Policy & Standard Background

Name: Risk Assessment Standard

New

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.

The 2017 version of OCIO 141.10 sections 1.1 identifies risk assessments as a key document in a security program, section 1.2 describes the appropriate times to conduct assessments, periodic, new or changed system, systems with category 3 and 4 data. Section 1.5 establishes risk assessments as part of compliance activities. Section 4.3 establishes the risk assessment as a step in the secure management of data. The new standard streamlines these requirements in a single document by building it on the framework detailed in NIST 800-30r1, Guide for Conducting Risk Assessments.

What is the business case for the policy/standard?

- **A formal risk assessment framework allows agencies to assess risk in a consistent fashion and enables the comparison of risk between agencies.**
- **Common foundations aligning with NIST allow for consistent measurement, solution interoperability, and reduced overhead using common documentation acceptable to multiple regulatory agencies.**

What are the key objectives of the policy/standard?

- **Provide standards for conducting risk assessments of state information systems.**
- **Provide leaders with information needed to make decisions according to their risk appetite and risk tolerance as determined by their risk management posture.**

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

- **This standard aligns with existing processes while integrating federal standards that are widely adopted.**

- **A common language and baseline promotes accountability and transforms ad hoc procedures into reproducible, measurable results.**

What are the implementation considerations?

- **Training opportunities to educate agencies will be needed, including online videos and workshops.**
- **Risk assessment templates will need to be provided to support agencies.**

How will we know if the policy is successful?

- **Agencies will perform risk assessments consistently and at necessary decision points.**
- **Agencies will report key risk indicators for the monitoring of risk.**
- **Agencies will track and monitor risks.**

State CIO Adopted:
TSB Approved:
Sunset Review:

WaTech
Washington Technology Solutions
Washington's Consolidated Technology Services Agency

Replaces:
IT Security Standard 141.10 (1.2.1)
December 11, 2017

INFORMATION SECURITY
RISK ASSESSMENT STANDARD

See Also:

RCW 43.105.450 Office of Cybersecurity
RCW 43.105.205 (3) Higher Ed
RCW 43.105.054 OCIO Governance
RCW 43.105.020 (22) "State Agency"

1. **Agencies must conduct risk assessments at critical points:**

    a. Prior to the acquisition of an information system, Cloud Service, or managed service which will store, process, or transmit Category 3 or Category 4 data.

    b. When an existing agency-controlled information system undergoes a significant change in technology or use. Examples include significant software upgrades, changes in hosting platforms or vendors, or changes in the data categorization or volume of records stored, processed, or transmitted by the system.

    c. At least once every three years for all agency-controlled information systems that store, process, or transmit Category 3 or Category 4 data.

    d. Annually for information systems the agency deems to be business essential.

    e. Prior to the sharing of Category 3 or Category 4 data with agencies and/or vendors. See the Data Sharing Policy for details.

    f. When a security patch is not applied.

2. **Agencies must prepare for the risk assessment by identifying the purpose, scope, assumptions and constraints, threat intelligence sources, and risk model and analytic approach.**

    a. Identify Purpose: Agencies must identify how it will use the risk assessment and the information needed to achieve that goal.

    b. Identify Scope: Agencies must identify the scope in terms of the technology/systems to be assessed, the categorization of data processed by those systems, and the risk owners for those systems.

    c. Identify Assumptions and Constraints: Agencies must identify the specific assumptions and constraints under which the risk assessment is conducted.

    d. Identify Threat Intelligence Sources: Agencies must identify the sources of descriptive, threat, vulnerability, and impact information to be used in the assessment. WaTech risk management resources that are designated for this purpose satisfy this standard.

e. Identify Risk Model and Analytic Approach: The methodology described in this standard provides agencies with a baseline risk assessment approach. Agencies must identify any supplemental risk models and/or analytic approaches appropriate to the risk assessment goals.

3. **Agencies must conduct risk assessments to identify threat sources, threat events, likelihood, impact, and risk.**

   a. Identify Threat Sources: Agencies must identify and characterize threat sources of concern to assets within the scope of the assessment; including capability, intent, and targeting characteristics for adversarial threats and range of effect for non-adversarial threats. The Vulnerability Management Standard includes threat intelligence requirements.

   b. Identify Threat Events: Agencies must identify actions that threat sources may initiate exploit vulnerabilities. The Vulnerability Management Standard includes requirements for threat event identification. This includes vulnerabilities identified by vendors or those discovered using hardware/software vulnerability scans.

   c. Determine Likelihood: Agencies must estimate the likelihood that threat events of concern result in adverse impacts, considering:

      i. The characteristics of the threat sources that could initiate the events.
      ii. The vulnerabilities identified.
      iii. The organizational susceptibility reflecting the safeguards/countermeasures planned or implemented to impede such events. Likelihood can be expressed either qualitatively, quantitatively, or semi-qualitatively depending on agency needs.

   Agencies must base their qualitative likelihood criteria on the below likelihood scale:

Likelihood Rating	Likelihood Measurement	Chance of the Risk Occurrence Within a Year
High	5	Greater than 80%
Moderately High	4	Greater than 60% and less than/equal to 80%
Moderate	3	Greater than 40% and less than/equal to 60%
Moderately Low	2	Greater than 20% and less than/equal to 40%
Low	1	Less than/equal to 20%

d. Determine Impact: Agencies must determine the adverse impacts from the threat events of concern, considering:

i. The characteristics of the threat sources that could initiate the events.
ii. The vulnerabilities identified.
iii. The organizational susceptibility reflecting the safeguards/countermeasures planned or implemented to impede such events.

Agencies must base their qualitative impact criteria on the below impact scale:

Impact Rating	Impact Measurement
High	5
Moderately High	4
Moderate	3
Moderately Low	2
Low	1

e. Determine Risk: Agencies must identify the risks posed by threat actors attacking vulnerabilities within the assessment scope. Inherent risk: Inherent risk is the impact and likelihood of a risk in the absence of controls. Inherent risk is calculated as follows:

Impact * Likelihood = Inherent Risk

Agency must rank their qualitative risk ratings on the scale below:

Residual Risk		Likelihood				
		High (5)	Moderately High (4)	Moderate (3)	Moderately Low (2)	Low (1)
Impact	High (5)	25	20	15	10	5
	Moderately High (4)	20	16	12	8	4
	Moderate (3)	15	12	9	6	3
	Moderately Low (2)	10	8	6	4	2
	Low (1)	5	4	3	2	1

4. **Agencies must communicate and share risk assessment results.**

    a. Agencies must communicate and share risk assessment results to appropriate agency decision makers and stakeholders to support risk response.

    b. Agencies must share risk-related information produced during the risk assessment with appropriate organizational personnel.

    c. Agencies are encouraged to consult with WaTech regarding any project to determine whether a Security Design Review and risk assessment is recommended.

REFERENCES

1. Risk Management Framework for Information Systems and Organizations (RMF).
2. National Institute of Standards and Technology (NIST) Special Publication 800-30 Revision 1, Guide for Conducting Risk Assessments.
3. NIST SP 800-39
4. CIS Critical Security Controls (cisecurity.org)
5. Risk Management Policy
6. Data Classification Standard
7. Security Assessment and Authorization Policy.
8. Vulnerability Management Standard
9. Definition of Terms Used in WaTech Policies and Reports
10. NIST Cybersecurity Framework Mapping
    - Identify.Asset Management-5: Resources are prioritized based on their classification, criticality, and business value
    - Identify.Risk Assessment-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk.

CONTACT INFORMATION

- For questions about this policy, please contact the WaTech Policy Mailbox.
- For technical security questions or to submit risk assessments, please contact the WaTech Risk Management Mailbox.
- To request a Security Design Review, please contact sdr@watech.wa.gov.