KirkpatrickPrice

Preparing for a FISMA Audit

FISMA is U.S. legislation intended to protect government information and assets from unauthorized access, use, disclosure, disruption, modification, or destruction. To comply with FISMA, organizations must demonstrate that they meet the standards set forth by NIST. How can you prepare for a FISMA audit? Start with this checklist before entering into a gap analysis or audit.

- ☐ **Access Control**

  In order to prevent unauthorized access to assets, systems, and applications, organizations must define how they limit and safeguard access.

- ☐ **Awareness and Training**

  Personnel must partake in formal security training so they gain an awareness of security risks associated with their responsibilities.

- ☐ **Audit and Accountability**

  For accountability purposes, there must be a way to trace information system users' activity and audit all unauthorized or inappropriate activity.

- ☐ **Configuration Management**

  Proper configuration is a pillar of data security. Organizations must implement, enforce, and maintain baseline configurations of information systems.

- ☐ **Contingency Planning**

  Contingency planning is a key factor in minimizing business disruption. Organizations should maintain an updated, implemented Business Continuity Plan.

- ☐ **Identification and Authentication**

  Organizations must identify and verify the identities of all system users. To do so, organizations may need to utilize MFA, follow role-based access practices, or set password rules.

- ☐ **Incident Response**

  When a security incident occurs, a formal, established process must be followed to ensure it's found, contained, and fixed.

- ☐ **Maintenance**

  The appropriate tools and techniques must be provided to run maintenance activities on all information systems.

☐ **Media Protection**

Media must be protected in storage, transport, sanitization, and use. Organizations should develop a media protection policy to ensure security practices are in place.

☐ **Physical and Environmental Protection**

Unauthorized physical access, damage to equipment or facilities, and theft can cause business disruptions. What protections are in place to mitigate physical and environmental threats?

☐ **Personnel Security**

Personnel must be screened prior to authorizing access to information systems with sensitive information.

☐ **Risk Assessment**

A risk assessment is fundamental to any organizational risk management program and is a methodology used to identify, assess, and prioritize organizational risk.

☐ **System and Services Acquisition**

When new information systems are introduced, they must be secured from the start and maintained throughout their lifecycles.

☐ **System and Communications Protection**

All information within an organization's network must be protected, whether it's being stored, processed, archived, destroyed, or transferred.

☐ **System and Information Integrity**

Organizations identify, report, and correct information system flaws in an appropriate and timely manner.