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.

Disaster Recovery Planning 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 is an update to the existing policy 151. Changes were made based on workgroup and community feedback to improve clarity for agency adoption and accountability. Updates to this standard draw from NIST SP 800-34 Rev. 1, Contingency Planning Guide for Federal Information Systems and NIST 800-53 Security and Privacy Controls for Information Systems and Organizations.

What is the business case for the policy/standard?

- Disaster recovery planning is essential for ensuring that mission critical and business essential functions can be resumed in the event of a disruption.
- Implementation of governance that limits runaway liability to operational, financial, safety, and reputational impacts

What are the key objectives of the policy/standard?

- Create a common understanding of disaster recovery planning requirements.
- Require testing of disaster recovery plans to validate contingency and recovery procedures.

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

Disaster recovery planning strengthens IT architecture security. Documentation of planning and validation supports accountable government.

What are the implementation considerations?

- Implementing a DRBC program requires an investment in planning, resources, and regular testing

- Small agencies have the option of contracting WaTech for support. WaTech will also provide templates and consultation for DR planning for agencies of all sizes.
- Prioritization of training and testing and coordination of efforts for interdependent systems.

How will we know if the policy is successful?

Specific: All agencies will document and test disaster recovery plans for mission critical and business essential functions.
Measurable: Agencies will validate test plans.
Achievable: The requirement for exercising plans was adjusted to every other year to ensure agencies have time to exercise each component of the plan.
Relevant: The recent pandemic demonstrated the need for agility in returning to normal operations that are not always identical to the original state.
Timebound: Agencies must complete DR reviews and testing annually as a minimum.
Equitable: Agencies of any size can rely on WaTech for support with DR planning, templates and tools.

WaTech
Washington Technology Solutions

IT Security Awareness and Training 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.

The original standard items on security awareness were consolidated and modified based on workgroup and community feedback to improve clarity for agency adoption and accountability. The update replaces 141.10 1.4, 2.1,4,5. Additional updates to this policy draw from NIST 800-53 Security and Privacy Controls for Information Systems and Organizations.

What is the business case for the policy/standard?

- Basic cybersecurity awareness training for all IT system users enhances the primary line of defense to maintain business continuity.
- This policy ensures agency staff have awareness and training aligned with their role in IT security.

What are the key objectives of the policy/standard?

- Ensure that users are familiar with potential threats to the IT ecosystem and aware of strategies they must employ to prevent or respond.
- Agency staff who have IT and IT security-related roles are informed and recognize their roles and responsibilities.

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 will need review and verify that their awareness and training requirements are sufficient
- Agencies may request additional training and support.

- Additional specific training cannot be designated to IT system users who do not already have this included in their job descriptions, but training paths can be suggested.

How will we know if the policy is successful?

Specific: Agency IT system users attest to their awareness of their duties and obligations.
Measurable: Activity and feedback on the awareness and training materials can be reported.
Achievable: WaTech offers basic cybersecurity training awareness for all agencies.
Relevant: People who are unaware of the cybersecurity risk are far more likely to allow a threat into the system than those who receive basic training.
Timely: Ransomware and other malware are easier than ever to deploy, so the risk will only continue to increase.
Equitable: Agencies of all sizes benefit when everyone completes basic cybersecurity awareness training. Agencies with additional resources and responsibilities will have corresponding needs for additional training.

WaTech
Washington Technology Solutions

Physical and Environmental Protection 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 standard expands on and replaces the current 141.10 (3) requirements. Changes were made based on workgroup and community feedback to improve clarity for agency adoption and accountability.

Updates to this policy draw from the GSA procedural guide CIO-IT Security-12-64 Physical and Environmental Protection (PE) which is based on NIST SP 800-53.

What is the business case for the policy/standard?

- Physical and environmental security must be commensurate with the risks, threats, and vulnerabilities unique to IT assets and their physical site, and geographic location.
- Physical and environmental security are essential controls to ensure agencies can conduct state business safely and with the assurance of the confidentiality, integrity, and availability of state information.

What are the key objectives of the policy/standard?

- Establish the requirements for mitigating the risks from physical security and environmental threats through the establishment of effective physical security and environmental controls.
- Establish requirements for physical security controls for State and agency data centers and information technology (IT) resources within or external to those data centers.

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 resources comprehensively.

What are the implementation considerations?

- Agencies will need to engage with facility management in cases of joint tenancy and will need to consider compensating controls when the modifications are not possible due to lease restriction or other limitations.
- Agencies will need update their procedures and documentation to align with new technologies on the premises both assets and protective measures.

How will we know if the policy is successful?

Specific: Agencies have documentation people, processes, and technology responsible for the physical and environmental controls within controlled areas.
Measurable: Agencies will use centralized inventories to understand the agency's IT profile and support a secure environment.
Achievable: Agencies will be able to produce a documented plan to resolve deficiencies.
Relevant: Documentation is available for disaster preparedness, business continuity, and other related exercises.
Timebound: Agencies maintain their documentation when changes happen and ensure they are up to date for audits every three years.
Equitable: Agreed upon procedures ensure that every audit is run the same way for consistency regardless of the agency.

WaTech
Washington Technology Solutions

Remote Access Standard Background

New, Update or Sunset Review? 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 addresses remote access at a high level. This new standard includes content from NIST 800-46 Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security.

What is the business case for the policy/standard?

This standard ensures accountability and the implementation of controls for remote access to the State Government Network and the information assets within.

What are the key objectives of the policy/standard?

The key objective of this standard is to establish consistent practices to enable agency staff to access the State Government Network while denying or limiting the access of unauthorized activities.

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 resources comprehensively.

What are the implementation considerations?

Agencies will configure their remote access solution in accordance with this standard.

How will we know if the policy is successful?

Specific: Agencies will only allow authorized access to resources on the agency's network.
Measurable: Analysis of the remote connection logs collected by the Office of Cybersecurity and host agencies will evidence compliance.
Achievable: Agencies will be able to demonstrate the approval request process and their configuration files demonstrating least privilege.

Relevant: Limiting or denying access to unauthorized activities is a key component of asset protection.

Timebound: Agencies will update their processes and documentation in preparation for audits every three years including compensating controls for those not yet in place.

Equitable: Agreed upon procedures ensure that every audit is run the same way for consistency regardless of the agency.

WaTech
Washington Technology Solutions

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.