Division of Enterprise Technology Strategy and Services

ETSS Policy 300.2

Risk Assessment Policy (RA)

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

doa.entsec@doit.ri.gov

1. Purpose

This policy establishes the requirements for effectively managing risk to State of Rhode Island information systems and data through security categorization, risk assessment, vulnerability monitoring and scanning, risk response, and criticality analysis. This policy ensures that inherent risks, vulnerabilities, threats, and countermeasures are assessed based on the criticality of information systems and data to achieve an acceptable level of enterprise risk. This policy supports the State's compliance with NIST SP 800-53 Revision 5 (Risk Assessment family), NIST SP 800-30 (Guide for Conducting Risk Assessments), NIST SP 800-37 (Risk Management Framework), NIST Cybersecurity Framework 2.0, IRS Publication 1075, and other applicable federal and state regulatory requirements.

2. Applicability

This policy applies to all State of Rhode Island Executive Branch departments, including agencies, boards, and commissions, as well as their employees (permanent, non-permanent, full-time, and part-time), interns, consultants, contractors, contractors, vendors, and any entity that has access to State information systems and data.

3. Definitions

The following terms are defined for the purposes of this policy. All other terms should be referenced in the ETSS Glossary of Terms, Acronyms, and Definitions.

Risk Assessment
A determination of risk, including likelihood and impact estimates, from potential threats and vulnerabilities that could result in a compromise of the confidentiality, integrity, or availability of information systems and data.

Security Categorization
A level of risk assigned to information systems and data based on risk assessments and the potential impact to individuals, system operations, and State assets should confidentiality, integrity, or availability be compromised.

Vulnerability

A weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

4. Procedures for Compliance

The following requirements establish the risk assessment controls that agencies and ETSS must implement.

4.1 Risk Assessment Policy and Procedures (RA-1)

Applies to: All systems (IAL1, IAL2)
Each agency shall develop, document, and disseminate a risk assessment policy and supporting procedures. The ETSS CISO is designated as the official responsible for the enterprise policy. The policy shall be reviewed at least every three (3) years and following significant changes. Supporting procedures shall be reviewed annually.

4.2 Security Categorization (RA-2)

Applies to: All systems (IAL1, IAL2)
Each agency shall:

a. Categorize the information system and data it processes, stores, and transmits in accordance with the ETSS Data Classification Policy (400.1) and ETSS PM-1.

b. Document security categorization results, including supporting rationale, within the applicable System Security Plan.

c. Ensure the security categorization decision is reviewed and approved by the agency authorizing official or designated representative.

4.3 Risk Assessment (RA-3)

Applies to: All systems (IAL1, IAL2)
Each agency shall:

a. Perform a risk assessment in accordance with PM-1, including identifying threats and vulnerabilities, assessing likelihood and magnitude of harm from unauthorized access or disclosure, and assessing the impact of adverse effects on individuals from processing PII.

b. Integrate risk assessment results from agency mission perspectives with system-level risk assessments.

c. Document risk assessment results within a report included as an artifact in the System Security Plan.

d. Disseminate results to designated agency personnel including the AIM, TSM, and ETSS Enterprise Security Team.

e. Review risk assessment results annually.

f. Update the risk assessment every three (3) years or upon significant changes, including new threats, increased monitoring findings, new business requirements, changes to the authorizing official, significant changes to inherited controls, or supply chain changes.

4.3.1 Supply Chain Risk Assessment (RA-3(1))

Applies to: All systems (IAL1, IAL2)
Each agency shall:

a. Assess supply chain risks associated with systems, components, and services provided by external parties. Assessments shall be conducted within the enterprise GRC platform (Archer) by the ETSS CISO or authorized delegate, evaluating inherent and residual risk, data sensitivity, dependency and criticality, and alignment with enterprise security requirements.

b. Update supply chain risk assessments at least annually and when significant changes occur to vendors, services, supply chains, systems, or regulatory requirements. Updates shall be coordinated between the ETSS VMO and CISO.

4.4 Vulnerability Monitoring and Scanning (RA-5)

Applies to: All systems (IAL1, IAL2)

Each agency shall:

a. Monitor and scan for vulnerabilities at least monthly and when new vulnerabilities are identified. Critical and high vulnerabilities shall be included in continuous monitoring per the ETSS CA Policy.

b. Employ enterprise vulnerability scanning tools (Qualys VMDR) that facilitate interoperability, automate vulnerability management, and measure impact. Findings shall be tracked through ServiceNow.

c. Analyze vulnerability scan reports and security control assessment results.

d. Remediate detected vulnerabilities per CVSS scoring: Critical (9-10) within 15 days, High (7-8.9) within 30 days, Moderate (4-6.9) within 90 days, Low (below 4) within 180 days. Corrective action plans are required within one week for critical, two weeks for high, one month for moderate, and three months for low. A POAM is required where timelines cannot be met.

e. Share vulnerability scan results with appropriate personnel to help mitigate similar vulnerabilities across systems.

f. Employ tools that readily update the vulnerabilities to be scanned.

4.4.1 Update Vulnerabilities to Be Scanned (RA-5(2))

Applies to: All systems (IAL1, IAL2)

Each agency shall update vulnerabilities to be scanned no less than monthly, prior to each new scan, and when new vulnerabilities are identified.

4.4.2 Breadth and Depth of Coverage (RA-5(3))

Applies to: Moderate and above (IAL2)

Each agency shall define the breadth and depth of vulnerability scanning coverage to ensure all system components within the authorization boundary are scanned, including network devices, servers, endpoints, databases, web applications, and cloud resources. Coverage shall be documented in the SSP and validated through continuous monitoring.

4.4.3 Privileged Access (RA-5(5))

Applies to: Moderate and above (IAL2)

Each agency shall require privileged access authorization for intrusive vulnerability scanning or scanning of systems containing classified data.

4.4.4 Public Disclosure Program (RA-5(11))

Applies to: All systems (IAL1, IAL2)

Each agency shall establish a public reporting channel for receiving vulnerability reports.

4.5 Risk Response (RA-7)

Applies to: All systems (IAL1, IAL2)

Each agency shall:

a. Respond to assessments, monitoring, and audits in accordance with enterprise risk tolerance. Response actions include mitigation, acceptance (with formal approval), avoidance, and transfer.

b. Include within the POAM each risk that cannot be mitigated by the expected completion date.

c. Include justification and compensating controls for each accepted risk. Inherited control risks can only be accepted by the control owner.

4.6 Criticality Analysis (RA-9)

Applies to: Moderate and above (IAL2)

Each agency shall perform a criticality analysis for all assets to identify critical systems, components, functions, and services at design, implementation, and major changes, with ETSS CISO and CTO oversight.

5. Repercussions for Non-Compliance

Failure to comply with this policy may result in corrective action proportional to the severity of the violation. Consequences may include:

a. Denial of system authorization for systems without a current risk assessment or security categorization.

b. Mandatory remediation of critical and high vulnerabilities within defined timelines.

c. System isolation or restricted network access for systems with unresolved critical vulnerabilities.

d. Escalation to ETSS leadership for systemic non-compliance with remediation timelines.

Non-compliance findings shall be documented and tracked through ETSS governance processes and recorded in the agency POAM.

6. Roles and Responsibilities

The following roles are accountable for the implementation, monitoring, and enforcement of this policy:

Chief Information Security Officer (CISO)

Designated as the official responsible for the enterprise Risk Assessment policy. Conducts or delegates supply chain risk assessments within the GRC platform (Archer). Provides enterprise oversight of vulnerability remediation timelines, risk response decisions, and criticality analysis.

ETSS Chief of the Vendor Management Office (VMO)

Coordinates supply chain risk assessments with the CISO and ensures updates are reflected in the GRC platform and vendor agreements.

ETSS Security Operations

Executes enterprise vulnerability scanning using Qualys VMDR, tracks findings through ServiceNow, analyzes scan results, and provides vulnerability data to support risk assessments and continuous monitoring.

System Owners

Responsible for completing risk assessments and security categorizations, implementing vulnerability remediation within timelines, coordinating supply chain risk assessments for system-specific acquisitions, and performing criticality analysis.

Agency Information Managers (AIMs) / Technical Support Managers (TSMs)

Receive risk assessment results, coordinate vulnerability remediation at the agency level, and support annual reviews of risk assessments.

Authorizing Officials

Review and approve security categorization decisions, accept residual risk through formal processes, and approve POAMs for risks not fully remediated.

7. Approval / Review Signatures

Digitally signed by Nathan Loura
Date: 2026.07.15 10:46:26 -04'00'

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

Brian Tardiff

Digitally signed by Brian Tardiff
Date: 2026.07.15 11:27:56 -04'00'

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