Event Logging	AU-2	AU-2
AU-3	Content of Audit Records	AU-3	AU-3 (1)
AU-4	Audit Log Storage Capacity	AU-4	AU-4
AU-5	Response to Audit Logging Process Failures	AU-5	AU-5
AU-6	Audit Record Review, Analysis, and Reporting	AU-6	AU-6 (1) (3)
AU-7	Audit Record Reduction and Report Generation	OPTIONAL	AU-7 (1)
AU-8	Time Stamps	AU-8	AU-8
AU-9	Protection of Audit Information	AU-9	AU-9 (4)
AU-10	Non-repudiation	OPTIONAL	OPTIONAL
AU-11	Audit Record Retention	AU-11	AU-11
AU-12	Audit Record Generation	AU-12	AU-12

CONTROL NO.	CONTROL NAME	INITIAL CONTROL BASELINES OPTIONAL	
		LOW (IAL1)	MODERATE (IAL2)
AUDIT AND ACCOUNTABILITY (CONT)			
AU-13	Monitoring for Information Disclosure	OPTIONAL	OPTIONAL
AU-14	Session Audit	OPTIONAL	OPTIONAL
AU-16	Cross-Organizational Audit Logging	OPTIONAL	OPTIONAL
ASSESSMENT, AUTHORIZATION, AND MONITORING			
CA-1	Assessment, Authorization, and Monitoring Policies and Procedures	CA-1	CA-1
CA-2	Control Assessments	CA-2	CA-2 (1)
CA-3	Information Exchange	CA-3	CA-3
CA-5	Plan of Action and Milestones	CA-5	CA-5
CA-6	Authorization	CA-6	CA-6
CA-7	Continuous Monitoring	CA-7(4)	CA-7 (1)
CA-8	Penetration Testing	OPTIONAL	OPTIONAL
CA-9	Internal System Connections	CA-9	CA-9
CONFIGURATION MANAGEMENT			
CM-1	Configuration Management Policy and Procedures	CM-1	CM-1
CM-2	Baseline Configuration	CM-2	CM-2 (2) (3) (7)
CM-3	Configuration Change Control	OPTIONAL	CM-3 (2) (4)
CM-4	Impact Analysis	CM-4	CM-4 (2)
CM-5	Access Restrictions for Change	CM-5	CM-5
CM-6	Configuration Settings	CM-6	CM-6
CM-7	Least Functionality	CM-7	CM-7 (1) (2) (5)
CM-8	System Component Inventory	CM-8	CM-8 (1) (3)
CM-9	Configuration Management Plan	OPTIONAL	CM-9
CM-10	Software Usage Restrictions	CM-10	CM-10
CM-11	User-Installed Software	CM-11	CM-11
CM-12	Information Location	OPTIONAL	CM-12 (1)
CM-13	Data Action Mapping	OPTIONAL	OPTIONAL
CM-14	Signed Components	OPTIONAL	OPTIONAL
CONTINGENCY PLANNING			
CP-1	Contingency Planning Policy and Procedures	CP-1	CP-1
CP-2	Contingency Plan	CP-2	CP-2 (1) (3) (8)
CP-3	Contingency Training	CP-3	CP-3
CP-4	Contingency Plan Testing	CP-4	CP-4 (1)
CP-6	Alternate Storage Site	OPTIONAL	CP-6 (1) (3)
CP-7	Alternate Processing Site	OPTIONAL	CP-7 (1) (2) (3)
CP-8	Telecommunications Services	OPTIONAL	CP-8 (1) (2)
CP-9	System Backup	CP-9	CP-9 (1) (8)
CP-10	System Recovery and Reconstitution	CP-10	CP-10 (2)
CP-11	Alternate Communications Protocols	OPTIONAL	OPTIONAL
CP-12	Safe Mode	OPTIONAL	OPTIONAL
CP-13	Alternative Security Mechanisms	OPTIONAL	OPTIONAL

Appendix B – Security Categorization Decision Flow