130 – Security Assessment and Authorization Standard

Purpose

The Security Assessment and Authorization Standard provides the minimum requirements for conducting security assessments and documentation of authorization(s) for security measures on the State Information Technology (IT) systems and system environments.

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 3-4 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 quarterly 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. Some agencies will have specific regulatory requirements that they must adhere to that go beyond what other agencies would need to adhere to. 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 is divided into two sections of controls. **Section One** includes the minimum baseline controls that Executive Branch agencies are to adhere to. **Section Two** includes additional controls for agencies that are subject to regulatory requirements. The list in Section Two is not all-inclusive. Agencies may have additional controls they must adhere to that are not listed here.

SECTION ONE: BASELINE CONTROLS

Policy and Procedures (CA-1):

- Develop, document, and disseminate to appropriate agency personnel or roles:
  - An assessment, authorization, and monitoring policy that:
    - Addresses purpose, scope, roles, responsibilities, management commitment, coordination among agency entities, and compliance; and
    - Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
  - Procedures to facilitate the implementation of the assessment, authorization, and monitoring policy and the associated assessment, authorization, and monitoring

controls;

- Designate appropriate agency personnel to manage the development, documentation, and dissemination of the assessment, authorization, and monitoring policy and procedures; and
- Review and update the current assessment, authorization, and monitoring:
  - Policy on an agency-defined frequency; and
  - Procedures on an agency-defined frequency.

Control Assessments (CA-2):

- Select the appropriate assessor or assessment team for the type of assessment to be conducted;
- Develop a control assessment plan that describes the scope of the assessment including:
  - Controls and control enhancements under assessment;
  - Assessment procedures to be used to determine control effectiveness; and
  - Assessment environment, assessment team, and assessment roles and responsibilities;
- Ensure the control assessment plan is reviewed and approved by the authorizing official or designated representative prior to conducting the assessment;
- Assess the controls in the system and its environment of operation on an agency-defined frequency to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security and privacy requirements;
- Produce a control assessment report that documents the results of the assessment; and
- Provide the results of the control assessment to the appropriate agency personnel or roles.

Control Assessments | Independent Assessors (CA-2(1)):

- Employ independent assessors or assessment teams to conduct control assessments.

Information Exchange (CA-3):

- Approve and manage the exchange of information between the system and other systems using (one or more): interconnection security agreements, information exchange security agreements, memoranda of understanding or agreement, service level agreements, user agreements, nondisclosure agreements;
- Document, as part of each exchange agreement, the interface characteristics, security and privacy requirements, controls, and responsibilities for each system, and the impact level of information communicated; and
- Review and update the agreements on an agency-defined frequency.

Plan of Action and Milestones (CA-5):

- Develop a plan of action and milestones for the system to document the planned remediation actions of the agency to correct weaknesses or deficiencies noted during the assessment of the controls and to reduce or eliminate known vulnerabilities in the system; and
- Update existing plan of actions and milestones on an agency-defined frequency based on the findings from control assessments, independent audits or reviews, and continuous monitoring

activities.

Authorization (CA-6):

- Assign a senior official as the authorizing official for the system;
- Assign a senior official as the authorizing official for common controls available for inheritance by agency systems;
- Ensure that the authorizing official for the system, before commencing operations:
  - Accepts the use of common controls inherited by the system; and
  - Authorizes the system to operate;
- Ensure that the authorizing official for common controls authorizes the use of those controls for inheritance by agency systems;
- Update the authorizations on an agency-defined frequency.

Continuous Monitoring (CA-7):

- Develop a system-level continuous monitoring strategy and implement continuous monitoring in accordance with the agency-level continuous monitoring strategy that includes:
  - Establishing the system-level metrics to be monitored;
  - Establishing the ongoing assessment of control effectiveness;
  - Ongoing control assessments in accordance with the continuous monitoring strategy;
  - Ongoing monitoring of system and metrics in accordance with the continuous monitoring strategy;
  - Correlation and analysis of information generated by control assessments and monitoring;
  - Response actions to address results of analysis of control assessment and monitoring information; and
  - Reporting the security and privacy status of the system to the appropriate agency personnel or roles.

Continuous Monitoring | Independent Assessment (CA-7(1)):

- Employ independent assessors or assessment teams to monitor the controls in the system on an ongoing basis.

Continuous Monitoring | Risk Monitoring (CA-7(4)):

- Ensure risk monitoring is an integral part of the continuous monitoring strategy that includes the following:
  - Effectiveness monitoring;
  - Compliance monitoring; and
  - Change monitoring.

Internal System Connections (CA-9):

- Authorize internal connections of components to the system;
- Document, for each internal connection, the interface characteristics, security and privacy requirements, and the nature of the information communicated;

- Terminate internal system connections when no longer needed; and
- Review on an agency-defined frequency the continued need for each internal connection.

SECTION TWO: REGULATORY CONTROLS

Executive Branch agencies must adhere to the baseline controls listed in the previous section of this standard. Executive Branch agencies throughout the State of Wisconsin may be subject to additional Federal, State, and/or Inter-agency regulatory requirements. It is each agency's responsibility to research and implement additional controls needed to meet regulatory compliance requirements and expectations outside of the State of Wisconsin baseline of controls.

Penetration Testing (CA-8):

- Conduct penetration testing on an agency-defined frequency on agency-defined systems or system components.

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 critical information, including, but not limited to network devices, servers, databases, printers, Internet, email, physical, virtual, cloud, and applications accessible to and/or managed by the agency.

Business/IT Owner – Anyone who is authorized for security measures on the State Information Technology (IT) systems and system environments. For example, Chief Information Security Officer (CISO), IT Director, designated Security Professional, etc.

Exception Process

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

Document History

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 the DET Bureau of Security. As such, the 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	10/29/19	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
4.0	07/14/23	Reviewed with Agency Security Officers and IT Directors and changes were incorporated	Reviewer: WI ISAC/Enterprise IT Author: DOA/DET/BOS	07/31/23
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:

Trina Zanow, CIO

DocuSigned by:
Trina Zanow
A11B57ECEC77402...

7/31/2023 | 4:07 PM CDT

Print/Type Signature Date
Title