WaTech
Washington Technology Solutions

IT Security Audit and Accountability Standard 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 standard expands on and replaces the current 141.10 (1.5,6) requirements. It also requires agencies to identify the root causes associated with audit findings and document a plan to remediate those findings.

What is the business case for the policy/standard?

- The audit process helps agencies identify areas of non-compliance they must address.
- Agencies require a risk-based mechanism to request a time-bound compliance waiver.

What are the key objectives of the policy/standard?

- Specify agency requirements agencies must follow when performing independent IT Audits.
- Require agencies to determine the cause of non-conformities to inform a risk-based control strategy.
- Require agencies to document an audit nonconformity resolution plan.

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

This policy supports both achieving compliance with state security policies/standards and the risk-based management of compliance nonconformities.

What are the implementation considerations?

- Agencies must ensure the independence of the team performing an audit, regardless of whether it is internal to the agency or an external auditor.
- Agencies must coordinate with the State Auditor's Office to ensure audits align with agreed-upon audit procedures.
- Agencies must develop a root-cause analysis process to analyze audit findings.

How will we know if the policy is successful?

Specific: Agencies will be able to confirm IT auditor independence.
Measurable: Agencies have IT audit performance procedures to ensure consistent IT audits.
Achievable: Agencies will be able to produce a documented plan to resolve audit findings.
Relevant: Auditing provides a checkpoint for agencies to measure compliance to their own IT policies and state IT policies.
Timebound: Agencies will perform audits every three years as required.
Equitable: Agreed upon procedures ensure that every audit is run the same way for consistency regardless of the agency.

SEC-09
State CIO Adopted:
TSB Approved:
Sunset Review:

WaTech
Washington Technology Solutions

Replaces:
IT Security Standard 141.10 (1.5e-1.6)
December 11, 2017

IT SECURITY AUDIT AND ACCOUNTABILITY STANDARD

See Also:
RCW 43.105.450 OCIO Governance
RCW 43.105.054 Office of Cybersecurity
RCW 43.105.020 (22) "State agency"
RCW 43.105.205 (3) Higher Ed

1. **Agencies must ensure an audit is performed once every three years to determine compliance with WaTech's IT security policies and standards.**

    a. Ensure the audit is performed by a qualified individuals accredited by an authorizing body, such as Information Systems Audit and Control Association (ISACA), Institute of Internal Auditors (IIA), American Institute of Certified Public Accountants (AICPA) or another nationally recognized information technology auditing certification.

    b. Agencies must refer auditors to the State Auditor's Office (SAO) to ensure information security audits are performed in accordance with the SAO's agreed upon procedures.

    c. The auditor must be independent of the agency's IT organization but may be within the agency.

    d. Submit the triennial audit notice of completion to the State Chief Information Security Officer risk management mailbox within thirty calendar days of the final audit report.

    e. Maintain documentation showing the results of the audit according to applicable records retention requirements.

2. **Agencies must respond to IT security audit non-conformities.**

    a. Within three months of the final audit report date, agencies must identify the root causes of their audit findings.

    b. Agencies must document and implement a waiver request according to the Technology Policy and Standards Waiver Request with a plan to correct audit nonconformities and track progress. Agencies must submit this plan to the State Chief Information Security Officer.

REFERENCES

1. Definition of Terms Used in WaTech Policies and Reports.
2. About IT Audits | Office of the Washington State Auditor.
3. NIST Cybersecurity Framework Mapping
    - 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. Supply Chain Risk Management-4: Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.

CONTACTS

- For questions about this standard, please email the policy mailbox.
- For technical questions, please email the risk management mailbox.
- For questions regarding the SAO process, please email SAOITAUDIT@sao.wa.gov.