State of Maryland

STANDARD

RISK ASSESSMENT

Document No.	Last Updated	Prepared By
MD-STD-316-RA-01	02/18/2026	DoIT OSM

Risk assessments are crucial for identifying, analyzing, and mitigating potential threats before they cause harm. In a Zero Trust Architecture (ZTA) framework, risk assessments play a vital role in continuously evaluating access requests, monitoring user behavior, and enforcing least privilege principles.

PURPOSE AND SCOPE

Purpose	This standard provides the technical and operational specifications needed for security threats and vulnerabilities to be systematically evaluated and addressed.
Scope	This standard covers system categorization, assessment of vulnerabilities, threat identification, and risk monitoring.
Applicability	This standard applies to all units of State government (as defined in SF&P 3.5-101(g)), hereafter referred to simply as "agencies."
Related Policy	This standard is part of a broader policy suite. Refer to MD-POL-100 Cybersecurity & Governance Policy, Appendix C for a list of related policies and standards.
Baseline	This standard has been developed using National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 5 Moderate Baseline[1] and State-specific organizationally defined parameters. Agencies may be required to deviate from this baseline when State statute, executive orders, or applicable regulations establish a conflicting requirement that precludes compliance.
Distribution	This document is approved for public distribution and may be shared with external stakeholders, partners, and regulatory bodies. It reflects the State's commitment to transparency, compliance, and operational excellence. Unauthorized modifications or misrepresentation of this document are strictly prohibited.

[1] NIST SP 800-53 Rev. 5: Security and Privacy Controls for Information Systems and Organizations.

FOREWORD

Agencies that use Department of Information Technology DoIT-managed services automatically receive, or *inherit*, the compliance those services already meet, reducing duplicative work and accelerating their overall compliance efforts. These centrally governed services, such as hosting platforms, identity management, and network infrastructure, are built with robust control frameworks that automatically extend to participating agencies. By leveraging these offerings, agencies not only align with key operational and security standards but also benefit from pre-configured environments, continuous monitoring, and policy enforcement mechanisms maintained by DoIT. Agencies are encouraged to leverage these services to accelerate readiness, gain cost efficiency, simplify compliance efforts, and allow agencies to focus more fully on mission delivery, knowing that foundational requirements are already in place. Agencies should review the scope of each managed service to understand which standards are inherited and where additional agency-specific controls may still be required.

GUIDANCE AND ENFORCEABILITY

Throughout this document, informational call-out boxes are utilized to provide additional context or elaborate on key topics. While these boxes primarily serve an informational purpose, any directives or mandated actions contained within them are authoritative and carry the same enforceability as the core requirements of this document. For the purposes of this document, the term “shall” denotes a mandatory requirement. Terms such as “where feasible”, “encouraged”, or similar phrasing indicate recommended practices that reflect organizational preference but are not enforceable requirements at this time.

CHANGE RECORD

Version	Summary of Changes	Changed By	Date
1.0	Initial Publication	Miheer Khona	02/18/2026

STANDARDS

316 State Strategy

These standards establish a baseline of risk assessment practices that each agency must implement to comply with State cybersecurity and privacy policies. Each agency shall designate specific personnel with IT responsibilities to ensure the effective implementation of these standards.

316-1 Develop Agency-Level Procedures (RA-1)

In alignment with this standard, develop and document agency-level risk assessment procedures. Agencies must disseminate the procedures to agency personnel with information technology (IT) security responsibilities. Agencies must review, and if needed, update the procedures as deemed appropriate by the agency based on changes and risk at least every **3 years**. At a minimum, the procedures must address purpose, scope, roles and responsibilities, and guidelines.

316-2 Categorize Systems (RA-2)

Categorize each system and the information it processes, stores, and transmits. Document the security categorization results, including supporting rationale, in the System Security Plan (SSP). Verify that the Authorizing Official (AO) reviews and approves the security categorization. As part of categorization, ensure a privacy threshold analysis (PTA) is performed as required by the State Chief Privacy Officer (SCPO).

High Water Mark

Federal Information Processing Standard Publication 199 (FIPS 199) provides a standardized approach for categorizing systems based on the potential consequences of a security breach. The process begins by identifying the types of information processed, stored, or transmitted by the system. For each information type, assess the potential impact of a loss of confidentiality, integrity, and availability using the categories Low, Moderate, or High. These assessments shall consider organizational mission, legal obligations, and potential harm to individuals or operations. The final impact level of the system is set using the high-water mark principle, meaning the highest impact rating among the three security objectives becomes the overall system categorization. Supporting resources like NIST SP 800-60 provide mappings between information types and impact levels to guide this process.

Where feasible, implement dynamic categorization of assets based on sensitivity, ensuring Personal Information and other non-public data receive enhanced protection.

316-3 Conduct Risk Assessments (RA-3)

Conduct risk assessments by identifying threats to and vulnerabilities in the system. Determine the likelihood and magnitude of harm from unauthorized access, use, disclosure, disruption, modification, or destruction of the system, the information it processes, stores, or transmits, and any related information. Determine the likelihood and impact of adverse effects on individuals arising from the processing of Personally Identifiable Information (PII). As part of risk assessments, ensure privacy impact assessments (PIA) are conducted as required by the SCPO.

Document risk assessment results in a Risk Assessment Report (RAR) and SSP. Weaknesses not readily corrected must be tracked in a system-level Plan of Action & Milestones (POA&M).

Disseminate risk assessment results to authorized system administrators, system owners, AOs and the State Chief Information Security Officer (SCISO). Update the risk assessment at least annually or when there are significant changes to the system, its environment of operation, or other conditions that may impact the security or privacy state of the system.

Zero Trust Architecture

Integrating real-time threat intelligence, behavior analytics, and automated analysis with dynamic rules into risk assessments transforms static evaluations into adaptive, context-aware processes. These capabilities allow organizations to continuously monitor user behavior and environmental signals, flag anomalies and adjust access decisions based on evolving threat landscapes. By embedding dynamic rule sets, systems can respond to suspicious activity with automated containment or escalation protocols. This fusion of intelligence and automation enhances both the precision and agility of risk assessments, aligning them with ZTA principles and modern compliance frameworks.

RA-3(1): Assess supply chain risks and update the supply chain risk assessment at least **annually**, or when there are significant changes to the relevant supply chain, or when changes to the system, environments of operation, or other conditions may necessitate a change in the supply chain.

316-4 Conduct Vulnerability Monitoring and Scanning (RA-5)

Monitor and scan for vulnerabilities in the system and hosted applications **continuously** and when new vulnerabilities potentially affecting the system are identified and reported. Additional penetration testing may be required for High Value State Systems (HVSS) as directed by the SCISO.

Employ vulnerability monitoring tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:

- Enumerating platforms, software flaws, and improper configurations;
- Formatting checklists and test procedures; and
- Measuring vulnerability impact.

Analyze vulnerability scan reports and results from vulnerability monitoring and remediate vulnerabilities within the remediation timelines defined in the MD-STD-319-SI, System & Information Integrity Standard, Section 319-2. The remediation timeline may be modified as deemed appropriate by the SCISO based on the impact level of the system, vulnerability severity, absence of compensating controls, and likelihood of exploit. POA&Ms must be created to track confirmed vulnerabilities identified through system scans. For any vulnerabilities that cannot be remediated within the applicable timeframes described above, expected remediation date and detailed remediation actions shall be clearly documented in the assigned POA&M.

Share information obtained from the vulnerability monitoring process and control assessments with authorized system administrators, system owners, AOs and the SCISO to help eliminate similar vulnerabilities in other systems. Employ vulnerability monitoring tools that include the capability to readily update the vulnerabilities to be scanned.

RA-5(2): Update the system vulnerabilities to be scanned prior to a new scan.

RA-5(5): Implement privileged access authorization to servers and network devices for scanning activities (as needed).

RA-5(11): Work with the SCISO to establish a public reporting channel for receiving reports of vulnerabilities in agency systems and system components, consistent with the State's Vulnerability Disclosure Program (VDP).

316-5 Implement Risk Response Actions (RA-7)

Respond to findings from security and privacy assessments, monitoring, and audits in accordance with organizational risk tolerance. To the extent possible, use automated risk mitigation strategies such as blocking unauthorized access or isolating compromised assets.

316-6 Perform Criticality Analysis (RA-9)

Identify critical system components and functions by performing a criticality analysis of agency systems, and services at the design stage. Refer to NIST IR 8179 for guidelines on how to perform the criticality analysis.

GUIDELINES

ID	Title	Description	Source
CSF Tools	Cyber Security Framework Tools	This website provides supplemental guidance for each security control listed in this document.	*csf.tools (LINK)*
NIST SP 800-30	Guide for Conducting Risk Assessments	This document provides a structured approach to performing a risk assessment.	*csf.tools (LINK)*
NIST SP 800-60 Vol. I & II	Guide for Mapping Types of Information and Information Systems to Security Categories	This document provides guidance on mapping types of information and information systems to security categories.	*csf.tools (LINK)*
FIPS 199	Standards for Security Categorization of Federal Information and Information Systems	Defines the security categories, security objectives, and impact levels for information systems.	*csf.tools (LINK)*
NIST SP 800-37	Risk Management Framework for Information Systems and Organizations	This document outlines the RMF process, which integrates risk assessments into a broader 6-step process.	*csf.tools (LINK)*
NIST SP 800-39	Managing Information Security Risk: Organization, Mission, and Information System View	This document provides insight into how all aspects of risk management fit into the broader organization-wide program.	*csf.tools (LINK)*
NIST IR 8179	Criticality Analysis Process Model: Prioritizing Systems and Components	This document provides a method for identifying and prioritizing systems, components, and services based on their importance to an organization's mission and the potential impact of their failure or compromise.	*csf.tools (LINK)*

DEFINITIONS

Each unique term used in this standard is defined in the **State of Maryland Cybersecurity & Privacy Glossary**.

COMPLIANCE CHECKLIST

ID	Standard	Compliance
316-1	**Develop Agency-Level Procedures (RA-1)**	☐ Yes ☐ No
316-2	**Categorize Systems (RA-2)**	☐ Yes ☐ No
316-3	**Conduct Risk Assessments (RA-3)**	☐ Yes ☐ No
316-4	**Conduct Vulnerability Monitoring and Scanning (RA-5)**	☐ Yes ☐ No
316-5	**Implement Risk Response Actions (RA-7)**	☐ Yes ☐ No
316-6	**Perform Criticality Analysis (RA-9)**	☐ Yes ☐ No

Note: When assessing the implementation and effectiveness of the security and privacy controls outlined in this standard, DoIT recommends the use of NIST SP 800-53A Rev. 5, to perform evaluations in a manner that is evidence-based, repeatable, and aligned with the system's documented security posture.