aronson LLC
ASSURANCE | TAX | CONSULTING
Expanding What's Possible

Decoding FISMA Compliance for Government Contractors

LISTENING TO A CONTRACTOR'S CONCERNS

"Our organization would like to pursue government contracts; however, with limited staff and budget, we are concerned about what it will take to comply with the IT security standards and documentation that is required as a result of FISMA."

The Federal Information Security Management Act (FISMA) of 2002 requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor or other source. The newly signed law, the Federal Information Security Modernization Act of 2014 (FISMA 2014), makes several key changes to FISMA that includes an emphasis on continuous monitoring and the notification of security incidents.

Many organizations that would like to pursue government contracts are concerned about what it takes to comply with the IT security standards and documentation that is required as a result of FISMA. In this whitepaper, we walk through the basics of the National Institute of Standards and Technology (NIST) compliance framework, the minimum security requirements, and how organizations can demonstrate FISMA compliance.

NIST COMPLIANCE FRAMEWORK

FISMA requires organizations to meet minimum security requirements by selecting the appropriate security controls as described by NIST Special Publication (SP) 800-53 revision 4, "*Security and Privacy Controls for Federal Information Systems and Organizations.*" Note that organizations must always reference the most current version of NIST SP 800-53 for the security control selection process.

According to NIST, an effective information security program should include the following:

1. **Periodic assessments of risk**, including the magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the organization.

2. **Policies and procedures** that are based on risk assessments that cost-effectively reduce information security risks to an acceptable level and ensure that information security is addressed throughout the life cycle of each organizational information system.

3. **Subordinate plans** for providing adequate information security for networks, facilities, information systems or groups of information systems, as appropriate.

4. **Security awareness training** to inform personnel (including contractors and other users of information systems that support the operations and assets of the organization) of the information security risks associated with their activities and their responsibilities in complying with organizational policies and procedures designed to reduce these risks.

5. **Periodic testing and evaluation** of the effectiveness of information security policies, procedures, practices, and security controls to be performed with a frequency depending on risk, but no less than annually.

6. **Remediation program** including processes for planning, implementing, evaluating, and documenting corrective actions to address any deficiencies in the information security policies, procedures, and practices of the organization.

7. **Security incident management procedures** including processes for detection, reporting, and response.

8. **Continuity of operations plans and procedures** to maintain availability of information systems that support the business needs and assets of the organization.

What is NIST?

The National Institute of Standards and Technology (NIST) is an agency of the U.S. Department of Commerce. NIST works with industries to develop and apply technology, measurements, and standards.

GUIDES FOR IMPLEMENTATION

As a result of the FISMA legislation, NIST established the FISMA Implementation Project in January 2003 to produce several key security standards and guidelines.

FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*

FIPS Publication 200, *Minimum Security Requirements for Federal Information and Federal Information Systems*

NIST Special Publication 800-18 Revision 1, *Guide for Developing Security Plans for Federal Information Systems*

NIST Special Publication 800-30 Revision 1, *Guide for Conducting Risk Assessments*

NIST Special Publication 800-37 Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*

NIST Special Publication 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*

NIST Special Publication 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*

NIST Special Publication 800-53A Revision 4, *Guide for Assessing the Security and Privacy Controls in Federal Information Systems and Organizations, Building Effective Security Assessment Plans*

NIST Special Publication 800-59, *Guideline for Identifying an Information System as a National Security System*

NIST Special Publication 800-60, Revision 1, *Guide for Mapping Types of Information and Information Systems to Security Categories*

NIST Special Publication 800-128, *Guide for Security-Focused Configuration Management of Information Systems*

NIST Special Publication 800-137, *Information Security Continuous Monitoring for Federal Information Systems and Organizations*

SPECIFICATIONS FOR MINIMUM SECURITY REQUIREMENTS

The Federal Information Processing Standards (FIPS) Publication Series of NIST is the official series of publications relating to standards and guidelines for FISMA. Organizations must meet the minimum security requirements detailed in FIPS Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*, and must select the appropriate security controls and assurance requirements as described in NIST SP 800-53. According to these standards, minimum security requirements should include the following:

Awareness and Training

1. Ensure that managers and users of organizational information systems are made aware of the security risks associated with their activities and of the applicable laws, executive orders, directives, policies, standards, instructions, regulations or procedures related to the security of organizational information systems.
2. Ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.

Certification, Accreditation, and Security Assessments

1. Periodically assess the security controls in organizational information systems to determine if the controls are effective in their application.
2. Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems; authorize the operation of organizational information systems and any associated information system connections.
3. Monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.

Audit and Accountability

1. Create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity.
2. Ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.
3. Confirm compliance with minimum auditable event requirements.

Configuration Management

1. Establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.
2. Establish and enforce security configuration settings for information technology products employed in organizational information systems.

Contingency Planning

1. Establish, maintain, and effectively implement plans for emergency response, backup operations, and post-disaster recovery for organizational information systems to ensure the availability of critical information resources and continuity of operations in emergency situations.

Identification and Authentication

1. Identify information system users, processes acting on behalf of users, or devices and authenticate (or verify) the identities of those users, processes or devices, as a prerequisite to allowing access to organizational information systems.

Incident Response

1. Establish an operational incident handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities.
2. Track, document, and report incidents to appropriate organizational officials and/or authorities.

Maintenance

1. Perform periodic and timely maintenance on organizational information systems.
2. Provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.

Media Protection

1. Protect information system media, both paper and digital.
2. Limit access to information on information system media to authorized users.
3. Sanitize or destroy information system media before disposal or release for reuse.

Planning

1. Develop, document, periodically update, and implement security plans for organizational information systems that describe the security controls in place or planned for the information systems and the rules of behavior for individuals accessing the information systems.

Physical and Environmental Protection

1. Limit physical access to information systems, equipment, and the respective operating environments to authorized individuals.
2. Protect the physical plant and support infrastructure for information systems.
3. Provide supporting utilities for information systems.
4. Protect information systems against environmental hazards.
5. Provide appropriate environmental controls in facilities containing information systems.

Personnel Security

1. Ensure that individuals occupying positions of responsibility within organizations (including third-party service providers) are trustworthy and meet established security criteria for those positions.
2. Ensure that organizational information and information systems are protected during and after personnel actions such as terminations and transfers.
3. Employ formal sanctions for personnel failing to comply with organizational security policies and procedures.

System and Services Acquisition

1. Allocate sufficient resources to adequately protect organizational information systems.
2. Employ system development life cycle processes that incorporate information security considerations.
3. Employ software usage and installation restrictions.
4. Ensure that third-party providers employ adequate security measures to protect information, applications, and/or services outsourced from the organization.

Risk Assessment

1. Periodically assess the risk to organizational operations (including mission, functions, image or reputation), organizational assets, and individuals, resulting from the operation of organizational information systems and the associated processing, storage, or transmission of organizational information.

DEMONSTRATING FISMA COMPLIANCE

FISMA requires periodic testing and evaluation of the security controls in an information system to ensure that the controls are effectively designed, implemented, and operating effectively. Security certification, a comprehensive evaluation of security control effectiveness through established verification techniques and procedures conducted by the organization or by an independent third party, is a required activity conducted to give those charged with governance confidence that the appropriate safeguards are in place. It should be noted that any significant modifications to controls may trigger the need for re-certification.

All government agencies, government contractors (including subcontractors), and organizations that exchange data directly with government systems must be FISMA compliant. Currently there is no standard "certification" of FISMA compliance. Phase II of the NIST implementation project is to develop a security assessment credentialing program that details requirements and responsibilities.

For now, contractors should receive direction from their respective agency regarding the expectations for FISMA compliance and how to demonstrate it. An agency might be very specific regarding what they require in terms of certain Information System Security standards and controls or they may require contractors to adhere to all FISMA requirements.

Did You Know?

According to the Office of Management and Budget's 2015 Annual Report to Congress on FISMA,

17

agencies' Inspector Generals (IGs) reported that their departments had programs in place to manage the FISMA compliance of contractor systems.

8

IGs reported that their departments' programs included all required attributes.

9

IGs reported that their departments' programs lacked at least one required element.

RESOURCES

Below are links to resources used for this report. Click the URLs to open the item in your web browser.

- Federal Aviation Administration - Obtain Security Authorization and Accreditation
- FIPS PUB 200 - Minimum Security Requirements for Federal Information and Information Systems
- NIST Information Technology Laboratory - Federal Information Security Management Act (FISMA) Implementation Project
- NIST Computer Security Division - Federal Information Security Management Act (FISMA) Implementation Project
- S.2521 - Federal Information Security Modernization Act of 2014
- Annual Report to Congress: Federal Information Security Management Act

ABOUT ARONSON'S TECHNOLOGY RISK SERVICES GROUP

Our Technology Risk Services Group is committed to helping our clients focus on risks holistically, rather than identifying and measuring risk in a silo. Aronson offers a comprehensive suite of cybersecurity capabilities for contractors including security strategy, security architecture, security risk assessment, contract security compliance assessment and remediation. We align our service delivery with industry leading frameworks such as NIST 800-37 and NIST 800-53.

INTERESTED IN LEARNING MORE?

For more information, contact **Payal Vadhani**, Partner of Aronson's Technology Risk Services Practice, at pvadhani@aronsonllc.com or 301.231.6259.

AUTHORS

Payal Vadhani, CISA
Partner
pvadhani@aronsonllc.com

Melissa Musser, CPA, CISA
Manager
mmusser@aronsonllc.com

ABOUT ARONSON LLC

Aronson LLC provides a comprehensive platform of assurance, tax, and consulting solutions to today's most active industry sectors and successful individuals. For more than 50 years, we have purposefully expanded our service offerings and deepened our industry specialties to better serve the needs of our clients, people, and community. From startup to exit, we help our clients maximize opportunity, minimize risk, and unlock their full potential. For more information about Aronson LLC, please visit www.aronsonllc.com, or call 301.231.6200.