



WHITE PAPER

FISMA: Making the Grade

An Introduction to the Federal Information Security Management Act



Where it all comes together.™



CONTENTS

+ Executive Overview	3
+ Introduction	3
+ FISMA Requirements	6
+ Options for FISMA Compliance	8
+ The Ideal Security Consulting Organization	9
+ The Case of the Nuclear Regulatory Commission	10



FISMA: Making the Grade

An Introduction to the Federal Information Security Management Act

+ Executive Overview

The Federal Information Security Management Act of 2002 (FISMA) makes permanent many of the new information security management responsibilities introduced by the Government Information Security Reform Act (GISRA), which became law in 2000. FISMA goes further, however, requiring objective assessments of the effectiveness of security controls at least once each year on every information system operated by, or for, the federal government. FISMA requires both an internal evaluation under the direction of the CIO and an independent assessment under the direction of the agency Inspector General. Since 2000, Congress has sought to step up pressure on the heads of agencies to comply with FISMA by collecting assessments and publishing a letter grade for each agency.

Because FISMA specifically addresses senior management responsibility, not technical specifications, technical solutions alone will not be sufficient for agencies to earn good marks on FISMA compliance. Rather, agencies must demonstrate how information security technology fits into the framework of an overall security strategy and budget that is in turn integrated with each agency’s mission and goals. FISMA compliance therefore requires not only new initiatives, but a new perspective from the head of the agency down to the security administrator.

+ Introduction

In the late 20th and early 21st centuries, government agencies had rapidly migrated to transformational, Internet-based communication systems. While this migration greatly improved performance and increasingly facilitated tighter coordination among disparate agencies, the resulting highly “open” nature of the current, federal computing environment also presented a new category of risk as threats to federal systems become more varied and sophisticated.

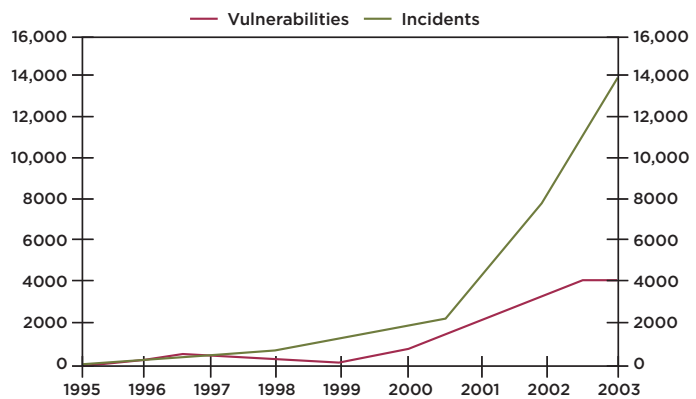


Figure 1
Growth in Reported Computer Security Events and Vulnerabilities¹

¹ The CERT Coordination Center (CERT/CC), Carnegie Mellon University, www.cert.org.

Agencies have employed firewalls, network-based anti-virus software, access management, email gateways, intrusion detection systems (IDS), and other technical provisions to mitigate this risk, but because of the highly unpredictable nature of such attacks—and ever-emerging, new threats—organizations must also employ comprehensive monitoring and analysis of network activity in order to respond selectively to each specific instance; no longer will a single, unattended firewall be flexible and intelligent enough to repel the number and variety of today's network intrusion attempts.

In 2002, in response to these widespread changes in the information security environment and the belief that agencies made only limited progress addressing the issues under GISRA, FISMA was signed into law. FISMA was designed to raise awareness among heads of government agencies as to the nature of the contemporary information security environment and to facilitate the development of effective security programs through the establishment of a comprehensive reporting and evaluation structure.

Central to FISMA requirements is a set of annual reports, including evaluations of the effectiveness of information security programs, from the CIO and the head of each agency to The Office of Management and Budget (OMB) and Congress. It is crucial, therefore, not only for Chief Information Security Officers (CISOs) to understand FISMA requirements, but for the head of each agency to understand these requirements as well. FISMA necessitates not only the implementation of specific security provisions, but the development of concerted, coordinated strategies for intelligently analyzing security threats and responding appropriately to each one. Technology solutions that significantly boost the score for an agency during a given year might not score as well in the following year, if the agency fails to justify how the solution fits into the agency's overall information security strategy.

Adding further complexity to the task of developing a comprehensive yet adaptable security program, laws that govern IT are frequently amended. Recently, for example, Reps. Adam Putnam (R-Fla.) and Tom Davis (R-Va.) proposed an amendment to the 1996 Clinger-Cohen Act, which require agencies to protect their IT investments through adherence to guidelines that minimize risk.

In complying with FISMA, therefore, agency heads must not only become familiar with security risk management, they must also take an active role in the oversight of information security policies and practices in their agency, as well as prepare required reports mandated by FISMA.

Many agencies have found it challenging to comply with FISMA, as illustrated in the chart below. However, the chart illustrates that scoring high marks on FISMA compliance is not impossible: the National Science Foundation progressed from a "D-" grade in 2002 to an "A-" grade in 2003, and the Nuclear Regulatory Commission (NRC) earned an "A" in 2003, the highest grade awarded under FISMA to date.

AGENCY	2002	2003
<i>Agency for International Development</i>	<i>F</i>	<i>C-</i>
<i>Agriculture Department</i>	<i>F</i>	<i>F</i>
<i>Commerce Department</i>	<i>D+</i>	<i>C-</i>
<i>Defense Department</i>	<i>F</i>	<i>D</i>
<i>Education Department</i>	<i>D</i>	<i>C+</i>
<i>Energy Department</i>	<i>F</i>	<i>F</i>
<i>Environmental Protection Agency</i>	<i>D-</i>	<i>C</i>
<i>General Services Administration</i>	<i>D</i>	<i>D</i>
<i>Health and Human Services Department</i>	<i>D-</i>	<i>F</i>
<i>Homeland Security Department</i>	<i>N/A</i>	<i>F</i>
<i>Housing and Urban Development Dept.</i>	<i>F</i>	<i>F</i>
<i>Interior Department</i>	<i>F</i>	<i>F</i>
<i>Labor Department</i>	<i>C+</i>	<i>B</i>
<i>NASA</i>	<i>D+</i>	<i>D-</i>
<i>National Science Foundation</i>	<i>D-</i>	<i>A-</i>
<i>Nuclear Regulatory Commission</i>	<i>C</i>	<i>A</i>
<i>Office of Personnel Management</i>	<i>F</i>	<i>D-</i>
<i>Small Business Administration</i>	<i>F</i>	<i>C-</i>
<i>Social Security Administration</i>	<i>B-</i>	<i>B+</i>
<i>State Department</i>	<i>F</i>	<i>F</i>
<i>Transportation Department</i>	<i>F</i>	<i>D+</i>
<i>Treasury Department</i>	<i>F</i>	<i>D</i>
<i>Veterans Affairs Department</i>	<i>F</i>	<i>C</i>

Figure 2

Federal Agencies Graded Under FISMA, 2002-2003²

The poor marks earned by most agencies, however, is cause of some concern. Not only will Congress and the OMB withhold funding from non-compliant agencies, but because FISMA compliance provides a useful benchmark for effective security, and effective security results in higher availability, confidentiality, and integrity of all data, high marks on FISMA compliance is beneficial to running the everyday business of the agency. In the online edition of Federal Computing Week, Rep. Tom Davis, co-author of FISMA, was quoted as saying, “While we’re making progress, it’s important to note that we’re still not at a point where information security is being taken seriously by every agency and department. Clearly, our goal of making computer security a constant management focus has not been met.” (“Government gets ‘D’ on security” in Federal Computing Week, December 9, 2003.)

² House Government Reform Committee’s Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, December 9th, 2003.

The Department of Homeland Security's poor performance can perhaps be explained by the fact that the agency had been in the process of being formed during the time FISMA evaluations took place. Under such conditions, it's difficult to implement widespread changes in a security program at a time when solutions are in development. Other agencies, perhaps, saw FISMA compliance as an afterthought rather than as an integral part of the agency's goals. Many, in all probability, focused too much on individual security technology products rather than overall security strategies.

This paper provides an understanding of both the technical and operational initiatives that are needed to meet this legislation—and to make the grade.

+ FISMA Requirements

In preparing agencies for FISMA compliance, agency heads, in conjunction with CIOs and CISOs, must develop provisions according to eight broad categories:

1. Risk Assessments
2. Policies and Procedures
3. Security Plans
4. Security Awareness Training
5. Annual Security Testing
6. Remediation Procedures
7. Incident Response Procedures
8. Contingency Plans

Risk Assessments

Performing risk assessments is vital (in addition to being required) simply because they allow evaluating parties to determine the degree to which information security provisions are commensurate with the risk they are designed to mitigate. (FISMA requires that assessments be performed at least annually; however, the optimal frequency for a positive overall FISMA evaluation will vary from agency to agency.) Through the course of such assessments, agencies will be called upon to estimate the amount of harm that would be caused by disruption of its services. These risks are the cornerstone for many of the other required activities.

Policies and Procedures

Agencies will be called upon to formulate information security policies and procedures to cost-effectively mitigate the risk uncovered through the assessments described above. FISMA specifically calls for agencies to design policies and procedures that ensure that information security is addressed throughout the lifecycle of an information-technology system, and not simply as a final, quality control procedure performed prior to deployment.

Security Plans

FISMA requires agencies to draft plans which describe security measures that address specific system requirements and comply with policies and procedures. Such plans must take into account the guidelines issued by the National Institute of Standards & Technology (NIST). FISMA specifies that such plans must cover training (of both security professionals and intended users), incident response capabilities, contingency plans, remediation, and system configuration standards.

Security Awareness Training

Under FISMA, all agencies are required to offer ongoing security awareness training to all personnel, including contractors and all other users of the agency's information technology systems. FISMA requires that such training acquaint participants with the risks associated with handling critical data and the responsibilities involved in providing effective security.

Annual Security Testing

FISMA calls for the evaluation of policies, procedures, and practices through annual testing of every information system on the agency's inventory. FISMA requires that these tests be performed as often as necessary, based on the amount of risk such systems are designed to protect, but at least once a year. FISMA further requires that such testing include not only the technical controls of the system, but also management and operational controls.

Remediation Procedures

Agencies are required to track all security deficiencies identified through testing and monitoring and to measure remediation progress and effectiveness for every system regardless of its level of importance.

Incident Response Procedures

FISMA requires each agency to develop or acquire sufficient capability to detect and respond to information security incidents within their agency. This includes the ability to mitigate the risks of attacks in progress. In an effort to foster collaboration and communication in pursuit of the goal of responding pro-actively to threats, FISMA specifies that agencies report all information security attacks to a central federal information security incident center, the US-CERT. This means that agencies must perform constant, vigilant scanning of all systems.

Contingency Plans

FISMA requires every information system on the agency's inventory to be subject to a documented plan containing procedures to ensure continuity of system operations in the event of a failure or system corruption. As part of the operational security controls for the system, such plans must also be tested annually.

10 Questions Agency Managers Should Ask Themselves

1. Is our inventory of computer and network devices complete and up-to-date?
2. Does the inventory include sufficient security configuration information to determine the patch levels and risk profile for each device?
3. Are devices in the inventory prioritized for security purposes?
4. Do we have a reliable process for discovering vulnerabilities, correlating vulnerabilities with the inventory, patching in a timely manner according to inventory priorities, and updating the inventory?
5. Does our agency have a consistent, effective process across the entire agency for assessing information security risk?
6. Are we able to consolidate the results of risk assessments agency-wide to form an overall picture of IT risk?
7. Are we effective in expressing the agency's IT risk in terms that agency leaders can understand and evaluate alongside other agency risks, such as legal, financial, regulatory and environmental risks?
8. Do we have a plan for how to complete the OMB e-Authentication risk assessments on every authenticated transaction in our agency?
9. Do we have adequate contingency plans in place for all critical information systems, and have those responsible for carrying them out demonstrate their understanding of the plans through live testing?
10. Do we have an available computer security incident response capability commensurate with the sensitivity and criticality of our IT systems, and have the practitioners successfully engaged in incident response exercises?

+ Options for FISMA Compliance

In complying with FISMA, agencies may elect to outsource the preparation and reporting of its obligations to a trusted third-party consultancy that focuses on information technology security, or agencies may choose to perform all work themselves. Consultant organizations have the requisite expertise to develop methodologies tailored to agency needs, but the main disadvantage to full outsourcing is that the agency may not gain the experience of developing and exercising the processes needed to evaluate and report on agency security programs. In fact, if management is not involved in the process, an agency is almost certain to fail to comply adequately with FISMA because effecting change at the management level is FISMA's central purpose. Acting in isolation, the consulting organization would have to learn about threats to the agency's mission and the agency's tolerance levels for different types of risk, and to recommend the most advanced cost-effective solutions for mitigating that risk. To proceed on this route, agencies must design and build a security infrastructure from scratch, which requires substantial investments in personnel, technology, tools, and training. For these reasons, a third route, partnering with a security consultancy, would provide the most effective compromise.

FISMA COMPLIANCE SOLUTION OPTIONS	PROS	CONS
<i>"Do-it-yourself"</i>	<ul style="list-style-type: none"> • Agency maintains full control 	<ul style="list-style-type: none"> • Requires substantial investments in networking and monitoring hardware • Time-consuming • Requires specialized security expertise that could require investments in training • Diverts resources from core mission activities
<i>Complete outsourcing to a security consultant</i>	<ul style="list-style-type: none"> • Gain benefits of security infrastructure and expertise • Faster implementation 	<ul style="list-style-type: none"> • Loss of ownership over the ongoing strategy-building process • Lack of management involvement may prevent an agency from adequately complying with FISMA
<i>Partnering with a security consultant</i>	<ul style="list-style-type: none"> • Gain benefits of security infrastructure and expertise • Faster implementation • Ownership over some of the ongoing strategy-building process • Optimize ROI by focusing security resources 	<ul style="list-style-type: none"> • None

+ The Ideal Security Consulting Organization

When partnering with a consulting organization for FISMA compliance, it is important to work with an organization that not only offers robust and in-depth knowledge of hardware and software from a vendor-neutral perspective, but one that also has the expertise to develop a fully-rounded information security strategy and program, in concert with each agency's particular needs and objectives. Specifically, such an organization must also be able to help the agency address each of FISMA's key requirements.

The "Shifting Playing Field" of FISMA Compliance

In addition, the ideal security consultancy will understand the "shifting nature" of FISMA compliance. That is, although an agency might spend the better part of a year addressing certain security provisions, Congress may decide to place a higher value on other aspects of FISMA. Agencies need to stay in close contact with Congress in order to anticipate such changes, and a skilled consultant can help greatly in this area. For this reason, hardware alone will not guarantee a high grade, no matter how full-featured and robust such hardware may be.

VeriSign's Capabilities

VeriSign, Inc. (Nasdaq: VRSN) has substantial expertise securing mission-critical enterprises all across the globe, and has been providing these services for over seven years. VeriSign is entrusted with running the Domain Name System (DNS) servers that allow the world's .com and .net domain names to function properly, ensuring that each Web user arrives at his or her intended Web page, and each email arrives at its intended destination. In this capacity, VeriSign helps securely process over 14 billion DNS lookups a day. In addition, VeriSign has secured over 400,000 business Web sites around the world with digital certificates.

In order to secure highly sensitive data, VeriSign relies on a robust infrastructure of secure, redundant servers, housed at VeriSign's Security Operations Centers (SOCs). Each facility is staffed around-the-clock by security, customer care, and networking specialists and is designed to provide continuous, failsafe operations. Using state-of-the-art equipment, VeriSign monitors all 13 of the world's root DNS servers, and leverages this infrastructure to provide state-of-the-art consulting and managed security services for government agencies. All of VeriSign's services are powered by the company's unique visibility into the world's Internet infrastructure.

VeriSign's SOC's are staffed by Certified Information Systems Security Professionals (CISSPs) who continuously monitor the health, status, and availability of security devices, run vulnerability scans, manage and monitor intrusion detection systems and firewalls, manage and update each client's security devices, and respond to security events. VeriSign correlates security events across devices and across enterprises, using intelligence derived from its operation of critical Internet infrastructure.

In addition, VeriSign's global PKI, the VeriSign Trust Network (VTN), is a globally-recognized and trusted digital authentication infrastructure. The VTN is an elaborate system of interrelated Certificate Authorities, each supported by a comprehensive security program that includes publicly-available security operations plans, best-practice statements, and policies and procedures, all of which are audited annually by KPMG to ensure rigorous enforcement of every aspect of the VTN security program.

+ The Case of the Nuclear Regulatory Commission

In the second quarter of 2002, the NRC scored a “C” rating on FISMA compliance. Compared with the average score of “F” across all agencies during that year, this was a respectable score, but the agency needed to make marked improvements on its security posture to avoid funding impacts or additional negative exposure. For these reasons, the NRC turned to VeriSign.

To assist the NRC, VeriSign’s Global Security Consulting organization methodically broke down the FISMA requirements into actionable, prioritized tasks, and tracked each task until completion. VeriSign sent a senior security consultant with extensive government agency experience to develop guidelines and a template for the entire Certification and Accreditation (C&A) process based on the whole series of NIST 800 standards in concert with NRC’s security policies. Because VeriSign and its consultants have extensive experience in the industry, VeriSign was aware that Congress would critically examine agencies’ incident-response capabilities as part of the FISMA evaluation. VeriSign therefore made sure that NRC became especially strong in this area.

NRC management designated the VeriSign senior security consultant as the senior advisor for security policy and programs within the Office of the CIO and, after a year under his guidance, VeriSign, the NRC, and its IT support contractors successfully executed the C&A process for all the systems within scope.

In the subsequent FISMA reporting period, which included a full audit conducted by the NRC Inspector General’s office in the second quarter of 2003, the House Government Reform Committee’s Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census awarded the NRC with an “A” grade, the highest rating to date of any Federal agency. (Only four agencies scored higher than a “C+” in 2003.) As VeriSign predicted, Congress put particular weight on the NRC’s incident-response capabilities. NRC’s achievement was accomplished through the efforts of multiple individuals across many Program Offices, but VeriSign’s leadership was singled out by the NRC as a significant factor in the overall score.

For more information about VeriSign’s consulting services, please visit www.verisign.com/products-services/security-services/security-consulting/.

Visit us at www.Verisign.com for more information.

©2005 VeriSign, Inc. All rights reserved. VeriSign, the VeriSign logo, “Where it all comes together,” and other trademarks, service marks, and designs are registered or unregistered trademarks of VeriSign and its subsidiaries in the United States and in foreign countries.

01/05