SEC-11
State CIO Adopted: February 11, 2023
TSB Approved: February 11, 2023
Sunset Review: February 11, 2026

Replaces:
IT Security Standard 141.10 (1.2)
December 11, 2017

INFORMATION SECURITY

RISK MANAGEMENT POLICY

See Also:
RCW 43.105.054 WaTech Governance
RCW 43.105.052 Powers and duties of agency—Application to higher education, legislature, and judiciary.
RCW 43.105.020 (22) "State agency"
RCW 43.105.450 Office of Cybersecurity
RCW 43.105.450 (7c) IT Security
NIST 800-37 - Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy.

The below points are organized by the seven steps of the National Institute of Standards and Technology Risk Management Framework (NIST RMF).

1. **Prepare Step: Agencies must define and document a risk management strategy appropriate to their mission.**

    a. Agencies must define their risk appetite and risk tolerance levels.

    b. Agencies must either mitigate or accept identified risks prior to their systems being placed into operation.

    c. Residual risk must be accepted by an agency officer authorized to make risk treatment decisions. Approval authority may be delegated if documented in writing, but ultimate responsibility for risk acceptance cannot be delegated.

    d. Agencies must develop a risk monitoring strategy.

2. **Identify Step: Agencies must identify the security categorization of its systems based on the data processed.**

    a. Refer to the SEC-08-01-S Data Classification Standard for data categorization requirements.

    b. Refer to SEC-02 Security Assessment and Authorization Policy for system categorization requirements.

3. **Select Step: Agencies must select controls appropriate for the environment.**

    a. Select risk mitigation controls from the latest versions of the Center for Internet Security (CIS) and NIST 800-53 - Security and Privacy Controls for Information Systems and Organizations controls frameworks. Agencies can select additional control frameworks as informed by their compliance requirements.

    b. Identify the parties responsible for managing, configuring, and operating the controls in their environments.

4. **Authorize Step: Agencies must authorize and document their risk management strategy.**

    a. This step applies to risk assessment associated with:

        i. The procurement of a new information system or service.

        ii. Significant changes to an existing information system's technology or in the data categories it stores, processes, or transmits.

    b. Submit the Risk Treatment Plan (RTP) for review according to SEC-02 Security Assessment and Authorization Policy.

    c. Provide their RTPs from the current controls assessment to WaTech.

5. **Implement Step: Agencies must implement the controls selected in Step 3 to treat the identified risk and document how the controls are deployed. Agencies must prepare the Risk Treatment Plan after the inherent risk is calculated to determine the best approach to mitigate the risk to an acceptable level. Treatment approaches include:**

    a. Risk acceptance means agencies must define their level of risk tolerance.

        i. The agency risk owners must sign off that they accept residual risks identified during the risk assessment.

    b. Risk mitigation is appropriate when an agency chooses to reduce risk by applying preventive, detective, or corrective controls:

i. Preventive controls – Mitigate risk by reducing the likelihood of a threat actor taking advantage of a vulnerability.

ii. Detective controls – Mitigate risk by monitoring for risk indicators, thus reducing the potential impact.

iii. Corrective controls – Mitigate risk by reducing the impact of risk once it is detected. Corrective controls remedy flaws that enabled a risk to occur.

c. Risk sharing shifts a portion of the risk responsibility or liability to other organizations. Liability is generally established by legislation or policy and may not be transferred.

d. Risk avoidance is when an agency entirely avoids activities that may cause the risk to materialize.

e. Agencies must rank the effectiveness of the risk-mitigation controls they select. Agencies must base this ranking on the qualitative scale shown below:

Control Effectiveness Rating	Control Effectiveness Measurement	Reduction in Likelihood Rating
Effective	1	50%
Partially Effective	2	25%
Ineffective	3	0%

6. **Residual Risk: Agencies must document, accept, and monitor the calculated risk remaining after the risk treatment plan is applied. Residual risk is calculated as follows:**

Impact * (Likelihood * Control effectiveness reduction) = Residual risk

7. **Monitor Step: Agencies must implement their system and environment monitoring strategies.**

a. Agencies must identify, document, and monitor for Key Risk Indicators (KRI), a metric used to provide an early signal of increasing risk exposure.

b. Analyze and respond to the output of system and environmental monitoring.

c. Annually report any unmitigated cybersecurity risk or compliance audit finding to WaTech (see SEC-09 IT Security Audit and Accountability Policy):

i. Agencies must identify and document the KRI review frequency that is commensurate with risk's rating. For example, KRI's related to high risks will be monitored with more frequency than KRI's for moderate or low risks.

ii. Update the Risk Assessment: Update the existing risk assessment using the results from ongoing monitoring of risk factors.

8. **Assess Step: Agencies must annually assess whether their controls are operating as designed.**

9. **Agencies must designate individuals responsible for satisfying the requirements set forth in this policy within their security program documentation, or delegate roles to WaTech as agreed under service agreements:**

a. Information Security Managers (ISMs): Responsible for assessing and mitigating risks using the approved process.

b. Information System Owners (ISOs) or agency equivalent: Responsible for ensuring that information systems under their control are assessed for risk and that identified risks are mitigated, transferred, or accepted.

c. Chief Information Security Officer or agency equivalent: Responsible for validating systems and specifications to facilitate agency compliance with this policy.

d. Chief Information Officer, or agency equivalent: Responsible for ensuring that their agency conducts risk assessments on information systems and uses the WaTech approved process.

10. **WaTech provides service support for agencies as agency equivalent authorities where agreed, as well as providing guidance on RTPs and business process development.**

REFERENCES

1. Definition of Terms Used in WaTech Policies and Reports.
2. NIST Risk Management Framework.

3. SEC-08-01-S Data Classification Standard.
4. SEC-02 Security Assessment and Authorization Policy.
5. CIS Critical Security Controls (cisecurity.org).
6. NIST 800-53 - Security and Privacy Controls for Information Systems and Organizations.
7. NIST Cybersecurity Framework Mapping 2.0:
    - ID.RM-1: Risk management processes are established, managed, and agreed to by organizational stakeholders.
    - ID.RM-2: Organizational risk tolerance is determined and clearly expressed.
    - RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks.
    - ID.GV-2: Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners.
    - ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis.

CONTACT INFORMATION

- For questions about this policy, please email the WaTech Policy Mailbox.
- For technical assistance, please email Risk Management.