

Does a SAS 70 Audit Leave you at Risk of a Security Exposure or Failure to Comply with FISMA?

A brief overview of security requirements for Federal government agencies applicable to contracted IT services, applications and outsourced business processes. This paper examines the use of a common industry assessment method to reveal differences in scope and intent with that of FISMA and NIST. These differences result in gaps that impact both Federal Government agencies and the solutions and services providers that serve them.

Does the SAS 70 Audit Meet the Requirements of FISMA and NIST?

Executive Summary

This whitepaper examines the requirements of Federal Information Security Management Act (FISMA) and associated NIST security standards that define the Federal Government information security framework. When Government uses outsourcing, managed services or software as a service (SaaS) approaches for business services or technology solutions, commercial providers must meet government security standards. A common industry assessment standard used is known as the Statement of Auditing Standards (SAS) No. 70. The objective of this paper is to contrast the SAS 70 assessment method to the FISMA requirements and NIST standards to highlight the differences and gaps which Federal government agencies must be aware and solution providers must address.

Background



The E-Government Act (Public Law 107-347) of 2002, Title III [Federal Information Security Management Act \(FISMA\)](#) recognized the importance of information security to the economic and national security interests of the United States. FISMA requires federal agencies to develop, document, and implement an information security program for the information and information systems that support the operations and assets of the agency, ***including those provided or managed by a contractor.***

FISMA requires the National Institutes of Standards and Technology (NIST) to develop standards and guidelines, including minimum requirements, for providing adequate information security for all agency operations and assets. The objective of FISMA and the NIST standards is to provide the means for agencies to accomplish their stated missions with security commensurate with risk.

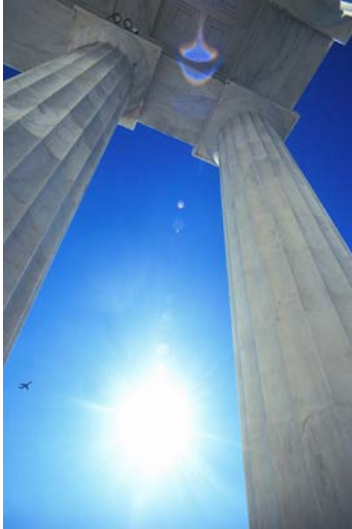
FISMA, together with NIST standards and guidance from the Office of Management and Budget (OMB), form a framework for developing and maturing an information security program. The framework spans program development, definition of controls and their assessment, the resulting certification and accreditation of system. The framework also supports the ongoing management and monitoring of processes and controls, continual assessment of threats and the ongoing management of risk and change.

In 2006, OMB issued guidance ([OMB Memo 06-20](#)) to Federal Agencies that requires each agency to ensure contracted services, systems and operations comply with FISMA and NIST security in an “equivalent” manner. In this guidance, OMB also requires each agency Office of Inspector General (OIG) to

Does the SAS 70 Audit Meet the Requirements of FISMA and NIST?

annually review a subset of each agency's contracted systems. Therefore, businesses that offer services and solutions to the Federal government must obtain certification and accreditation of its systems and associated operational, management and technical controls in accordance with NIST.

Government Outsourcing That Involves Data and Technology



When Federal government agencies engage vendors and commercial service providers to provide a service or capability that involves transmission, storage or processing of Government information, agencies must ensure these providers comply with FISMA and NIST. With the recent guidance from OMB, vendors and commercial service providers should expect increased security requirements in contracts and task orders. Two specific security controls in NIST SP 800-53 that deserve special attention in this context are:

SA-4 Acquisitions

Control: The organization includes security requirements and/or security specifications, either explicitly or by reference, in information system acquisition contracts based on an assessment of risk and in accordance with applicable laws, Executive Orders, directives, policies, regulations, and standards.

Supplemental Information: The solicitation documents (e.g., Requests for Proposals) for information systems and services include, either explicitly or by reference, security requirements that describe: (i) required security capabilities (security needs and, as necessary, specific security controls and other specific FISMA requirements); (ii) required design and development processes; (iii) required test and evaluation procedures; and (iv) required documentation. The requirements in the solicitation documents permit updating security controls as new threats/vulnerabilities are identified and as new technologies are implemented. [...] The level of detail required in the documentation is based on the FIPS 199 security category for the information system. [...] The information system required documentation includes security configuration settings and security implementation guidance. OMB FISMA reporting instructions provide guidance on configuration requirements for federal information systems. NIST Special Publication 800-70 provides guidance on configuration settings for information technology products.

SA-9 Outsourced Information System Services

Control: The organization: (i) requires that providers of external information system services employ adequate security controls in accordance with applicable laws, Executive Orders, directives,

Does the SAS 70 Audit Meet the Requirements of FISMA and NIST?

policies, regulations, standards, guidance, and established service-level agreements; and (ii) monitors security control compliance.

Supplemental Information: An external information system service is a service that is implemented outside of the accreditation boundary of the organizational information system (i.e., a service that is used by, but not a part of, the organizational information system). Relationships with external service providers are established in a variety of ways, for example, through joint ventures, business partnerships, outsourcing arrangements (i.e., through contracts, interagency agreements, lines of business arrangements), licensing agreements, and/or supply chain exchanges. Ultimately, the responsibility for adequately mitigating risks to the organization's operations and assets, and to individuals, arising from the use of external information system services remains with the authorizing official. Authorizing officials must require that an appropriate chain of trust be established with external service providers when dealing with the many issues associated with information system security. For services external to the organization, a chain of trust requires that the organization establish and retain a level of confidence that each participating service provider in the potentially complex consumer-provider relationship provides adequate protection for the services rendered to the organization. Where a sufficient level of trust cannot be established in the external services and/or service providers, the organization employs compensating security controls or accepts the greater degree of risk to its operations and assets, or to individuals. The external information system services documentation includes government, service provider, and end user security roles and responsibilities, and any service-level agreements. Service-level agreements define the expectations of performance for each required security control, describe measurable outcomes, and identify remedies and response requirements for any identified instance of non-compliance.

Does the SAS 70 Audit Meet the Requirements of FISMA and NIST?

FISMA and NIST Requirements Compared to SAS 70 Type II Audit



The table below presents an analysis of the critical aspects of the Federal government FISMA regulation and associated NIST security standards. For each critical area, the SAS 70 Type II audit feature is examined. Links are included to supporting referenced information.

| Category | Federal Government Security and Privacy Requirements | Type II SAS 70 Audit |
|------------------------|---|---|
| Governing Organization | <p>Office and Management and Budget (OMB) issues guidance on implementation of FISMA.</p> <p>National Institute of Standards and Technologies (NIST) issues standard and best practices associated with implementation of FISMA.</p> | <p>Statement on Auditing Standards (SAS) No. 70, (SAS 70) is an internationally recognized auditing standard developed by the American Institute of Certified Public Accountants (AICPA).</p> |
| Target Industries | <p>Federal Government agencies with unclassified, non-national security systems.</p> <p>Companies that provide services and solutions to the Federal Government where government information is processed or stored in the Company's computer systems.</p> | <p>Financial Services, Technology and Business Process Outsourcing, Healthcare, Insurance.</p> |
| Scope | <p>A framework and standards for the evaluation and continuous monitoring of operational, management and technical controls related to the system or application. The scope contains the following high-level areas:</p> <ul style="list-style-type: none"> Description of the system, security controls and organization Categorization of the system, its information and functions according to national standards for security impact Independent Security Test and Evaluation f controls. Assessment of risk and determination of impacts Certification and accreditation Daily, monthly, quarterly and annual tasks to maintain operation within acceptable risk. <p>A certification is valid for up to 3 years if the system is properly continuously monitored and there are no significant changes.</p> | <p>An assessment of the controls associated with the system, service or application structured in a way to identify weaknesses to system owner and its clients/customers. The scope contains the following elements:</p> <ul style="list-style-type: none"> Independent auditor's report with their opinion. Service organization's description of controls. Information provided by the independent auditor; includes a description of the auditor's tests of operating effectiveness and the results of the tests. <p>A Type I audit includes the service organization's description of its controls and objectives, and an auditor's opinion on the suitable design of the controls in meeting the specified objectives. The Type I report reflects an opinion at a specified point in time.</p> <p>A Type II audit, additionally includes test and evaluation of the effectiveness of the internal controls. The Type II attests, with reasonable assurance, to the effectiveness of the controls in meeting the specified objectives over a period of time, typically 6 months.</p> |
| Security Frameworks | <p>In the Federal Government, NIST provides the framework for security through its Special</p> | <p>A variety of security frameworks exist in the private sector ranging from:</p> |

Does the SAS 70 Audit Meet the Requirements of FISMA and NIST?

| Category | Federal Government Security and Privacy Requirements | Type II SAS 70 Audit |
|--|---|---|
| | <p>Publications series:</p> <ul style="list-style-type: none"> • FIPS PUB 200 – Minimum Security Requirements for Federal Information and Information Systems • NIST SP 800-37 – C&A guidance • NIST SP 800-18 – Security Plans • NIST SP 800-53 – Security Controls • NIST SP 800-53A – Control Assessment • NIST SP 800-34 – Contingency Plans | <ul style="list-style-type: none"> • ISO 17799 (focus on security-related controls) • COSO (The Committee of Sponsoring Organizations) • ISACA (Information Systems Audit and Control Association) Control Objectives for Information Technology (COBIT) • PCI (Payment Card Industry) Data Security Standard |
| Intended Purpose of the Effort | <p>FISMA, supported by the NIST Special Publication 800-37 “Guide for the Security Certification and Accreditation of Federal Information Systems” is intended to identify risks to the owner of the system and information and provide the processes for quantifying the risks and impacts.</p> <p>The process supports the implementation of a cost-effective, risk-based information security programs that establishes a level of security due diligence for federal agencies and contractors.</p> <p>The result of the process is a consistent and cost-effective application of security controls leading to more consistent, comparable and repeatable security control assessments.</p> <p>The objective is to provide more complete and reliable information to authorizing officials, to facilitate more informed security accreditation decisions.</p> | <p>A SAS 70 effort is audit based intended to provide system owners, their business partners and clients with information about effectiveness of control implementation at the company with regard to assertions in financial statements.</p> <p>The use of the SAS 70 has recently expanded as a tool to demonstrate third-party assessment of controls to support business relationships with partners and clients.</p> |
| Intended Audience of Reports | Owner of the system and/or information, the chief information officer, and business partners that interconnect or share information with the organization through the system. | Corporate industry management, its clients, business partners and external auditors |
| Certification and Accreditation | NIST Special Publication 800-37 supported by the 800 series of publications govern the certification process. The result of execution of the process results in a letter of certification from the certifying authority to the approving authority. The approving authority accepts residual risk and authorizes the system for processing for not greater than 3 years. | A SAS 70 audit does not result in a certification. The audit produces a report of the auditor’s opinions regarding the effectiveness of management and operational controls. These reports can be issued as either “unqualified” or “qualified” opinions. Typically these reports are provided to clients. |
| External Review or Audit | <p>FISMA requires Office of Inspector Generals (OIG) of government agencies to perform annual reviews of agencies which extends to agency systems. OMB has issued guidance that requires OIGs to review BOTH agency-owned systems as well as contracted / outsourced services and systems.</p> <p>The audit standard applied by the OIG is FISMA and related NIST guidance within the audit framework of the President’s Council on Integrity</p> | <p>SAS 70 reports are frequently provided to business partners and clients upon request and their auditors. If the scope of the SAS 70 audit is not sufficient to meet the objectives of the business matter, a follow-up audit can be performed specifying the scope that is required.</p> <p>The audit standard is governed by American Institute of Certified Public Accountants (AICPA).</p> |

Does the SAS 70 Audit Meet the Requirements of FISMA and NIST?

| Category | Federal Government Security and Privacy Requirements | Type II SAS 70 Audit |
|--|---|--|
| | <p>& Efficiency (PCIE) Quality Standards for Inspections.</p> | |
| Controls Spectrum | <p>NIST SP 800-53 defines the security controls required by FISMA.</p> <ul style="list-style-type: none"> • Risk Assessment • Certification and Accreditation • System Services and Acquisition; • Security Planning; • Configuration Management; • System and Communications Protection; • Personnel Security; • Awareness and Training; • Physical and Environmental Protection; • Media Protection; • Contingency Planning; • Maintenance; • System and Information Integrity; • Incident Response; • Identification and Authentication; • Access Control; and • Accountability and Audit <p>The controls are selected based on the security sensitivity of the information and the system (defined by FIPS PUB 199). Low, Moderate and High sensitivities equate to Low, Moderate and High control baselines from NIST SP 800-53.</p> <p>NIST permits tailoring of the controls based on the security sensitivity, system functions, and use of common or compensating controls.</p> | <p>In a SAS 70 audit, the service organization is responsible for describing its control objectives and control activities that might be of interest to auditors. If the service organization does not have a security policy covering a particular area, or has one that allows ineffective security (for example, an organization may not have a policy that ensures secure configuration baselines are maintained through new releases), the SAS 70 audit report could contain a favorable opinion since the control activities would match the stated control objectives which are both none.</p> <p>It is up to the company and the auditor to determine the controls. The selection is often based on either the desired end product or the type of security framework implemented by the company. The controls could include any or all of the following controls:</p> <ul style="list-style-type: none"> • Security Policy • System Access Control • Computer & Operations Management • System Development and Maintenance • Physical and Environmental Security • Compliance • Personnel Security • Security Organization • Asset Classification and Control • Business Continuity Management (BCM) |
| Continuous Monitoring to Maintain Accreditation | <p><u>Ongoing</u></p> <ul style="list-style-type: none"> • Vulnerability Management • Security Configuration Management • Patch Management • Account Management • Audit Review and Management <p><u>As Needed</u></p> <ul style="list-style-type: none"> • Change Management • Security Impact Assessments • Vulnerability Scanning • Penetration Testing <p><u>Quarterly</u></p> <ul style="list-style-type: none"> • POA&M update, review and approval • FISMA performance measures update <p><u>Annually</u></p> <ul style="list-style-type: none"> • Selected Control Testing • Contingency Plan Testing • Incident Response Testing • Update Security Plan • Awareness Training for all users • Specialized training for personnel with significant security responsibilities | <p>Dependent on the defined scope of the SAS 70 audit, the engagement with the audit firm and the security framework implemented by the company.</p> |

Does the SAS 70 Audit Meet the Requirements of FISMA and NIST?

| Category | Federal Government Security and Privacy Requirements | Type II SAS 70 Audit |
|------------------------|---|---|
| Personnel and Training | <p>FISMA requires that organization identify all personnel that perform duties with significant security responsibilities. The organization must track these individuals and ensure appropriate annual training is provided.</p> <p>FISMA also requires that all users of the system complete annual security awareness training to be kept advised of policy and procedures as well as threats and consequences associated with security.</p> | Dependent on the defined scope of the SAS 70 audit and the security framework implemented by the company. |
| Privacy / PII | <p>OMB requires all data that contains information subject to Privacy Act or deemed Personally Identifiable information to be:</p> <ul style="list-style-type: none"> • Encrypted on all data on mobile computers/devices • Protected via two-factor authentication for remote access • Desktop and mobile devices configured to auto-lock screen and require re-authentication after 30 minutes inactivity; and • Log all computer-readable data extracts and verify each extract has been erased within 90 days or its use is still required. | Dependent on the defined scope of the SAS 70 audit and the security framework implemented by the company. |
| Incident Response | Organization complies with FISMA and US-CERT incident handling and reporting procedures to include reporting incidents involving PII. | Dependent on the defined scope of the SAS 70 audit and the security framework implemented by the company. |
| Internet Connections | Provider is an OMB-approved TIC. | Dependent on the defined scope of the SAS 70 audit and the security framework implemented by the company. |
| Security Configuration | Contractor systems meet NIST defined standard security configuration baselines for platforms, have a process to continually monitor compliance and track deviations and associated remediation progress. | Dependent on the defined scope of the SAS 70 audit and the security framework implemented by the company. |

Does the SAS 70 Audit Meet the Requirements of FISMA and NIST?

Conclusions



A SAS 70 audit is a snapshot in time of an organization, its system and associated internal controls. It is not focused solely on security and it does not provide a framework for program development, continual improvement and continuous monitoring. A SAS 70 Type II audit provides valuable insights into a company's services, but alone does not meet the requirements of a FISMA / NIST certification and accreditation. Organizations must develop and implement a security program that incorporates the security framework(s) depending on the industries its serves.

Next Steps

Federal Government Agencies

SecureIT assists program offices to efficiently incorporate the appropriate security requirements into acquisitions. Working with your contracting officers, COTRs and Program Managers, SecureIT can assist your team to effectively incorporate security requirements and to identify security performance measures appropriate for your business need. This will enable you to monitor security performance and compliance of the provider. SecureIT provides independent assessment, measurement and monitoring services after contract award to assist Government customers to monitor security performance, assess impacts, and manage change and risks.

Commercial Vendors and Service Providers

SecureIT can assess your present security framework, identify gaps with FISMA and NIST standards, and provide recommendations to position for NIST certification. SecureIT provides consulting services through the bid and proposal stages to assist your organization to understand government security requirements and to craft solutions that provide value and demonstrate compliance. Following contract award, companies can engage SecureIT to prepare the required NIST security artifacts and perform a NIST-based certification and accreditation of the system or service your organization offers to Federal government agencies. Our ongoing security support services ensure your organization maintains its accreditation.

Does the SAS 70 Audit Meet the Requirements of FISMA and NIST?

About SecureIT

SecureIT helps private and public sector clients manage technology risks and create value through effective practices in IT security. SecureIT provides services and solutions in the areas of Cybersecurity, Information Assurance, Governance & Compliance, IT Audit, and Security Training. SecureIT designs enterprise security programs, implements best practices and assesses technology implementation for security risk. Professionals with industry knowledge and technical expertise devise strategies and solutions to reduce risk, increase efficiency and overcome the challenges of compliance. Located in Reston, VA, SecureIT serves clients in the Federal government including; DISA, HHS, DOJ, Treasury, Commerce, USAID, Education, DHS, and IMF as well as as the private sector with clients such as Freddie Mac, CSC, FINRA, and E*TRADE.

For more information, call 703.464.7010, email info@secureit.com or visit www.secureit.com

Notice

The SECURE|IT logo, and all page headers, footers and icons are trademarks or registered trademarks of SecureIT Consulting Group. Other company names or products mentioned are or may be trademarks of their respective owners. Information in this document is subject to change without notice.