VERACODE

White Paper

Understanding NIST 800-37 FISMA Requirements

Contents

Overview

The Federal Information Security Management Act of 2002 ("FISMA", 44 U.S.C. § 3541, et seq.) is a United States federal law enacted in 2002 as Title III of the E-Government Act of 2002 (Pub.L. 107-347, 116 Stat. 2899). The Act is meant to bolster computer and network security within the Federal Government and affiliated parties (such as government contractors) by mandating information security controls and periodic audits.

I. The Role of NIST in FISMA Compliance

The National Institute of Standards and Technology (NIST) is chartered with developing and issuing standards, guidelines, and other publications which federal agencies must follow to implement FISMA and manage cost-effective programs to protect their information and information systems. NIST Special Publications (SP) 800-series combined with NIST's FIPS 199 and FIPS 200 create the risk-based framework which federal agencies use to assess, select, monitor and document security controls for their information systems.

NIST standards and guidelines are organized as follows:

- **Federal Information Processing Standards (FIPS)** are developed by NIST in accordance with FISMA. FIPS are approved by the Secretary of Commerce and are compulsory and binding for federal agencies. Since FISMA requires that federal agencies comply with these standards, agencies may not waive their use.

- **Guidance documents and recommendations** are issued in the NIST Special Publication (SP) 800-series. Office of Management and Budget (OMB) policies (including OMB Memorandum M-06-20, FY 2006 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management) state that for other than national security programs and systems, agencies must follow NIST guidance.1

- **Other security-related publications**, including interagency and internal reports (NISTIRs), and ITL Bulletins, provide technical and other information about NIST's activities. These publications are mandatory only when so specified by OMB.

II. NIST Risk Management Framework for FISMA

NIST has created a set of standards and guides which create a Risk Management Framework for agencies to manage organizational risk in accordance with FISMA requirements. This framework sets forth an approach to security control selection and specification with consideration to effectiveness, efficiency, and constraints. Federal agencies must undertake the following steps to maintain an effective information security program:

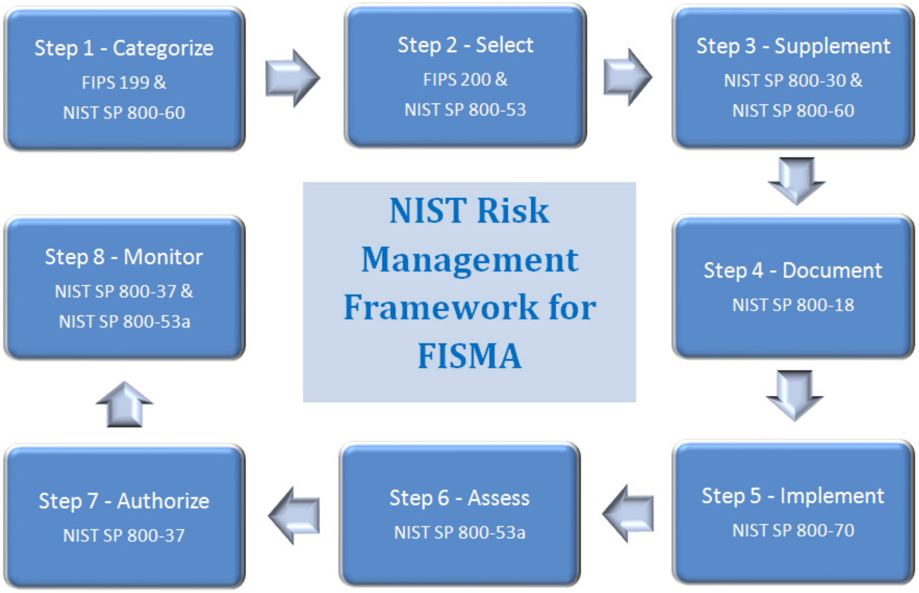


Figure 1 NIST Framework

- **Step 1 -** Define criticality /sensitivity of information system according to potential impact of loss
- **Step 2 -** Select baseline (minimum) security controls to protect the information system; apply tailoring guidance as appropriate
- **Step 3 -** Use risk assessment results to supplement the tailored security control baseline as needed to ensure adequate security and due diligence
- **Step 4 -** Document in the security plan, the security requirements for the information system and the security controls planned or in place
- **Step 5 -** Implement security controls; apply security configuration settings
- **Step 6 -** Determine security control effectiveness (i.e., controls implemented correctly, operating as intended, meeting security requirements)
- **Step 7 -** Determine risk to agency operations, agency assets, or individuals and, if acceptable, authorize information system operation
- **Step 8 -** Continuously track changes to the information system that may affect security controls and reassess control effectiveness

III. Application Security and FISMA

Federal agencies have aggressively moved towards an eGovernment model, adapting and migrating paper-based processes to an internet-based service model. As a result, virtually all federal information activity is controlled by software and universally accessible via web applications. Not surprisingly, attacks are now focused at the application layer, with as much as 75% of all new attacks targeted against software.   As shown in the figure below, the National Vulnerability Database is reporting over 3,400 new software vulnerabilities disclosed in the first half of 2007 alone.

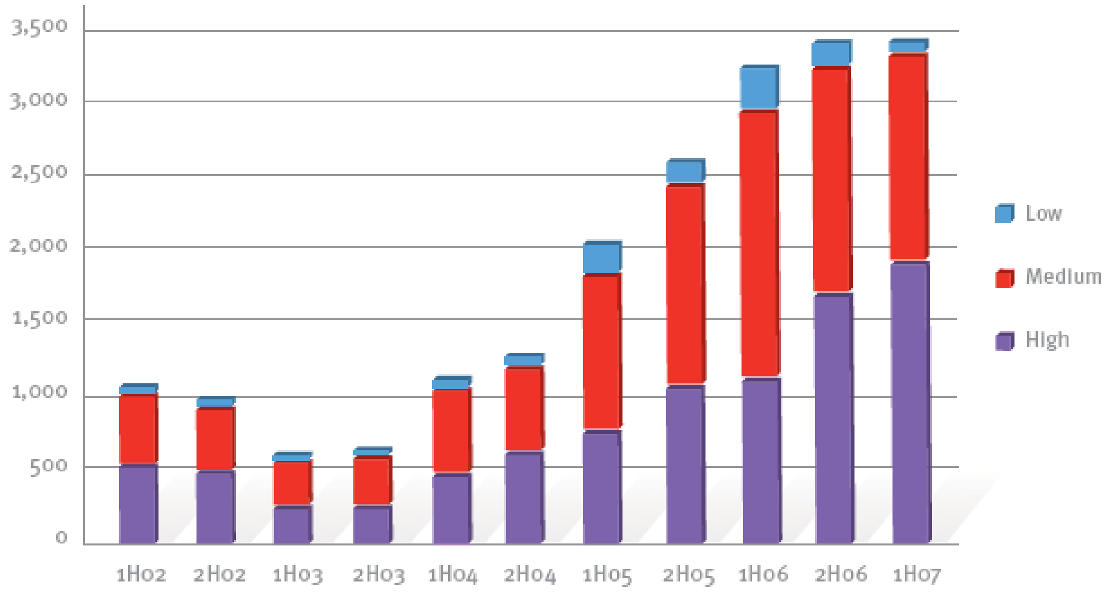


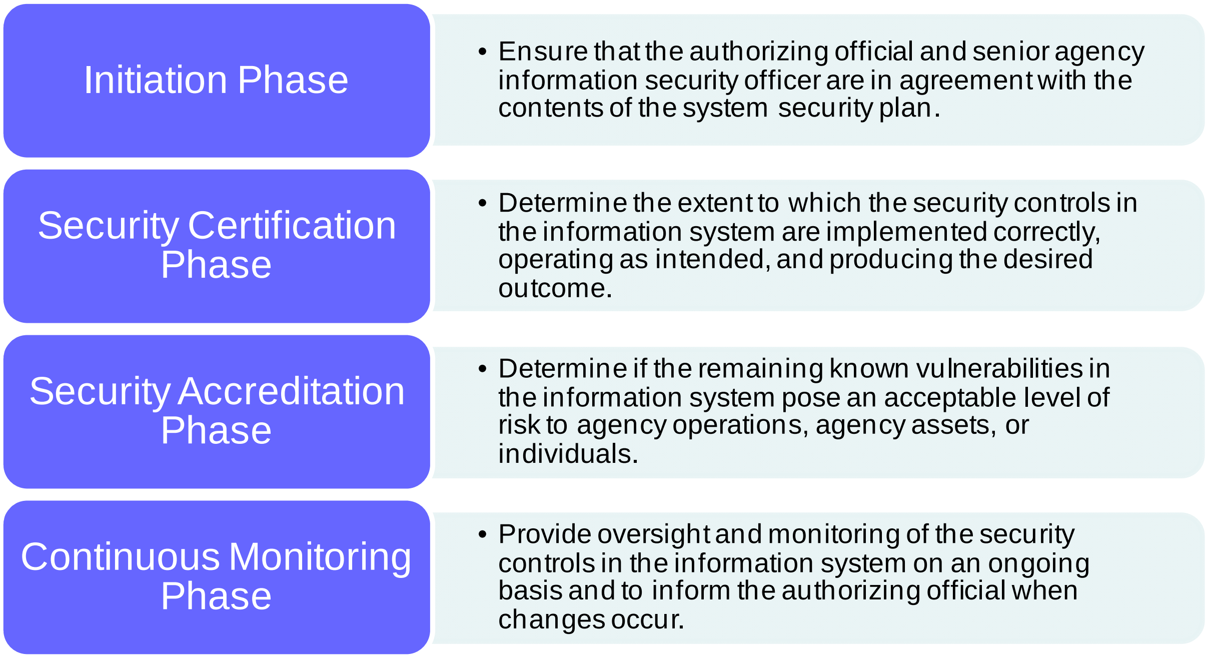
Figure 2 Vulnerabilities by Severity (Source: Microsoft from NVD statistics)

Not only is the number of vulnerabilities increasing, but perhaps the most alarming trend is the rise of “High Severity” vulnerabilities as a percentage of the total. As a result, auditors are looking more closely at controls related to software security and federal agencies must ensure that software applications have been tested for vulnerabilities that may compromise their systems in order to achieve FISMA compliance.

IV. NIST SP 800-37 and FISMA

As part of its FISMA responsibility to develop standards and guidance for federal agencies, NIST created Special Publication (SP) 800-37 “Guide for the Security Certification and Accreditation of Federal Information Systems.” This guide is an integral part of the NIST Risk Management Framework for FISMA and is used by agencies to understand requirements and implement tasks pertaining to the certification, accreditation and continuous monitoring of information systems.

The NIST SP 800-37 certification and accreditation process consists of four distinct phases as shown in Figure 3 below:



Initiation Phase

- Ensure that the authorizing official and senior agency information security officer are in agreement with the contents of the system security plan.

Security Certification Phase

- Determine the extent to which the security controls in the information system are implemented correctly, operating as intended, and producing the desired outcome.

Security Accreditation Phase

- Determine if the remaining known vulnerabilities in the information system pose an acceptable level of risk to agency operations, agency assets, or individuals.

Continuous Monitoring Phase

- Provide oversight and monitoring of the security controls in the information system on an ongoing basis and to inform the authorizing official when changes occur.

Figure 3 NIST SP 800-37 Phases

Once there is agreement on the contents of the system security plan during the initiation phase, the certification agent can begin the assessment of the security controls in the information system. The certification agent is an individual, group, or organization responsible for conducting a security certification, or comprehensive assessment of the information system and to ensure the creditability of the assessment result should be an outside expert that is independent from the persons directly responsible for the development, implementation and management of the information system.

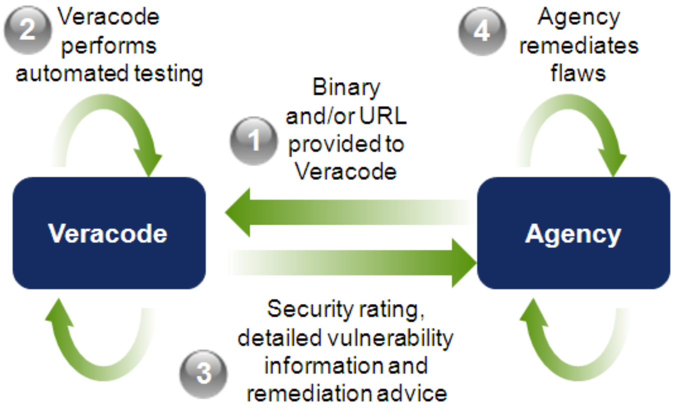
However, security certification does not include the determination of risk to the agency. It is the security accreditation phase where the senior management of the agency reviews the findings of the security certification and assesses the risk posed to agency operations, agency assets, or individuals to make a decision if the system should be accredited. By accrediting an information system, an agency official accepts responsibility for the security of the system and is fully accountable for any adverse impacts to the agency if a breach of security occurs.

V. How Veracode Can Help

To help address the needs of federal agencies to assess their application security risks for FISMA compliance, Veracode has designed the first complete, automated application security testing service that incorporates multiple vulnerability scanning technologies in an integrated on-demand model. Based on its centralized on-demand platform, Veracode can deliver results in a matter of hours across the entire agency without the need to purchase any hardware, software or hire additional consultants.

How Veracode's SecurityReview Works

As an easy-to-use on-demand service, all Veracode requires from the agency to scan software applications is either a URL of the web application, the application binary for internally developed software or the vendor contact for third-parties that provided software to the agency. Since Veracode's on-demand service is based on web scanning and binary analysis, no source code is required to conduct the testing. Results to the agency are available in as quickly as 24 to 72 hours, providing detailed vulnerability reports which are used to provide documentation and evidence for the agency's information security program.


2 Veracode performs automated testing
4 Agency remediates flaws
1 Binary and/or URL provided to Veracode
Veracode
Agency
3 Security rating, detailed vulnerability information and remediation advice

Independent Review with Standards-Based Ratings

As an expert in application security, Veracode is in a unique position to provide an independent assessment and standards-based rating to ensure your applications comply with FISMA rules. Auditors require proof that your applications are free from vulnerabilities and they need a method to evaluate findings against a well-known industry benchmark. Veracode's Ratings System solves this issue by producing a software security rating based on respected government standards including NIST for definitions of assurance levels, MITRE's Common Weakness Enumeration (CWE) for classification of software weaknesses and FIRST's Common Vulnerability Scoring System (CVSS) for severity and ease of exploitability. These universally accepted vulnerability scoring methods provide auditors confidence that you have effective security controls in place.

VI. NIST SP 800-37 Tasks & Veracode Solutions

NIST has divided the four phases of SP 800-37 into a series of ten tasks which agencies use to streamline their certification and accreditation processes and comply with FISMA. While these tasks are applicable to all aspects of information security, Veracode's application security testing provides independent testing which can be used as evidence and documentation to support a variety of NIST SP 800-37 activities. The following table provides guidance on how Veracode can be used to support tasks identified by NIST SP 800-37:

NIST 800-37 Task	Description	Veracode Solution
Task 1: Preparation		
Task 1.3 Threat Identification	Confirm that potential threats that could exploit information system flaws or weaknesses have been identified and documented in the system security plan, risk assessment, or an equivalent document.	Veracode's application security testing can be used to identify threats in the agency's application inventory which could affect the confidentiality, integrity or availability of the system.
Task 1.4 Vulnerability Identification	Confirm that flaws or weaknesses in the information system that could be exploited by potential threat sources have been identified and documented in the system security plan, risk assessment, or an equivalent document.	Per NIST's recommendation, Veracode provides an "automated scanning" solution to identify vulnerabilities in software.
Task 1.6 Initial Risk Determination	Confirm that the risk to agency operations, agency assets, or individuals has been determined and documented in the system security plan, risk assessment, or an equivalent document.	Veracode can identify "vulnerabilities resulting from the absence of security" within software applications.
Task 4: Security Control Assessment		
Task 4.1 Documentation and Supporting Materials	Assemble any documentation and supporting materials necessary for the assessment of the security controls in the information system; if these documents include previous assessments of security controls, review the findings, results, and	The application security report provided by Veracode can be used as part of the documentation and supporting materials during the security control assessment.

NIST 800-37 Task	Description	Veracode Solution
	evidence.	
Task 4.2 Methods and Procedures	Select, or develop when needed, appropriate methods and procedures to assess the information system.	Veracode's application security testing can be used to provide an automated method and procedure for software assessments.
Task 4.3 Security Assessment	Assess the management, operational and technical security controls in the information system using methods and procedures selected or developed.	Veracode's automated application security testing provides a method and procedure for assessing the technical security controls around software applications.
Task 4.4 Security Assessment Report	Prepare the final security assessment report.	Veracode's application security report can be provided as supporting evidence as part of the final report.
Task 5: Security Certification Documentation		
Task 5.1: Findings and Recommendations	Provide the information system owner with the security assessment report.	Veracode's application security report can be provided as supporting evidence as part of the findings and recommendations.
Task 5.3: Plan of Action and Milestones Preparation	Prepare the plan of action and milestones based on the results of the security assessment.	Veracode provides agencies with a recommended remediation plan with milestones for improving the security of the evaluated software.
Task 8: Configuration Management and Control		
Task 8.2: Security Impact Analysis	Analyze the proposed or actual changes to the information system (including hardware, software, firmware, and surrounding environment) to determine the security impact of such changes.	Veracode enables applications to be tested for security vulnerabilities prior to deployment as part of a change control management process.
Task 9: Security Control Monitoring		
Task 9.2: Selected Security Control Assessment	Assess an agreed-upon set of security controls in the information system to	Using Veracode's application security testing, agency's can analyze applications for

NIST 800-37 Task	Description	Veracode Solution
	determine the extent to which the controls are implemented correctly and producing the desired outcome with respect to meeting the security requirements**.**	vulnerabilities to determine if the controls related to securing applications from vulnerabilities are being met.
Task 10: Status Reporting and Documentation		
Task 10.2: Plan of Action and Milestones Update	Update the plan of action and milestones based on the documented changes to the information system (including hardware, software, firmware, and surrounding environment) and the results of the continuous monitoring process.	Veracode provides agencies with a recommended remediation plan with milestones for improving the security of the evaluated software.

Table 1 NIST 800-37 Tasks Mapped to Veracode Solutions

VII. Summary and Conclusions

With 75 % of all new attacks against software and 90 % of all vulnerabilities in software, NIST and FISMA recognize that federal agencies must place a strong emphasis on application security. Federal agencies that wish to improve their overall security along with their FISMA Grade should prepare for the new threats targeted at their applications and prepare themselves well in advance for more stringent requirements by evaluating their software using third-party application security service providers.

About Veracode

Veracode is the world's leader for on-demand application security testing solutions. Veracode SecurityReview is the industry's first solution to use patented binary code analysis and dynamic web analysis to uniquely assess any application security threats, including vulnerabilities such as cross-site scripting (XSS), SQL injection, buffer overflows and malicious code. SecurityReview performs the only complete and independent security audit across any internally developed applications, third-party commercial off-the-shelf software and offshore code without exposing a company's source code. Delivered as an on-demand service, Veracode delivers the simplest and most-cost effective way to implement security best practices, reduce operational cost and achieve regulatory requirements such as PCI compliance without requiring any hardware, software or training.

Veracode has established a position as the market visionary and leader with awards that include recognition as a Gartner "Cool Vendor" 2008, Info Security Product Guide's "Tomorrow's Technology Today Award 2008," Information Security "Readers' Choice Award 2008," AlwaysOn Northeast's "Top 100 Private Company 2008", NetworkWorld "Top 10 Security Company to Watch 2007," and Dark Reading's "Top 10 Hot Security Startups 2007."

Based in Burlington, Mass., Veracode is backed by .406 Ventures, Atlas Venture and Polaris Venture Partners. For more information, visit www.veracode.com.