

Security Assessment and Authorization Policy Background

New, Update or Sunset Review? Sunset Review.

What due diligence was conducted to determine the content of this policy/standard? If this is an update or sunset review, provide information as to what changes were made, if any, as well as reasons behind the policy/standard content.

This policy replaces IT Security Standard 141.10 (1.2.1, 1.5) Changes were made based on workgroup and community feedback to improve clarity for what is required for authorizing a new system and when WaTech must perform a security design review.

Updates to this standard draws from [NIST 800-37 Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy](#)

What is the business case for the policy/standard?

- The system authorization process considers the risks of operating that system and the controls applied to mitigate those risks.
- The Security Design Review ensures document of a system's compliance with State security standard is documented prior to deployment.

What are the key objectives of the policy/standard?

- Identify the compliance gaps and compensating controls to protect state data to make informed business decisions.
- Describe when a security design review is required and agency responsibilities for security design reviews.

How does policy/standard promote or support alignment with strategies?

[Strategic Planning | Washington Technology Solutions](#)

This policy supports efficient and accountable government by ensuring agencies are managing IT roles and responsibilities comprehensively.

What are the implementation considerations?

- Agencies must complete an IT risk assessment of the proposed IT system or application upon receipt of the SDR results.
- Agencies must include the SDR results in its systems/application authorization process.

How will we know if the policy is successful?

Specific: Agencies will provide evidence of SDR completion for all new applications/systems which require an SDR.

Achievable: Agencies will provide evidence of a completed IT risk assessment for all systems/applications new systems/applications authorized by the agency to operate.

Relevant: Standards for security assessment and system authorization are needed now because all agencies are all working toward modernization of existing systems.

Timebound: Agencies are required to assess security and properly authorize systems prior to going live with them.

Equitable: Agencies of all sizes benefit from informed decision-making made possible by security assessments. Requiring authorization ensures business and customer needs are driving technology developments.

SEC-02

State CIO Adopted: Month 1 2023

TSB Approved: Month 1 2023

Sunset Review: Month 1 2023



Replaces:
IT Security Standard 141.10 (1.2.1, 1.5)
Month 1, 2023

Security Assessment and Authorization Policy

See Also:

RCW [43.105.054](#) OCIO Governance

RCW [43.105.205](#) (3) Higher Ed

RCW [43.105.020](#) (22) "State agency"

[Security Policy Compliance Agency Resources SharePoint](#)

1. Agencies must assess the IT security risks and compliance with IT security policies and standards of a proposed information technology system and/or application as part of an agency's security program and portfolio management process.

- a. Agencies must assess the IT security risks of the proposed IT implementation per the [Risk Assessment Standard](#).
- b. Agencies must define responsibilities, including those of the vendor and the agency.

2. Agencies must document the controls mitigating the IT project solutions' security risks within a [Risk Treatment Plan \(RTP\)](#). See the [Risk Management Policy](#). This must include, but is not limited to, the following:

- a. User identification and authentication management method.
- b. System hosting model; e.g., cloud or agency premise.
- c. Security boundary devices, e.g., firewalls, intrusion detection/prevention systems (IDPS).
- d. Vulnerability management e.g., scanning and patching.
- e. Resource constraints.
- f. System development lifecycle (SDLC) deficiencies.

3. A senior-level agency executive or delegate must review and approve the agency's assessment and the RTP.

- a. Agencies must update the agency's system authorization process at least

every three years or when a significant system change likely to substantially affect the security or privacy posture of the system occurs.

4. Agencies must develop and maintain a continuous risk indicator and compliance monitoring program for the proposed IT project. See the [Risk Management Policy](#).

- a. Agencies must review and document the system interconnections associated with the proposed IT project annually. See the [Risk Assessment Standard](#).

5. WaTech [Security Design Reviews \(SDR\)](#)s are required for maintenance and new development of systems and infrastructure projects under certain circumstances.

- a. A WaTech SDR is required when:
 - i. A new agency IT implementation includes at least one of the following conditions:
 - A. Agency-managed Cloud services – SaaS, PaaS, and IaaS.
 - B. Vendor-managed Cloud or dedicated hosting.
 - C. Internet available services hosted on-premises.
 - D. If required by the agency security program or policies.
 - ii. The WaTech SDR team assesses IT implementations under oversight and determines whether a WaTech SDR is required for the proposed technological solution(s). See the [IT Investment Approval and Oversight Policy](#).
 - iii. The agency is planning significant changes for a solution previously reviewed and approved by the SDR team. See the [Change Management Policy \(under development - see 141.10 \(8.1\)\)](#).
 - iv. The SDR team may provide best practices for but does not require security design reviews of public internet platforms like YouTube or social media platforms like Facebook and Twitter that are:
 - A. Used to communicate with the public, **and**;
 - B. State data stored on the platforms is limited to category 1.
- b. Agencies must minimally provide the following when a WaTech SDR is required:

- i. The SDR checklists for the system.
 - ii. A system architecture diagram showing security controls and information flows.
 - iii. The risk assessment associated with the system which may be completed simultaneously with an SDR.
 - iv. The planned risk-mitigation controls and how they will be implemented.
 - v. Other supporting documentation and information deemed relevant by the security design review team.
- c. Agencies must agree to operate the system in compliance with state standards according to the SDR as part of the system authorization process.

REFERENCES

1. [Risk Assessment Standard](#)
2. [Risk Management Policy](#)
3. [IT Investments Approval and Oversight Policy](#)
4. [Change Management Policy \(under development - see 141.10 \(8.1\).](#)
5. [Definition of Terms Used in WaTech Policies and Reports.](#)
6. [NIST 800-37 Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy](#)
7. NIST Cybersecurity Framework Mapping
 - Identify. Asset Management-1: Physical devices and systems within the organization are inventoried.
 - Identify. Asset Management-3: Organizational communication and data flows are mapped.
 - Identify.Governance-1: Organizational cybersecurity policy is established and communicated.
 - Identify.Governance-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed.
 - Identify. Risk Assessment-1: Asset vulnerabilities are identified and documented.
 - Protect. Information Protection Processes and Procedures-2: A System Development Life Cycle to manage systems is implemented.

CONTACT INFORMATION

- For questions about this policy, please contact the [WaTech Policy Mailbox](#)
- For risk management document submissions, contact the [WaTech's Risk Management Mailbox](#).
- For technical questions or to request a Security Design Review, please contact sdr@watech.wa.gov.