FISMA COMPLIANCE AND CERTIFICATION OVERVIEW FOR FEDERAL CONTRACTORS
FISMA COMPLIANCE & CERTIFICATION OVERVIEW FOR FEDERAL CONTRACTORS

Seeking to gain a stronger understanding of FISMA compliance & certification for your organization and need comprehensive answers to questions regarding the Federal Information Security Management Act of 2002, which was subsequently amended in 2014, and now known as the Federal Information Security “Modernization Act”. Then turn to the experts at FLANK, a leading provider of FISMA compliance assessments for federal contractors. Becoming FISMA compliant can be a complex, lengthy, and challenging endeavor for many organizations, due largely to misconceptions and misleading information as to what the compliance process entails.

While FISMA compliance & certification is not an overnight process, it can be achieved in an efficient manner, provided federal contractors have a clear understanding of the road ahead, deliverables required, and the milestones to be met. Additionally, obtaining high-quality, industry leading FISMA policies and procedures - those mapped directly to NIST SP 800-53 - will save federal contractors thousands of dollars, so visit flank.org to learn more about our FISMA toolkits and policy templates.

Use our FISMA compliance & certification overview in getting your organization ready for tackling the FISMA mandates.
UNDERSTAND THE ORIGINS OF FISMA COMPLIANCE AND CERTIFICATION

The Federal Information Security Management Act (FISMA) was passed as Title III of the E-Government Act (Public Law 107-347) in December 2002. It effectively required 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. It signified the federal government’s sincere efforts to modernize, strengthen, and create a comprehensive information security framework for federal contractors, one that still exists to this day, thanks to the continued adoption and implementation of FISMA.

Fast-forward to 2014, and FISMA was effectively amended and slightly renamed; now known as the “Federal Information Security Modernization Act (FISMA) of 2014.

While FISMA compliance & certification initially began as a somewhat cumbersome process, it has gained widespread acceptance throughout federal agencies, which in turn has created a ripple effect to include thousands of federal contractors providing critical services to federal information systems. In a world where outsourcing continues to grow at unprecedented rates, especially with the federal government who relies on contractors all throughout the country, FISMA compliance & certification has steadily become a strict mandate for such entities. As a result, more and more federal contractors are now finding themselves caught in the ever-growing and widening FISMA net cast by federal agencies.
UNDERSTAND THE IMPORTANCE OF NIST REGARDING FISMA COMPLIANCE & CERTIFICATION:

The National Institute of Standards and Technology (NIST) has been deeply involved with FISMA since it became law, with NIST chiefly responsible for developing information security standards (Federal Information Processing Standards - FIPS) and guidelines (Special Publications in the 800-series - SP 800), while also assigning NIST specific responsibilities, such as the development of the following: (1). Standards to be used for categorizing information systems. (2). Guidelines and recommendations relating to information systems in each respective category. (3). Minimum information security requirements for each respective category.

GET TO KNOW NIST SP 800-53

Becoming FISMA compliant ultimately means adhering to the stated security controls found within the most current version of NIST Special Publication (SP) 800-53, which as of this writing (February, 2018), is NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, Revision 4. Depending on the impact assessment assigned, which can be either LOW, MODERATE, or HIGH, the number of security controls to comply with can be enormous indeed. Note: Revision 5 Draft is now available for review.

It’s important to note that in recent years, two (2) emerging standards have risen to the top in terms of global acceptance and recognition - ISO 27002 and NIST SP 800-53. ISO 27001/27002 continues to be a widely used standard throughout the EU and other regions around the world, while NIST SP 800-53 has slowly, but surely, become the standard bearer in North America in terms of InfoSec frameworks.
THERE ARE NUMEROUS NIST SP DOCUMENTS ESSENTIAL FOR FISMA COMPLIANCE

While NIST SP 800-53 is the primary publication for facilitating FISMA compliance, numerous other 800 series “Special Publication” materials play a significant role also. As information security continues to evolve, NIST in turn has developed various SP documents that reflect the growing changes and security threats facing businesses today. Here’s a small list of notable SP 800 documents that are often incorporated into an organization’s overall FISMA efforts. Look upon the material as helpful publications that provide guidance, clarity, and best practices when aiming for FISMA compliance & certification.

- NIST SP 800-30: Guide for Conducting Risk Assessments, (Revision 1, September, 2012)

CONTACT US TODAY AT FISMA@FLANK.ORG TO LEARN MORE.
FISMA COMPLIANCE & CERTIFICATION IS A PROCESS, NOT A PAPERWORK EXERCISE

While documentation (see below) in the form of information security policies and procedures is absolutely critical, FISMA compliance & certification also requires a structured process, for which federal contractors should be fully aware of the following:

CRITICAL INITIATIVES MUST BE IMPLEMENTED

Do you have a security awareness training program in place? How about performing an annual risk assessment of organizational threats and other related risk factors? Have you developed, assessed, and tested a formalized incident response program? Herein lies the critical initiatives that must be implemented for FISMA compliance & certification - in essence - the numerous operational initiatives that require careful planning and orchestration among key personnel within one’s business.

As with most federal compliance programs, especially FISMA, businesses instinctively focus on the information security requirements - and understandably so - as there are literally dozens of InfoSec areas to comply with. However, don’t neglect the core operational (i.e., non-technical/non-security) requirements as put forth in NIST SP 800-53.

- NIST SP 800-53A: Security and Privacy Controls for Federal Information Systems and Organizations (Revision 4, January 22, 2015)
- NIST SP 800-53: Security and Privacy Controls for Information Systems and Organizations (Revision 5, August, 2017)
- SP 800-137: Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations (Sep 2011)
POLICIES AND PROCEDURES ARE ABSOLUTELY CRITICAL FOR FISMA COMPLIANCE & CERTIFICATION

Without question, one of the most demanding, time-consuming, and challenging aspects of becoming FISMA compliant is developing all the required information security and operational policies and procedures as illustrated in the NIST SP 800-53 publication. Remember that 800-53 is the authoritative publication for assessing FISMA compliance & certification, and it’s an incredibly detailed in terms of information security. With eighteen (18) individual controls to comply with – many of them quite technical – the need for InfoSec policies that map to each of these stated controls is an absolute mandate.

But who has time to spend endless hours authoring FISMA policies and procedures? Even if your organization has information security policies currently in place, can they honestly stand up to the rigorous criteria of NIST SP 800-53? Additionally, when is the last time any real effort was made in reviewing and enhancing your InfoSec policies? The lack of documentation is often the main reason why federal contractors fall behind on FISMA compliance, and it’s why FLANK has developed a comprehensive set of FISMA/NIST SP 800-53 Policy Toolkits and other supporting materials.

From FISMA compliance & certification to DFARS NIST 800-171, and more, we offer a wide-variety of policy toolkits for helping federal contractors develop all required policy documentation, ultimately saving businesses thousands of dollars. Visit flank.org today to learn more about our compliance toolkits.

POLICIES ARE MEANINGLESS WITHOUT ENFORCEMENT

Anyone can author high-quality, well-written InfoSec policies for FISMA compliance & certification, but if there’s no enforcement measures in place, what good are they? Specifically, personnel need to be aware of an organization’s information security framework, what actions they can perform, what the consequences are for non-compliance with the policies, and more.
After all, there’s a reason why all of today’s federal compliance programs require InfoSec policies and procedures; that’s because contractors need well-written guidelines for all employees regarding the use, application, and interaction of an organization’s security operations. In a world with no policy documentation, enforcement of information security best practices is nearly impossible.

TECHNICAL TOOLS AND SECURITY SOFTWARE ARE ESSENTIAL

As with FISMA policies and procedures, implementing all necessary security tools can also be an incredibly time-consuming, challenging, and expensive endeavor. Buried within the eighteen (18) controls of the NIST SP 800-53 publication are strict requirements for a wide-range of security protocols, such as the implantation of two-factor authentication, File Integrity Monitoring, vulnerability scanning, Intrusion Detection Systems (IDS), encryption, and much more.

More specifically, here’s an in-depth list and discussion regarding required – or, at the very least – highly recommended tools and security feature necessary for FISMA compliance & certification:

- Two-Factor/Multi-Factor Authentication (2FA): Have users that need to access your network either remotely, or have privileged access, regardless if they are remote or not? If so, then you need to put in place a two-factor authentication (2FA) utility. Luckily, there’s dozens to choose from, are relatively inexpensive, and also not too terribly challenging in terms of implementation.

- Just remember that the 2FA solution needs to meet two of the following three conditions: (1). Something you know. (2). Something you have. (3). Something you are.
File Integrity Monitoring: Knowing the “who, what, when, where, and why” when it comes to accessing, viewing, modifying/changing files is essential in today’s InfoSec world, and its why businesses use File Integrity Monitoring (FIM). File Integrity “checkers”, as stated in NIST SP 800-53, is essential for FISMA compliance & certification.

Log Collection, Parsing, and Analysis: Setting baseline parameters regarding the collection, capture, and recording of specific events, is a requirement for FISMA compliance & certification. More specifically, the Audit and Accountability control within NIST SP 800-53 provides detailed information on the various auditing events that should be captured and recorded. The Environmental Protection Agency (EPA) offers a great example when it comes to the various auditing events that should be captured for network devices, operating systems, applications, and more. Download the pdf at: https://www.epa.gov/sites/production/files/2015-10/documents/cio-2150-p-03.2.pdf

Vulnerability Scanning: Performing vulnerability scans is essential for determining what weaknesses and other security related threats possibly exist within your environment. Generally speaking, vulnerability scans are performed both internally and externally on information systems as a best practice. There are a large number of vendors offering scanning solutions, so choose wisely.

Fortunately, many of these security features are available from a large number of cybersecurity vendors offering threat detection and prevention solutions that collect and analyze data, and more. The challenge, however, is two-fold: First, mining through the endless vendors offering such tools can be an exhausting experience. Second, the costs to acquire and implement these solutions can be operationally taxing. Fortunately, FLANK offers assistance in choosing the right vendor as we have years of experience working with dozens of security providers.

We’ve seen almost every tool on the marketplace - what works, what doesn’t, who has the best tools for a specific industry and/or environment - and this allows us to provide expert, objective recommendations on the best tools for businesses to deploy. It’s just one of the many services we provide for FISMA compliance & certification for federal contractors throughout North America. Visit flank.org to learn more about us.
UNDERSTAND THE “CERTIFICATION & ACCREDITATION PROCESS” AND THE NEW “ASSESSMENT & AUTHORIZATION” (C&A) PROCESS

NIST Special Publication 800-37, “Guide for the Security Certification and Accreditation (C&A) of Federal Information Systems,” published in May, 2004 (which is out of print and can be hard to locate online because it’s been “retired” and replaced by a newer version) provided a relatively simple and straightforward process for becoming FISMA compliant. It’s still useful, however, as it helps better understand the entire process, particularly in regards to C&A. Specifically, the following four (4) phases were required for certifying and accrediting a federal information system:

- **Initiation Phase:** This phase contains essentially three core tasks, which are (1) preparation; (2) notification and relevant resource identification; along with (3) an analysis of the System Security Plan (SSP), its update, and overall acceptance. The purpose of the initiation phase is to ensure that the authorizing official and senior agency information security officer are in general agreement with the information contained in the SSP, including the system’s security requirements, before the certification agent starts the assessment of the security controls within the defined information system.

- **Security Certification Phase:** This phase consists of two core tasks, which are (1) security control assessment; and (2) security certification documentation. More specifically, the Security Certification phase assesses the overall security controls, as to their implementation and operation, the desired outcome with respect to meeting the security requirements for the system. This phase also addresses specific initiatives to implement for correcting control gaps, weaknesses, and deficiencies in the security controls, thus reducing and hoping to eliminate known vulnerabilities in the information system. This phase often requires the most time and work, as a combination of technical, security, and operational remediation has to be performed.

- From authoring FISMA policies and procedures to implementing security tools - such as two-factor authentication, vulnerability scanning, audit logs and trails, and more - the Security Certification phase can be challenging.
**Security Accreditation Phase:** This phase consists of two tasks, which are (1) security accreditation decision, and (2) security accreditation documentation. The purpose of this phase is to determine if the remaining known vulnerabilities in the information system still pose an acceptable level of risk to agency operations, agency assets, or individuals. Following the successful completion of this phase, the information system owner will have (1) authorization to operate the information system, (2) an interim authorization to operate the information system under specific terms and conditions, (3) denial of authorization to operate the information system.

**Continuous Monitoring Phase:** Once the controls are in place for FISMA compliance, organizations will still need to proactively monitor them on a regular basis. Ultimately, this means putting in place a process for regularly inspecting, assessing, changing - and enhancing - one’s internal controls.

**LEARN ABOUT THE NEW AND IMPROVED RISK MANAGEMENT**

While the above-referenced historical four (4) phase C&A process is still in use in terms of the various deliverables that must be developed for meeting FISMA compliance, the “new and improved” risk management process within NIST SP 800-37, “changes the traditional focus of C&A as a static, procedural activity to a more dynamic approach that provides the capability to more effectively manage information system-related security risks in highly diverse environments of complex and sophisticated cyber threats, ever-increasing system vulnerabilities, and rapidly changing missions.”

Simply stated, the risk management process for facilitating FISMA compliance is now more flexible, adaptable, and takes into account the evolving changes - and threats - of today’s information security and cybersecurity landscape.

Yes, you still have to produce the various documents and associated deliverables as discussed in the initial four (4) phase approach for C&A, it’s just that the road journeyed down for such a process is slightly different now. Specifically, the six (6) step risk management process (http://bit.ly/2xqZL9n) consists of the following:
Step 1: Categorize Information Systems: Step 1 essentially requires organizations to determine the criticality and sensitivity of the information being processed, stored, and transmitted by an information system.

Step 2: Select Security Controls: Step 2 requires organizations to select an initial set of baseline security controls for the information system based on the security categorization, ultimately tailoring and supplementing the security control baseline as needed based on risks to one’s organization.

Step 3: Implement Security Controls: Step 3 requires organizations to actually implement the security controls and describe how the controls are employed within the information system and its environment of operation.

Step 4: Assess Security Controls: Step 4 requires organizations to actually assess the security controls using appropriate assessment procedures to determine if the controls are in place and operating effectively as required and in accordance with organizational mandates and required NIST SP 80-53 guidelines.

Step 5: Authorize Information System: Step 5 requires the organization to prepare, and submit relevant documentation for allowing the information system to be authorized for use.

Step 6: Monitor Security Controls: Step 6 requires organizations to monitor their control environment, a practice more commonly known as “Continuous Monitoring” where policies, procedures and processes are in place for assessing, monitoring, and enhancing controls.

This publication, developed by the Joint Task Force Transformation Initiative Working Group, transforms the traditional Certification and Accreditation (C&A) process into the six-step Risk Management Framework (RMF).
GET ACQUAINTED WITH ESSENTIAL FISMA TERMINOLOGY

⭕ Security Plan/System Security Plan (SSP): According to the National Institute of Standards and Technology (NIST), a System Security Plan (SSP) is a document that provides an overview of the security requirements of the system and describe the controls in place or planned, for meeting those requirements. The SSP also delineates responsibilities and expected behavior of all individuals who access the system. The SSP should be viewed as documentation of the structured process of planning adequate, cost-effective security protection for a system.

⭕ Security Assessment Report (SAR): The Security Assessment Report (SAR) essentially contains the results of the security tests and evaluations of an organization’s information system. The SAR, and the results documented within it, supports program goals, efforts, and activities necessary for achieving compliance with organizational security requirements within a stated NIST framework and/or publication. The SAR describes the risks associated with the vulnerabilities identified during a security assessment and can also serve as the risk summary report as referenced in NIST SP 800-37 Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems.

⭕ Plan of Action and Milestones (POAM): A document that identifies critical tasks and related deliverables that need to be accomplished for ultimately ensuring full and complete compliance with a stated framework or publication. Thus, the POAM details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.

⭕ Authorization to Operate (ATO): The official management decision given by a senior organizational official to authorize operation of an information system and to therefore accept the relevant risk(s) to organizational operations (such as mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the nation based on the implementation of an agreed-upon set of security controls.
Risk management: The process of managing risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system, and includes: (i) the conduct of a risk assessment; (ii) the implementation of a risk mitigation strategy; and (iii) employment of techniques and procedures for the continuous monitoring of the security state of the information system.

Risk Assessment: The process of identifying risks to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation, arising through the operation of an information system. Part of risk management, incorporates threat and vulnerability analyses and considers mitigations provided by security controls planned or in place.

Security Authorization: The official management decision given by a senior organizational official for purposes of authorizing an operation of an information system and to also fully accept the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security controls.

Security Control: The management, operational, and technical controls (i.e., policies, procedures, processes, and safeguards or countermeasures) relating to an information system to protect the confidentiality, integrity, and availability of the system and its information.

System Development Life Cycle: A process for planning, creating, testing, and deploying an information system. The SDLC concept applies to a wide-range of hardware and software configurations, as a system can be composed of hardware only, software only, or a combination of both.

Risk Management Framework: The Risk Management Framework from the National Institute of Standards and Technology (NIST) is a comprehensive process that essentially integrates security and risk management policies, procedures, and processes into the system development life cycle for an organization.
Security Categorization: The process of determining the security category for information or an information system.


Common Control: A security control that is essentially inherited by one or more organizational information systems.

Information System Owner: Person or persons essentially responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system.

Common Control Provider: The person or persons responsible for the development, implementation, assessment, and monitoring of the actual common controls (i.e., security controls inherited by information systems).

LEARN ABOUT THE “SECURITY AUTHORIZATION PACKAGE”

The Security Assessment Report (SAR) is one of three key documents in the security authorization package. This is essentially a report produced “after” an official assessment is conducted by a qualified auditor. The SAR contains the formal findings of the assessment.

The Plan of Action and Milestones (POAM), prepared for the authorizing official by the information system owner or the common control provider, is second of three key documents in the security authorization package and describes the specific tasks that are planned. The POAM is essentially used to document remediation and the related next steps an organization is to take for correcting any noted gaps or deficiencies within their control environment.

And the Security Plan, more commonly known as the System Security Plan - or simply the “SSP” is a document that provides an overview of the security requirements of the system and describe the controls in place or planned, for meeting those requirements. The System Security Plan also delineates responsibilities and expected behavior of all individuals who access the system.
The System Security Plan should be viewed as documentation of the structured process of planning adequate, cost-effective security protection for a system. It should reflect input from various managers with responsibilities concerning the system, including information owners, the system operator, and the system security manager.

The security authorization package thus contains the following: (1). The Security Assessment Report (SAR); and the (2). Plan of Action and Milestones, commonly known as the POAM. (3). The Security Plan, again, more commonly known as the System Security Plan (SSP). The information in these three key documents is used by authorizing officials to make risk-based authorization decisions.

FISMA WAS AMENDED IN 2014, AND HERE’S WHAT YOU NEED TO KNOW

FISMA was amended in 2014, and is known officially known as the Federal Information Security Modernization Act of 2014. While the update provides several modifications to FISMA for helping enhance and clarify Federal security practices to current threats, the changes primarily affect federal agencies themselves. Specifically, FISMA compliance requires the following:

- Emphasizes the authority of the Director of the Office of Management and Budget (OMB) with oversight, while authorizing the Secretary of the Department of Homeland Security (DHS) to administer the implementation of security policies and practices for Federal Information Systems.

- Federal agency reporting requirements are to now include specific information about threats, security incidents, and compliance with security requirements. Furthermore, it also requires the OMB Director, in consultation with the Secretary of DHS, to report to Congress on an annual basis the “effectiveness of [federal agency] information security policies and practices”. Requires agencies to notify Congress of major security incidents.

- Federal agencies are to provide notice to Congress “expeditiously”, but no later than 30 days after the date for which an agency discovers a breach.
Within one year of the enactment of FISMA, the OMB Director, is required to revise Budget Circular A-130 to eliminate inefficient or wasteful reporting.

As a federal contractor, how do these changes affect you? Many of them are administrative in nature and have a minimal impact for federal contractors, but more important is what remains the same, and that’s the overall intent of FISMA. You still need to develop a mature control environment with adequate security, technical and operational controls. You still need to develop comprehensive information security policies and procedures, those that align with NIST SP 800-53. You still need to conduct continuous monitoring/continuous compliance activities for maintaining your FISMA requirements. In short, FISMA is still FISMA.

CONTINUOUS MONITORING IS ESSENTIAL FOR FISMA COMPLIANCE & CERTIFICATION

While an Authorization to Operate (ATO) is essentially granted every three (3) years, that doesn’t remove the fact that federal contractors have to engage in continuous monitoring initiatives for ensuring FISMA compliance is maintained annually. What is “Continuous Monitoring” - it’s the efforts an organization must implement for regularly reviewing, assessing, and making changes to one’s control environment for ensuring the core tenants of FISMA - and ultimately the security controls within NIST SP 800-53 - are being upheld. Anyone can claim FISMA compliance & certification for a “point-in-time”, but the real challenge of adhering to FISMA is the Continuous Monitoring initiatives that must be practiced.

FLANK offers a comprehensive, easy-to-use, and implement Continuous Monitoring program, so contact us today at FISMA@flank.org to learn more.

WHY FLANK FOR FISMA COMPLIANCE & CERTIFICATION?

FLANK offer numerous solutions for helping federal contractors become FISMA compliant - that’s why! Need documentation, such as FISMA specific information security policies and procedures developed in accordance with NIST SP 800-3? We have them. Need assistance in remediating technical and operational controls? We can do that also. From planning your FISMA compliance & certification initial activities to authoring the System Security Plan (SSP), Security Assessment Report (SAR), Plan of Action and Milestones (POAM), FLANK can assist every step of the way.
Federal agencies have become very aggressive in demanding FISMA compliance for contractors they outsource to, so don’t be surprised if the FISMA compliance & certification regulatory requirement comes calling. Be ready. Talk to FLANK today.

**FISMA ALL-IN-ONE TOOLKIT AVAILABLE FOR DOWNLOAD**

Becoming compliant with FISMA and the NIST SP 800-53 controls is often an expensive and time-consuming process, but thanks to FLANK’s world-class leading FISMA Compliance All-in-One Toolkit, you’ve got all the tools, templates, and other supporting documentation for helping ensure rapid compliance with the Federal Information Security Modernization Act (FISMA).

Available for instant download, you’ll receive professionally developed NIST SP 800-53 specific information security policies, procedures, forms, checklists, templates, scoping & readiness documents, and more that map directly to all three levels of categorization of controls in accordance with NIST SP 800-53 (LOW, MOD, HIGH).

Available for instant download, the FISMA Compliance All-in-One Toolkit comes complete with the following 7 sections:

- NIST SP 800-53 Information Security Policies and Procedures Packet
- NIST SP 800-53 Policy Packet
- FISMA System Security Plan (SSP) Template
- FISMA Scoping & Readiness Assessment Templates
- Cyber Incident Response and Reporting Program
- Third-Party Due-Diligence & Vendor Management Program
- Risk Management & Risk Assessment Program

**CONTACT US TODAY AT FISMA@FLANK.ORG TO LEARN MORE.**
ABOUT US

We’re global experts when it comes to security, governance, and compliance solutions, there’s no debating that, and we can help you implement efficient and scalable solutions for your growing business. Security can be difficult, compliance can be challenging, and governance can be costly - we more than understand these issues - and it’s why you should be talking to Flank, the organization that helps you in “protecting your perimeter”.

WE’RE FLANK. “TO DEFEND OR GUARD AT THE FLANK”.

REFERENCES:

https://csrc.nist.gov/publications/final-pubs
https://www.nist.gov/itl