230 – Risk Assessment Standard

Purpose

The purpose of the Risk Assessment standard is to set forth requirements and expectations related to, and supporting Information Technology (IT) and Information Systems (IS) risk assessments, criticality analysis, security categorization of data, risk response (e.g., POAM remediation), vulnerability monitoring and scanning, etc. to identify the risk posture as part of the risk management framework process for the State of Wisconsin computing environments including its information systems and data. Various risk assessment types and strategies are used to address risk assessment, risk management, and risk mitigation/acceptance for State information and IT systems.

Standard

Based on NIST SP 800-53 Rev. 5, DET's Standards address a diverse set of security and privacy requirements. As a currently established baseline for implementation, DOA utilizes all low level, and selected moderate level controls in support of its security posture initiatives. Agencies shall categorize their data and identify the potential impact (high, moderate, or low), and select controls appropriately as defined by Table 3-1 in NIST SP 800-53B for the allocated impact levels (high, moderate, low) of controls and control enhancements. Agencies shall update DET on the status of their baseline control implementation through the reporting and monitoring process.

Executive Branch Agencies shall develop policies, procedures, or processes for their own State information systems and system environments to protect State information, if applicable. **Note:** Some agencies will specific regulatory requirements to follow that go above and beyond the requirements for other agencies. Implementation of the standard controls within this document can be (1) a common (inheritable) control, (2) a system-specific control, or (3) a hybrid control. The control implementation defines the scope of applicability for the control, the shared nature or inheritability of the control, and the responsibility for control development, implementation, assessment, and authorization.

This standard contains the minimum baseline controls that Executive Branch agencies shall implement; however, those agencies may also be required to implement controls outside of the scope of the controls listed in this document.

BASELINE CONTROLS

Policy and Procedures (RA-1):

- Develop, document, and disseminate to appropriate agency personnel or roles:
  - A risk assessment policy that:
    - Addresses purpose, scope, roles, responsibilities, management commitment, coordination among agency entities, and compliance.

    - Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.
  - Procedures to facilitate the implementation of the risk assessment policy and the associated risk assessment controls.
- Designate appropriate agency personnel to manage the development, documentation, and dissemination of the risk assessment policy and procedures.
- Review and update the current risk assessment:
  - Policy on an agency-defined frequency.
  - Procedures on an agency-defined frequency.

Security Categorization (RA-2):

- Categorize the systems and information it processes, stores, and transmits.
- Document the security categorization results, including supporting rationale, in the security plan for system.
- Verify that the authorizing official or authorizing official designated representative reviews and approves the security categorization decision.

Note: Categorization is not the same as Classification. Categorization identifies the type of data (e.g., FTI, PHI, Federal PII, HIPAA) where Classification is the higher tier of several categories. Using the example, the classification based on Federal guidance would be Sensitive But Unclassified (SBU) or Controlled Unclassified Information (CUI) under NIST SP 800-171 Rev. 2. Low, Moderate, and High controls are based on potential impact and selected to reduce the potential impact unless it is determined the likelihood of the potential impact is minimized. Federal security categories can be found in NIST SP 800-60 Vol. 1 and 2, on the Federal Register, or on some Federal agency websites.

Risk Assessment (RA-3):

- Conduct a risk assessment, including:
  - Identifying threats to and vulnerabilities in the system.
  - Determining the likelihood and magnitude of harm from unauthorized access, use, disclosure, disruption, modification, or destruction of the system, the information the system processes, stores, or transmits, and any related information.
  - Determining the likelihood and impact of adverse effects on individuals arising from the processing of personal identifiable information (PII).
- Integrate risk assessment results and risk management decisions from the agency and mission or business process perspectives with system-level risk assessments.
- Document risk assessment results in security and privacy plans and risk assessment plans.
- Review risk assessment results on an agency-defined frequency.
- Disseminate risk assessment results to agency-defined personnel or roles.

- Update the risk assessment on an agency-defined frequency 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.

Risk Assessment | Supply Chain Risk Assessment (RA-3(1)):

- Assess supply chain risks associated with agency-defined systems, system components, and system services.
- Update the supply chain risks assessment on an agency-defined frequency, when there are significant changes to the relevant supply chain, or when changes to the system, environments of operations, or other conditions may necessitate a change in the supply chain.

Vulnerability Monitoring and Scanning (RA-5):

- Monitor and scan for vulnerabilities in the system and hosted applications on an agency-defined frequency and when new vulnerabilities potentially affecting the system are identified and reported.
- 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
  - Measuring vulnerability impact
- Analyze vulnerability scan reports and results from vulnerability monitoring.
- Remediate legitimate vulnerabilities in accordance with an agency assessment of risk.
- Share information obtained from the vulnerability monitoring process and control assessments with agency-defined personnel or roles to help eliminate similar vulnerabilities in other systems.
- Employ vulnerability monitoring tools that include the capability to readily update the vulnerabilities to be scanned.

Vulnerability Monitoring and Scanning | Update Vulnerabilities to Be Scanned (RA-5(2)):

- Update the system vulnerabilities to be scanned on an agency-defined frequency, prior to a new scan, and when new vulnerabilities are identified and reported.

Vulnerability Monitoring and Scanning | Privileged Access (RA-5(5)):

- Implement appropriate privileged access authorization to system components for vulnerability scanning activities.

Vulnerability Monitoring and Scanning | Public Disclosure Program (RA-5(11)):

- Establish a public reporting channel for receiving reports of vulnerabilities in agency systems and system components.

Risk Response (RA-7):

- Respond to findings from security and privacy assessments, monitoring, and audits in accordance with agency risk tolerances.

Privacy Impact Assessments (RA-8):

- Conduct privacy impact assessments for systems, programs, or other activities before:
  - Developing or procuring information technology that processes personally identifiable information.
  - Initiating a new collection of personally identifiable information that:
    - Will be processed using information technology.

Criticality Analysis (RA-9):

- Identify critical system components and functions by performing a criticality analysis for agency-defined systems, system components, and system services. For example, critical systems and components can be documented in contingency plans, system security plans, asset databases (e.g., CMDB), or architecture diagrams.

Definitions

Executive Branch Agency - State of Wisconsin legislatively defined Departments and all customers of DET services, equipment, and/or technologies. Agency or State Agency may be used interchangeably with Executive Branch Agency.

State information - Any information that is created, accessed, used, stored, or transmitted by an Executive Branch Agency.

State information systems and system environments - All equipment or services used to input, store, process, transmit, and output information, including, but not limited to network devices, servers, databases, printers, Internet, email, physical, virtual, cloud, and applications accessible to and/or managed the agency.

System Development Life Cycle, SDLC– The five phases of the system development life cycle (SDLC) process, is the overall process of developing, implementing, and retiring information systems from initiation, analysis, design, implementation, and maintenance to disposal (source: https://www.nist.gov/publications/system-development-life-cycle-sdlc)

Exception Process

Exceptions to any Executive Branch Agency's Security Policies or Standards shall follow the Executive Branch Risk Exception Procedure.

Document History/Owner

This standard was developed as required by the State of Wisconsin Information Technology Security Policy

Handbook, under the authority of Wis. Stat. § 16.971.

This standard is effective upon approval and publication until retired. Revisions and updates continue the effective date by documenting required changes over time.

Ownership for this standard is assigned to DOA, DET Bureau of Security. As such, the DOA, DET Bureau of Security is responsible for the maintenance, update(s), and review of this document annually before the anniversary of the effective date.

Version #	Revision or Review Date	Description of Change(s)	Reviewer/Author	Date Approved
2.0	11/03/20	Reviewed with Agency Security Officers and IT Directors and changes were incorporated	Reviewer: WI ISAC/ITDC Author: DOA/DET/BOS	11/11/20
3.0	06/24/22	Reviewed with Agency Security Officers and IT Directors and changes were incorporated	Reviewer: WI ISAC/ITDC Author: DOA/DET/BOS	06/24/22
4.0	07/14/23	Reviewed with Agency Security Officers and IT Directors and changes were incorporated	Reviewer: WI ISAC and Enterprise IT Author: DOA/DET/BOS	08/01/23
5.0	7/2/24	Reviewed with Agency Security Officers and IT Directors and changes were incorporated	Reviewer: WI ISAC and Enterprise IT Author: DOA/DET/BOS	7/30/24
NOTE: Keep only the origination and the last 10 years of update information. Only notate prior three revisions. Include only interim/final revision statuses.				

Authorized and approved by:

Troy Stairwalt, State of Wisconsin Chief Information Security Officer

DocuSigned by:
Troy Stairwalt
1DEEB606FC2524A8...

7/31/2024 | 4:05 PM CDT

Print/Type Title | Signature | Date