

Prepared By:



Michael Rasmussen
Risk & Compliance
Lecturer, Writer, & Advisor

Six Critical Elements to Achieve Economies in FISMA Compliance

Federal Information Security Management Act (FISMA) Overview

The Purpose of FISMA

For the past eight years, government agencies have struggled to comply with the requirements of the Federal Information Security Management Act of 2002 (FISMA).¹

The goal of FISMA is to control information security as it impacts national security and the economic interests of the United States. Compliance obligates each U.S. federal government 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.”²

The question before federal agencies is: How can they meet the requirements of FISMA in a cost-efficient but effective manner?

Achieving economies in FISMA compliance requires government agencies to take a risk-based approach to managing information security.

1 FISMA represents Title III of the E-Government Act of 2002, Pub.L. 107-347, 116 Stat. 2899

2 <http://csrc.nist.gov/groups/SMA/fisma/overview.html>

Through process automation, continuous compliance reporting, and security control enforcement, Lumension eases the FISMA compliance burden by delivering on the six elements of compliance economy: agility, consistency, efficiency, transparency, accountability, and security.

Table of Contents

Federal Information Security Management Act (FISMA) Overview ..1	
<i>The Purpose of FISMA</i>	1
<i>Requirements of FISMA</i>	2
Critical Elements to Achieving Economies in FISMA Compliance	3
Applying the Critical Elements for Economical FISMA Compliance ..5	
<i>Concluding Thoughts – Achieving FISMA Compliance Economically</i>	6
About this Paper	7
About Corporate Integrity	7
About Michael Rasmussen	8

www.Corp-Integrity.com
research@Corp-Integrity.com
+1.888.365.4560

Six Critical Elements to Achieve Economies in FISMA Compliance

Requirements of FISMA

FISMA defines information security as “the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction to provide for confidentiality, integrity, and availability of information and information systems.” Responsibility for FISMA compliance is divided across:

- The **National Institute of Standards and Technology (NIST)** for developing standards, guidelines, and tools to comply with FISMA. This includes education for federal agencies about how to approach FISMA compliance.
- The **Office of Management and Budget (OMB)**, to conduct compliance reviews of each agency to strengthen information system security.
- The **head of each agency**, which is accountable for meeting FISMA requirements through policy and procedures that manage information security risks.

The scope of FISMA extends beyond federal agencies and applies to contractors and other organizations using information or information systems on behalf of a federal agency.

FISMA requires each federal agency (and related contractors) to:

- **Inventory agency information systems:** Federal agencies must develop and maintain an inventory of all major information systems under the control of the agency. This includes identification of all interfaces between information systems and other systems and/or networks. Federal agencies must determine how an “information system” is defined. The information system must have identified system boundaries where components have a common purpose and are managed by a single system owner.
- **Categorize information systems:** Each agency must categorize information and information systems based on risk exposure (specifically modeled around confidentiality, integrity, and availability (CIA)).³ If the system has multiple categorizations of information, it is defined as a whole to the highest level of categorization in respective CIA areas.
- **Define minimum-security controls:** All information systems must meet minimum levels of security, regardless of risk categorization.⁴ While there is some flexibility within the agency in applying the minimum-security controls, it must be done in accordance with SP800-53.⁵
- **Establish an ongoing risk-assessment process:** Defining and applying appropriate security controls requires a risk-based approach that involves the system owner and information system stakeholders across the agency. A risk-assessment process confirms the minimum-security controls to determine if additional controls are needed to protect agency operations, assets, individuals, other organizations, or national security.
- **Develop system security plans for each information system:** The system security plan (SSP) documents each information system, its vulnerabilities, threats and associated security controls.⁶ Nothing is static - system security plans require regular review and modification as systems change. The system owner must review the plan on a regular basis, and when changes are made, keep it current.
- **Conduct regular certification and accreditation (C&A) of the systems:** The SSP is the foundation for the next step in FISMA compliance – the C&A. The certification agent analyzes the security plan and validates that security controls

³ Guidance is found in FIPS PUB 199 (<http://csrc.nist.gov/publications/PubsFIPS.html>) as well as in NIST SP 800-60 (<http://csrc.nist.gov/publications/PubsSPs.html>).

⁴ FIPS 200 “Minimum Security Requirements for Federal Information and Information Systems” <http://csrc.nist.gov/publications/PubsFIPS.html>.

⁵ Each federal agency must meet minimum-security requirements by implementing security controls established in NIST Special Publication 800-53, “Recommended Security Controls for Federal Information Systems” <http://csrc.nist.gov/publications/PubsSPs.html>.

⁶ NIST SP 800-18, Revision 1, “Guide for Developing Security Plans for Federal Information Systems” <http://csrc.nist.gov/publications/PubsSPs.html>.

Six Critical Elements to Achieve Economies in FISMA Compliance

described in the SSP are operating and consistent with FIPS requirements. After this process, the system is officially designated as accredited by a senior agency official, which authorizes operation of the information system and accepts the residual risk.⁷

- **Provide ongoing monitoring of information systems:** Systems are dynamic and change as processes, technology, and the agency itself changes. The agency must have in place mechanisms to continuously monitor risk and controls of information systems and keep SSPs up to date. Changes to the information system should trigger a process to update the SSP and conduct a risk assessment to determine if new controls are necessary or controls should be modified. Significant changes may require a system recertification.

Approaching FISMA compliance is not a simple task, and there are a variety of approaches. Some add overhead and encumber the agency, while others achieve efficiency in compliance while reducing operational compliance costs.

Critical Elements to Achieving Economies in FISMA Compliance

A FISMA compliance approach that relies on a manual and labor-intensive process can produce mountains of paper and electronic documents that no one can organize and make sense of. Such a compliance strategy results in overwhelming confusion where the assumption is that everything is in place because personnel are too busy to make sense of it all: that is, until things break down and all the fingers are pointed at the agency.

Instead, the agency should focus on automation and efficiency in compliance while achieving greater control and security. FISMA compliance best practices require that the agency approach FISMA-related processes and controls with these critical elements in mind:

- **Agility:** Agencies need a sustainable process and infrastructure for FISMA compliance. Agencies must also sustain risk and compliance for information systems and associated SSPs on an ongoing basis. Point-in-time assessments are not sufficient by themselves. Agency systems are changing hour-by-hour and minute-by-minute. The dynamic nature of agency operations demands that an organization address FISMA compliance continuously. Achieving agility requires a continuous compliance process that includes:
 - Full discovery of the IT environment and its information and technology assets.
 - Automatic assessment of the environment and devices that connect to it.
 - Automated risk assessment that provides structure around the process of collecting scores and evidence for physical and procedural controls.
 - Policy enforcement of software updates, security patches, and standardized configurations.
 - Flexibility, to handle unique needs and requirements.
- **Consistency:** While guidance has been established by NIST, it is up to the agency head to see that it is consistently applied across agency information systems. Multiple roles in the agency need to work together in an integrated process supported by technology architecture to manage FISMA processes, tasks, and workflows. Achieving consistency in FISMA compliance requires a streamlined compliance workflow and process management capabilities that ensure:
 - Comprehensive inventory and management to:
 - Deliver visibility of both physical and virtual environments from one consolidated console.

⁷ The C&A process is established in NIST SP 800-37 "Guide for the Security Certification and Accreditation of Federal Information Systems" <http://csrc.nist.gov/publications/PubsSPs.html>.

Six Critical Elements to Achieve Economies in FISMA Compliance

- Manage an IT asset repository for all resource types, including applications, databases, servers, networks, data centers, people, and processes.
- Continuous monitoring of compliance and IT risk postures, establishing a mandatory baseline policy that all systems must meet.
- Policies are based on industry best practices with pre-configured checks and elements that can be added and modified based on specific security needs.
- The ability to add, create, define, edit, import and export security configurations and checklists.
- Normalized common controls within a single control, cross-referenced to standards and regulations that call for the requirement.
- **Efficiency:** FISMA compliance can be burdensome – implementing a process and solution to manage the documentation, tasks, reporting, and monitoring of FISMA brings efficiency to agency operations that have other pressing matters. Agencies are best served by addressing a common process (supported by technology) to ease the burden on the agency by leveraging common processes, assessments, and information through technology integration and enablement. Efficiency in FISMA compliance comes through automation of compliance and security processes, including:
 - Addressing multiple management needs through a single solution.
 - Maximum policy flexibility with automated enforcement, saving both time and effort by IT staff.
 - The combination of standard configuration checklists from variety of industry vetted sources with a repository of software vulnerabilities delivering information with context to properly remediate.
 - Automatic risk profile analysis that saves time over manual risk analysis practices.
- **Transparency:** The agency, as well as Congressional and OMB oversight, demands transparency across defined information systems for reporting. Agencies should be able to track and monitor the state of security, risks and vulnerabilities, and action items across the agency. Agencies seeking to achieve transparency in FISMA compliance must:
 - Provide harmonization of compliance controls across a range of mandates in addition to FISMA.
 - View risk holistically across multiple information systems, processes, and departments, to:
 - Collect device, security and configuration information to provide consolidated visibility for system owners.
 - Provide a global view of vulnerability status for all agency assets with an at-a-glance understanding of risk and system status.
 - Document changes and demonstrate progress toward audit and compliance requirements.
- **Accountability:** The head of the agency is ultimately accountable for FISMA compliance, and responsibility extends down to system owners who are tasked with maintaining FISMA compliance and keeping documentation current. Accountability is intimidating when multiple risks, mandates, and requirements are attacking information systems from every angle. The agency must manage FISMA compliance effectively, efficiency, and responsively. This requires a system of accountability where the head of the agency can see the status of FISMA issues, events, incidents, and unresolved actions, and hold individuals responsible for their resolution. Accountability in FISMA compliance requires:
 - Complete compliance status and visibility, to provide:

Six Critical Elements to Achieve Economies in FISMA Compliance

- A complete view of overall FISMA compliance that drills down into specific assets, requirements, and agency systems and processes.
 - Constant audit readiness through automated collection and centralization of security configuration and vulnerability assessment results.
 - Workflow-based surveys to ensure accountability for procedural and physical controls.
 - Stakeholder surveys to determine the business impact of a risk scenario that compromises CIA.
 - Risk-based analysis of the IT posture that enables the agency to drill down on suspicious behavior for further investigation.
- Information system and role-based reporting and administration.
 - Comprehensive reporting to agency management and authorities at a moment's notice.
- **Security:** Ultimately security is what FISMA is about - peace of mind that the agency is not exposing government operations, national security, individuals, and the interests of the country and its citizens to unwanted information risks. Security oversight must anticipate and model various threats, likelihoods, and impacts to the agency, and select and prioritize controls to bring information systems in line with acceptable risk tolerance. Specific security economies in FISMA compliance are achieved through:
 - Identification of controls that enhance security while meeting compliance requirements.
 - Security policy enforcement, including:
 - In-depth assessment of vulnerabilities, patch status, security configurations, installed software, and hardware inventory.
 - Vulnerability audits and remediation across software and endpoints.
 - Automated enforcement of malware protection and endpoint control and security.
 - Timely response to issues and visibility across the agency's information systems environment.
 - Continuous monitoring and enforcement of security – particularly when new information, processes, and technology assets are added.

Applying the Critical Elements for Economical FISMA Compliance

Agencies should implement processes and corresponding technologies that bring economy and efficiency to FISMA compliance.

Lumension is a technology provider in the IT GRC space that Corporate Integrity has researched and evaluated. Through process automation, continuous compliance reporting, and security control enforcement, Lumension eases the FISMA compliance burden by delivering on the six elements of compliance economy: agility, consistency, efficiency, transparency, accountability, and security.

Automating and simplifying information security and compliance management helps agencies gain economies, as well as control, in FISMA compliance. Lumension's product portfolio delivers capabilities that address the specific need for agencies to gain control of FISMA to:

Six Critical Elements to Achieve Economies in FISMA Compliance

- **Discover, inventory, and categorize information systems:** The first step of FISMA compliance is to understand the environment. Agencies are required to inventory and categorize information systems as part of FISMA compliance. Lumension provides solutions to automate discovery and maintain the inventory of information systems.
- **Monitor vulnerability exposure and SSP compliance:** Agencies must continuously monitor for risk exposure and maintain information system minimum controls and additional controls defined in the SSPs. Lumension automates continuous monitoring of the environment by scanning for new vulnerabilities, and validates that information systems are compliant with written SSPs.
- **Remediate and maintain information systems according to SSPs:** When monitoring processes find vulnerabilities or configurations that are not compliant with defined SSPs, Lumension takes action through automatic remediation to bring information systems back into FISMA compliance with the SSP.
- **Manage security configurations across all endpoints:** Enforcement of SSPs does not start and stop with major servers and enterprise applications. Lumension delivers security controls across all endpoints that define an information system for FISMA compliance.
- **Control removable device use and enforce data encryption:** Agencies often find their defined information system for FISMA compliance is pervasive, as information becomes mobile and is transferred between systems. Lumension provides controls that define policies for removable devices and storage, and enables data encryption across removable devices.
- **Streamline overlapping technical and procedural controls across SSPs:** Various endpoints and information systems may fall under the authority of different SSPs. The most stringent controls must be applied to a given information system controlled by multiple SSPs. Lumension provides a single repository for documenting and managing controls to gain efficiencies in maintaining and monitoring the complexities of SSPs in FISMA compliance.
- **Maintain trusted application use on information systems:** Vulnerability and exposure to information systems may result in unauthorized and inappropriate use of applications as defined by FISMA. Lumension ensures only authorized applications are used on information systems to stay in compliance with SSPs.
- **Enforce compliance with evolving requirements:** FISMA compliance is not a point-in-time effort. It requires ongoing monitoring and adaptation to a dynamic environment. Many federal agencies find they must comply with other government regulations in addition to FISMA, and need a way to manage and report on compliance across regulations. Lumension monitors and enforces compliance continuously across regulatory requirements and a changing environment.
- **Enable reporting and monitoring of FISMA compliance:** Enforcement of controls is only one part of the FISMA compliance process. Agencies must also manage workflows, tasks, and reporting across FISMA compliance steps, whether it means establishing SSPs or conducting C&As. Lumension enables economies in FISMA compliance by managing workflow, tasks, documentation, and reporting across the entire FISMA compliance process.

Concluding Thoughts – Achieving FISMA Compliance Economically

FISMA is not a point-in-time effort. Eight years of agencies battling FISMA compliance demonstrate that it is an ongoing process. Information systems are dynamic and changing, which requires a continuous approach to FISMA and maintains compliance as the agency itself changes.

Achieving economies in FISMA compliance starts with enabling the automation and enforcement of compliance processes. This includes providing a common FISMA compliance architecture that integrates the information system inventory, classification, minimum-security controls, risk assessment, SSPs, C&As, and continuous monitoring of FISMA. Agencies should particularly aim to streamline and make FISMA compliance more efficient by getting rid of the mountain of paperwork and individual electronic documents produced by manual approaches to FISMA. Federal agencies need a centralized compliance

Six Critical Elements to Achieve Economies in FISMA Compliance

data warehouse of all FISMA-related content and must provide a full history of changes and modifications to FISMA compliance documentation.

Federal agencies should implement approaches and solutions to automate the monitoring of information systems for changes, vulnerabilities, and controls to validate that the agency is staying within its defined boundaries in the SSP. System owners, as well as the head of each agency, need to know where they stand on FISMA compliance. Compliance costs grow significantly when reporting is encumbered by a massive amount of documents and information collected inconsistently across the agency. Agencies should aim for reporting that is streamlined, efficient and relevant, so system owners and the head of the agency can rest assured they are staying within the boundaries of SSPs and that C&As go smoothly.

About this Paper . . .

This white paper is brought to you by Lumension.

Lumension Security, Inc., a global leader in endpoint management and security, develops, integrates and markets security software solutions that help businesses protect their vital information and manage critical risk across network and endpoint assets.

Lumension enables more than 5,100 customers worldwide to achieve optimal security and IT success by delivering a proven and award-winning solution portfolio that includes Vulnerability Management, Endpoint Protection, Data Protection and Compliance and IT Risk Management offerings. Lumension is known for providing world-class customer support and services 24x7, 365 days a year.

Headquartered in Scottsdale, Arizona, Lumension has operations worldwide, including Virginia, Texas, Utah, Florida, Ireland, Luxembourg, the United Kingdom, Australia, and Singapore. Lumension: IT Secured. Success Optimized.™ More information can be found at www.lumension.com.

Six Critical Elements to Achieve Economies in FISMA Compliance

About Corporate Integrity . . .

Corporate Integrity is a research advisory firm providing leadership in education, research, benchmarking, and analysis on the issues and corresponding solutions for corporate governance, enterprise risk, and compliance management.

Through ongoing research, interactions, and benchmark analytics, Corporate Integrity is the authority in understanding how organizations can foster a culture that “walks the talk” – where integrity is central to governance, risk and compliance (GRC) practices. Corporate Integrity educates organizations and GRC professionals on achieving sustainability, consistency, efficiency, accountability, and transparency in their corporate GRC practices.

In addition to helping organizations understand and improve their internal GRC processes, Corporate Integrity assists technology providers and professional service firms in aligning their sales, product, service, and marketing strategies to the requirements of the roles responsible for GRC.

With the deepest GRC expertise and understanding available in the market, Corporate Integrity has developed a range of service offerings to assist organizations, GRC professionals, technology vendors, and professional services firms focused on GRC.

About Michael Rasmussen . . .

Michael Rasmussen is the authority in understanding Governance, Risk, and Compliance (GRC). He is a sought-after keynote speaker, author, and collaborator on GRC issues around the world and is noted for being the first analyst to define and model the GRC market for technology and professional services.

With more than 15 years of experience, Michael’s objective is to assist organizations in defining GRC processes that are sustainable, consistent, efficient, transparent, and accountable. His thought leadership is tuned to:

- **Educate** GRC professionals within corporations to identify, understand, and analyze GRC strategies, drivers, trends, and best practices;
- **Assist** technology providers with alignment of their product and marketing strategies to the needs and requirements of GRC professionals; and
- **Collaborate** with professional services firms on their portfolio of GRC service offerings to better equip them to serve their respective clients.

A leader in understanding risk and compliance standards, frameworks, regulations, and legislation, Michael aims to improve corporate integrity through advancing GRC initiatives. He has served in leading roles in public policy contributions to US Congressional reports and committees, and currently serves on the Leadership Council and Steering Committee of the Open Compliance and Ethics Group. Michael has been quoted extensively in the press and is respected for his commentary on broadcast news channels.

In June 2007, Treasury & Risk recognized Michael as one of the 100 most influential people in finance with specific accolades noting his work in “Governance and Compliance: Saving the Planet and the Corporation.” Most recently, in October 2008, he was recognized as a “Rising Star in Rocky Times: Corporate America’s Outstanding Executives Under the Age of 40.”

During his career, Michael has worked in the market analyst, consulting, and enterprise sectors. Prior to founding Corporate Integrity, Michael was a Vice-President and top analyst at Forrester Research, Inc. Before Forrester, he led the risk consulting practice at a professional services firm in the Midwest. Earlier, his career included industry experience in healthcare as well as manufacturing.

Michael’s educational experience includes a Juris Doctorate as well as a Bachelor of Science in Business.