230 – Risk Assessment Standard

Purpose

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

This standard uses the NIST SP 800-53 Rev. 5 framework as the guideline to establish control objectives to address a diverse set of security and privacy requirements. Not all controls within NIST SP 800-53 Rev. 5 may be selected for the Statewide baseline policies and standards. Agencies must categorize their data and identify the potential impact (high, moderate, or low), and select controls appropriately. This standard uses Table 3-1 in NIST SP 800-53B for the allocated impact levels (high, moderate, low) of controls and control enhancements. At a minimum, all low controls are selected, and certain moderate controls are selected. Agencies are to reflect their controls through the annual reporting process to DOA-DET.

Executive Branch Agencies are to develop policies, procedures, or processes for their own State information systems and system environments to protect State information, if applicable. 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. Agencies should consider the following for inclusion in their policies, procedures, or processes:

Security Categorization (RA-2):

- Agencies categorize the systems and information it processes, stores, and transmits.
- Agencies document the security categorization results. If appropriate, include any rationale in an overall security plan for potential moderate impact systems.
- Agencies designated authorizing personnel or representatives to review and approve 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):

- Risk assessments can be conducted at multiple levels: State-wide, Agency, mission/business process, or information system level, at any stage of the system development life cycle (SDLC), or during any steps in risk management framework. Agency requirements for conducting a risk assessment for potentially moderate or high impact areas should include:
    - Identifying threats to and vulnerabilities in their own systems.
    - 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.
    - Determine 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, mission, or business process perspectives with system-level risk assessments.
- Document risk results.
- Disseminate risk assessment results to Agency-defined personnel or roles.
- Review and update the risk assessment 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.

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

- Agencies shall follow the procurement rules at their agency.

Vulnerability Monitoring and Scanning (RA-5):

- Monitoring and scanning for vulnerabilities in the system and hosted applications monthly or when there are significant vulnerabilities that can affect the systems or applications. Perform configuration scans quarterly, when there are significant changes in the configuration, or when there are significant vulnerable configurations.
- Employing 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.
- Analyzing vulnerability scan reports and results from vulnerability monitoring.
- 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.

- Develop a timeline to resolve vulnerabilities based on severity, likelihood and criticality of systems as well as documented exception process.

Update System Vulnerabilities (RA-5(2)):

- Update the system vulnerabilities to be scanned monthly, prior to a new scan, and when new vulnerabilities are identified and reported.

Privileged Access (RA-5(5)):

- Implement appropriate privileged access authorization to systems for vulnerability scanning.

Risk Response (RA-7):

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

Criticality Analysis (RA-9):

- Identifying and documenting critical 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.

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. Retrieved: 2017/09/01.)

Exception Process

Exceptions to any Executive Branch Agencies Security Policies, Procedures or Standards must follow the Executive Branch Agencies 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 Wisconsin State Statute 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
1.0	10/15/18	Submitted to and approved by the IT Executive Steering Committee	Reviewer: ITESC Author: DOA/DET	10/15/18
1.0	10/29/19	Reviewed with Agency Security Officers and feedback collected. Planning for making revisions.	Bureau of Security	10/29/19
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
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:

Alan Greenberg, CISO — DocuSigned by: Alan Greenberg 7062227F849B429... — 7/8/2022 | 1:55 PM CDT

Print/Type Title — Signature — Date