



**FISMA Compliance**  
***A Holistic Approach to FISMA***  
***and Information Security***

Contents
<b>1 Executive Summary</b>
<b>1 FISMA Overview</b>
<b>3 Agency Challenges</b>
<b>4 The IBM ISS Approach To FISMA Compliance</b>
<b>4 Overview</b>
<b>5 The IBM ISS FISMA Compliance Solution</b>
<b>6 Assessment</b>
<b>7 Remediation</b>
<b>8 Audit</b>
<b>9 Summary and Conclusions</b>

**Executive Summary**

Threats and attacks against information systems are on the rise. IBM Internet Security Systems™ (ISS) and other security companies are now identifying more than 150 new viruses, Trojans, bots and vulnerabilities each week. Attacks launched by dangerous adversaries are targeting information systems globally – including U.S. federal systems – to inflict irreparable damage and ultimately threaten the nation’s security. As a result, the Federal Information Security Management Act (FISMA) was passed to ensure the protection of the nation’s critical infrastructure against vulnerabilities that threaten economic and national security. FISMA provides a framework for developing, implementing, monitoring and reporting on an agency’s information security program.

Protecting the nation’s infrastructure, sustaining a secure environment against new threats and complying with complex and evolving regulatory requirements pose many challenges for agencies. While progress has been made in identifying and addressing agency security weaknesses, deficiencies continue to exist in security policy, procedures and practices. Maintaining an effective, compliant environment goes beyond periodic audits, paperwork and reporting. It requires a holistic strategy and approach to improving security posture and compliance.

This whitepaper provides an overview of FISMA legislation and discusses how the IBM ISS strategic approach to developing and maintaining an enterprise-wide security infrastructure best addresses FISMA requirements and continuous security improvements.

**FISMA Overview**

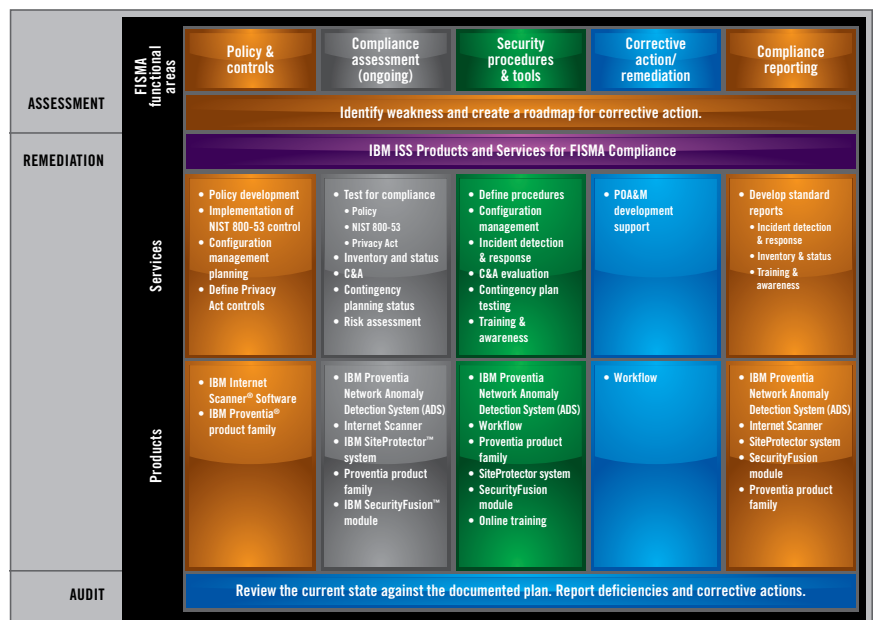
The Federal Information Security Management Act was passed in 2002 as framework to manage risk and ensure the confidentiality, availability and integrity of federal information and information systems. FISMA assigns specific development, management, oversight and reporting responsibilities to two federal agencies, the National Institute of Standards and Technology (NIST) and the Office of Management and Budget (OMB).

## Federal Information Security Management Act (FISMA)

FISMA provides a framework for ensuring the protection of government information, operations and assets. The legislation requires agency officials to implement policies, procedures and practices to strengthen information security and reduce security risks. FISMA compliance requires agencies to:

- *Develop an agency-wide security program*
- *Implement and adhere to security configuration standards developed by NIST*
- *Identify and resolve risks*
- *Perform ongoing assessment and testing*
- *Conduct annual reviews on the effectiveness of the agency's information security and privacy programs and report the results to the OMB annually.*

In order to provide a framework to manage and measure agency security and risk, FISMA tasked NIST with the development of standards and guidelines for selecting, categorizing and assessing information systems. The table below shows the basic NIST framework for FISMA.



## **Agency Challenges**

Information security and FISMA compliance present many challenges to federal agencies, including:

- *Ensuring the integrity of information*
- *Maintaining security against new threats*
- *Balancing the demands of complying with evolving regulations*
- *Planning and testing of security controls and contingency plans*
- *Meeting reporting requirements*
- *Improving FISMA scores*
- *Dealing with constrained resources and budgets*

FISMA requires compliance for all data and information systems that support the agency's operations and assets, including those provided by or managed by other agencies or contractors. As part of the FISMA process, agencies must be able to produce a complete and accurate inventory of all systems including their security status and requirements. This can be a difficult task when systems are spread across many organizations and geographies.

Congress holds agencies accountable to improve their security posture, and therefore links budgetary considerations to agency performance and scoring. 2006 Scorecard results show that progress has been made in developing security policies and procedures, though weaknesses continue to exist in the planning and testing of contingency plans, certifying and accrediting systems and remediation.

Complying with evolving, multi-sourced and complex standards and reporting requirements and maintaining a sound security posture against evolving threats can be a challenge. However, the significance of ensuring security and compliance is substantial. This necessitates the implementation of a proactive security and compliance program that continuously protects, monitors, assesses and collects data across numerous agency divisions and sites.

FISMA solutions based solely on products may improve security and FISMA scoring in a specific area, but do not adequately address agency-wide security needs nor sustain protection against evolving threats. Focusing limited resources on interpreting changing compliance standards and reporting requirements diverts critical attention from managing risk and ensuring protection. Instead, agencies should develop a proactive information security program that integrates quality security policies, processes and supporting technology with business strategy. The program should also support the development of a strategic framework for regulatory compliance and more effectively enable a sustainable security infrastructure. A risk-based framework includes agency-wide security planning, accountability, configuration, implementation and testing, assessment and measurement, remedial action, and a continuous improvement process.

### **The IBM ISS Approach to FISMA Compliance**

The IBM ISS compliance solution for FISMA encompasses people, processes and tools to implement an enterprise-wide security program that meets FISMA requirements, sustains security improvements, and protects against current and future threats.

### **Overview**

IBM ISS has applied its solutions in numerous regulatory environments, including:

- *Health Insurance Portability and Accountability Act (HIPAA)*
- *Sarbanes-Oxley Act*
- *Gramm-Leach-Bliley Act*
- *Supervisory Control And Data Acquisition (SCADA)*
- *ISO 27002*
- *California Breach Law (Bill No. 1386)*

The IBM ISS FISMA solution is based on knowledge and experience gained from helping clients achieve compliance with the above-mentioned regulations. IBM ISS has learned that organizations that take a strategic approach to implementing a complete security solution achieve the most success. Establishing the right security and compliance framework must account for people, processes and technology. In support of developing such a program, IBM ISS draws on its knowledge, experience and capabilities, including:

- *Proactive security intelligence conducted by the IBM ISS X-Force® research and development team, which forms the basis for all IBM ISS services and products*
- *Standardized policies and procedures known to work for FISMA*
- *Documents, tools and checklists that support procedures as well as reporting requirements*
- *Award-winning suite of security solutions that support a complete security program*
- *Global Security Operations Centers that continuously monitor security threats to facilitate proactive information security management.*

### **The IBM ISS Solution for FISMA Compliance**

IBM ISS helps agencies evaluate, protect, manage and improve security and compliance through a comprehensive three-phased approach, beginning with assessment of an agency's compliance environment and a prioritized roadmap for implementing improvements in security performance and compliance; delivery and implementation of products and services to help remediate security weaknesses and sustain security improvements; and ongoing audits of security program effectiveness and compliance in order to monitor and protect against future security threats. The end result is a complete security solution focused on protecting critical and sensitive information.

The IBM ISS Approach to Reducing Risk and Improving Security



### Assessment

IBM ISS begins the FISMA compliance process with a thorough evaluation of an agency's security program. IBM ISS performs comprehensive discovery across security architecture, security management practices and operational security. The IBM ISS team performs an exhaustive audit to assess the organization's posture against the required NIST standards to ensure FISMA regulatory compliance. IBM ISS reviews every element of the agency's security practice, including but not limited to:

- *Policies and procedures*
- *Configuration management*
- *Contingency planning and testing*
- *Penetration testing and vulnerability remediation*
- *Emergency response and disaster recovery plans*
- *Training and awareness*

The assessment is typically a four-to-six week effort tailored to an agency's unique needs and designed to accurately deliver the insights required to thoroughly address agency-specific FISMA reporting requirements. IBM ISS will institute a strategy of ongoing compliance auditing so the organization will be able to achieve and maintain compliance over time. IBM ISS provides a detailed evaluation of the agency's compliance performance and a prioritized roadmap of recommendations for implementing security program and compliance reporting improvements.

## **Remediation**

The remediation phase implements a total security solution using appropriate products and services to develop and sustain a compliance-driven enterprise infrastructure. IBM ISS executes the roadmap of prioritized security improvement recommendations to achieve full FISMA compliance.

For each of the FISMA functional areas defined in the illustration above, IBM ISS provides a complete solution of services and products designed to improve overall information security and protection and to meet compliance requirements.

## **Policies and Controls**

Policies and controls are critical building blocks to compliance, and IBM ISS develops the necessary policies or improves existing policies, and develops or improves configuration management plans.

## **Compliance Assessment**

Just having policies and controls is not sufficient unless they are tested and proven effective. IBM ISS provides the agency with the appropriate tools to help test for compliance as well as the professional services support for installing and configuring the tools. IBM ISS security experts compile inventories and complete certification and accreditation (C&A) documentation, processes and systems, including quality assurance policies and procedures for C&A. IBM ISS provides professional consulting services to conduct threat and risk assessments, including multiple sites and contractor locations.

## **Security Procedures and Tools**

The IBM ISS team can develop missing procedures or improve existing procedures such as password control, login activation/deactivation and software change controls. The team can also advise clients on the effectiveness of existing tools and make recommendations for scalable improvements that can be implemented agency-wide to ensure consistency.



The IBM ISS solution for FISMA compliance includes professional consulting services to evaluate existing C&As. IBM ISS provides guidance on reporting tools necessary to achieve compliance with respect to C&As.

IBM ISS develops a plan for testing contingency plans and works with the agency to test the contingency plans for correctness and effectiveness.

Procedures and tools are only effective if personnel are aware of them and trained to properly use them. IBM ISS can also provide training through Internet-based courseware on its security products. IBM ISS can also provide customized onsite training on the use and administration of security procedures.

**Corrective Action and Remediation**

The IBM ISS team works with agency personnel to develop Plans of Action and Milestones (POA&Ms) for correcting deficiencies. IBM ISS also helps execute plans and uses milestones and metrics to measure progress and success.

**Compliance Reporting**

IBM ISS provides a suite of products and custom configuration resources to assist with proper documentation to support the FISMA reporting process.

**Audit**

An effective security program is a continuously improving process that monitors risks, measures improvements and ensures resilience in the face of change. IBM ISS provides ongoing audits to review corrective actions and measure security and compliance improvements. This allows an agency to review and measure progress periodically, promoting ongoing improvements to increase scores at FISMA reporting time.

During an audit, the IBM ISS team measures the performance improvements against the discovered weaknesses and remediation plans to ensure the effectiveness of remedial actions and to ascertain measurable improvement. IBM ISS assesses and monitors an agency's resiliency against new vulnerabilities and threats and identifies corrective actions to more effectively manage risk and maintain information integrity.

Continuous monitoring, measurement and validation of security program improvements help ensure that the agency's infrastructure governs security effectively and that the nation's assets are protected.

## **Summary and Conclusions**

Protecting the privacy and security of federal information and systems and complying with FISMA requirements is a significant challenge to federal agencies. Faced with cost-effectively meeting FISMA compliance requirements while achieving business objectives and mission, agencies must be efficient to balance both demands.

A best-practice approach to FISMA compliance requires development, implementation and continuous measurement and monitoring of an agency-wide, risk-based security program. Such a solution instills accountability, proactive protection, integrity and continuous improvement. The IBM ISS holistic approach to FISMA compliance helps agencies implement an adaptive environment that improves their security posture and ensures ongoing compliance. The IBM ISS goal is to build quality, measurable validation and continuous improvement processes into security and compliance programs.

IBM ISS leverages its knowledge of regulatory compliance, a complete suite of products and services, proactive intelligence research and world-class security experience to help agencies effectively comply with FISMA and sustain information integrity.

### **IBM ISS: The Trusted Security Provider to Federal Agencies**

Agencies can rely on IBM ISS to help them achieve FISMA compliance and improve information security. IBM Internet Security Systems (ISS) is the trusted security expert to global enterprises and world governments, providing products and services that protect against Internet threats. IBM ISS delivers proven cost efficiencies and reduces regulatory and business risk across the enterprise. IBM ISS products and services are based on the proactive security intelligence conducted by the IBM Internet Security Systems X-Force® research and development team – a world authority in vulnerability and threat research. For more information, visit

**[www.ibm.com/services/us/iss](http://www.ibm.com/services/us/iss)** or call 1 800 776-2362.



© Copyright IBM Corporation 2007

IBM United States  
IBM Global Services  
Route 100  
Somers, NY 10589  
U.S.A.

Produced in the United States of America.

10-07

All Rights Reserved.

IBM and the IBM logo are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both.

Internet Security Systems and X-Force are registered trademarks of Internet Security Systems, Inc. in the United States, other countries, or both. Internet Security Systems, Inc. is a wholly-owned subsidiary of International Business Machines Corporation.

Other company, product and service names may be trademarks or service marks of others.

References in this publication to IBM products or services do not imply that IBM intends to make them available in all countries in which IBM operates.