altiris®

Nine Steps to FISMA Compliance

How to raise your FISMA report card and keep your IT systems and data secure while achieving your agency's mission

White Paper

June 22, 2006

ABOUT ALTIRIS

Altiris, Inc. is a pioneer of IT lifecycle management software that allows IT organizations to easily manage desktops, notebooks, thin clients, handhelds, industry-standard servers, and heterogeneous software including Windows, Linux, and UNIX. Altiris automates and simplifies IT projects throughout the life of an asset to reduce the cost and complexity of management. Altiris client and mobile, server, and asset management solutions natively integrate via a common Web-based console and repository. For more information, visit www.altiris.com.

Altiris, Inc.
588 West 400 South
Lindon, UT 84042

Phone: (801) 226-8500
Fax: (801) 226-8506

CONTENTS

EXECUTIVE SUMMARY

All federal agencies are required to comply with the Federal Information Security Management Act (FISMA) guidelines for IT systems security. Failure to pass a FISMA inspection can result in unfavorable publicity, increased oversight of your agency, computer breaches, and even a reduction in your IT budget. In this white paper, we'll look at:

- What FISMA is and why it was created
- Key steps in achieving FISMA compliance
- Tools that can help you meet FISMA requirements

A LOOK AT THE PROBLEM

The Federal Information Security Management Act (FISMA) is a comprehensive framework for securing the federal government's information technology (IT).

FISMA provides a set of specific guidelines for federal agencies on how to plan for, budget, implement, and maintain secure systems. These new, stricter security guidelines replaced an expired set of rules under the Government Information Security Reform Act (GISRA).

Each federal agency must develop, document, and implement a program to provide security for the data and IT systems that support its operations and assets—including both its own systems as well as those belonging to other agencies, contractors, and others supporting its mission. To achieve FISMA compliance, your agency must:

- Plan for security
- Ensure that appropriate officials are assigned security responsibility
- Periodically review IT security controls
- Authorize system processing prior to operations and periodically, thereafter

Not only do all federal agencies receive an annual "grade" for their FISMA compliance programs, but these grades are made public on at least one federal Web site. A high grade on the FISMA report card indicates that your agency's systems are secure, your data is locked down, and it gives the American people public verification of that fact.

Figure 1

Your agency's FISMA compliance rating is available for anyone, including the press, to view on the Web.

FISMA Report Card (2001-2005) **Source:** http://reform.house.gov

Agency	2005	2004	2003	2002	2001
Agriculture	24	49.5	40	36	31
AID	100	99	70.5	52	22
Commerce	67	56.5	72.5	68	51
DoD *	38.75	65	65.5	38	40
Education	71	76.5	77	66	33
Energy	46.75	48.5	59.5	41	51
EPA	97.5	84	74.5	63	69
GSA	92.5	79.5	65	64	66
HHS	45.5	49.5	54	61	43
DHS	33.5	20.5	34	n/a	n/a
HUD	67.5	28	40	48	66
Interior	41.5	77	43	37	48
Justice	66.5	82.5	55.5	56	50
Labor	99	83	86.5	79	56
NASA	80	60	60.5	68	70
NRC	60.5	88	94.5	74	34
NSF	95	77.5	90.5	63	87
OPM	98	72.5	61.5	52	39
SBA	78	60	71	49	49
SSA	99	86	88	82	79
State	37.5	69.5	39.5	54	69
Transportation	71.5	91.5	69	28	48
Treasury *	60.5	68	64	49	54
VA *	46	50	76.5	50	44
OVERALL	67.4	67.3	65	55	53
Grades	A	B	C	D	F

altiris

* Numbers for FY 2003 derived solely from agency self-reporting; no Inspector General evaluation available

PENALTIES FOR FISMA NON-COMPLIANCE

If you fail to comply with FISMA, or get a low grade, it's instantly public knowledge. Unfortunately, in recent years the media covering government IT affairs has developed a fondness for reporting on agency FISMA grades.

In 2005, eight agencies—including the Department of Defense (DOD) and Department of Homeland Security (DHS)—received a failing grade, an F, from FISMA. A recent article in *ComputerWorld* puts a spotlight on the DOD and DHS compliance failures. It quotes U.S. representative Diane Watson, who asks, "Is there incompetence?" and answers, "I don't feel comfortable that my homeland is secure" (16 March 2006).

A poor FISMA grade is a sign that your agency may be especially vulnerable to cyber attack. In 2005, an agency with one of the lowest FISMA grades suffered a major security breach, resulting in the theft of personal identity information from millions of U.S. citizens. After the breach, at least one agency official resigned, and another was placed on administrative leave. This incident might have been prevented if FISMA security protocols were in place.

"A low score can severely impact an agency's reputation and threaten the jobs of those who are responsible for regulatory compliance," notes a fact sheet published by Symantec. CIOs may have to testify before Congress to explain their inadequate performance. Worst of all, the Office of Management and Budget (OMB) may delay or cancel funding for agency programs.

HOW FISMA WORKS

FISMA was created under Title III of the E-Government Act of 2002. The act requires federal agencies to give the public access to various government agency systems and data. The head of each agency must implement policies and procedures to cost-effectively reduce IT security risks to an acceptable level.

For instance, U.S. citizens can access IRS data for a variety of purposes, such as finding out what tax bracket they're in based on income. The IRS IT systems challenge: provide the desired level of public access while keeping confidential data—for example, how much money your next-door neighbor made this year—secure.

Agencies must report annually to the OMB on the effectiveness of their IT security programs. The reports must include an independent evaluation by either the agency Inspector General or an external auditor.

Once validated, the report is submitted to Congress for review. Congress has the ultimate authority, because they write the laws and provide funding to each agency.

The E-Government Act gives two government organizations the most active involvement in FISMA: NIST and OMB.

The National Institute of Standards and Technology (NIST) develops IT security standards and guidelines. Federal agencies must follow these rules, which require compliance reporting by each agency on 17 specific security controls.

Table 1

National Institute of Standards and Technology (NIST) security controls.

CLASS	FAMILY	ALTIRIS
Management	Risk Assessment	✓
Management	Planning	✓
Management	System and Services Acquisition	✓
Management	Certification, Accreditation, and Security Assessments	✓
Operational	Personnel Security	✓
Operational	Physical and Environmental Protection	✓
Operational	Contingency Planning	✓
Operational	Configuration Management	✓
Operational	Maintenance	✓
Operational	System and Information Integrity	✓
Operational	Media Protection	✓

Operational	Incident Response	✓
Operational	Awareness and Training	✓
Technical	Identification and Authentication	✓
Technical	Access Control	✓
Technical	Audit and Accountability	✓
Technical	System and Communications Protection	✓

In addition, FISMA requires that the OMB oversee IT security policies and practices across the federal enterprise.

To date, NIST has published numerous security standards and guidelines in support of FISMA. For more information, visit csrc.nist.gov/sec-cert/ca-proj-phases.html.

NIST has also created a database application that contains the security controls, control enhancements, and supplemental guidance from NIST Special Publication 800-53, Recommended Security Controls for Federal Information Systems. For more information, visit csrc.nist.gov/sec-cert/support-tools-applications.html.

NINE STEPS TO ACHIEVING FISMA COMPLIANCE

The NIST Computer Security Division has proposed the following nine-step process for increasing the security of federal agency IT systems:

1. Categorize your information and information systems.
2. Select the appropriate minimum or baseline security controls.
3. Refine the security controls using a risk assessment.
4. Document the security controls in the system security plan.
5. Implement the security controls in the information system.
6. Assess the effectiveness of the security controls.
7. Determine agency-level risk to the mission of business case.
8. Authorize the information system for processing.
9. Monitor the security controls on a continuous basis.

Federal agency security managers with IT budgets less than $500,000 spend approximately 45 percent of their time on compliance issues. Managers with budgets more than $10 million spend 27 percent of their time on compliance issues.

By beginning to implement this nine-step process today, your agency can be proactive in strengthening IT security while reducing the time and burden of reporting. Agencies that do not put the IT security and reporting systems to satisfy FISMA risk facing a panic situation; that is, discovering IT security system flaws and an inability to generate the required reports at audit time.

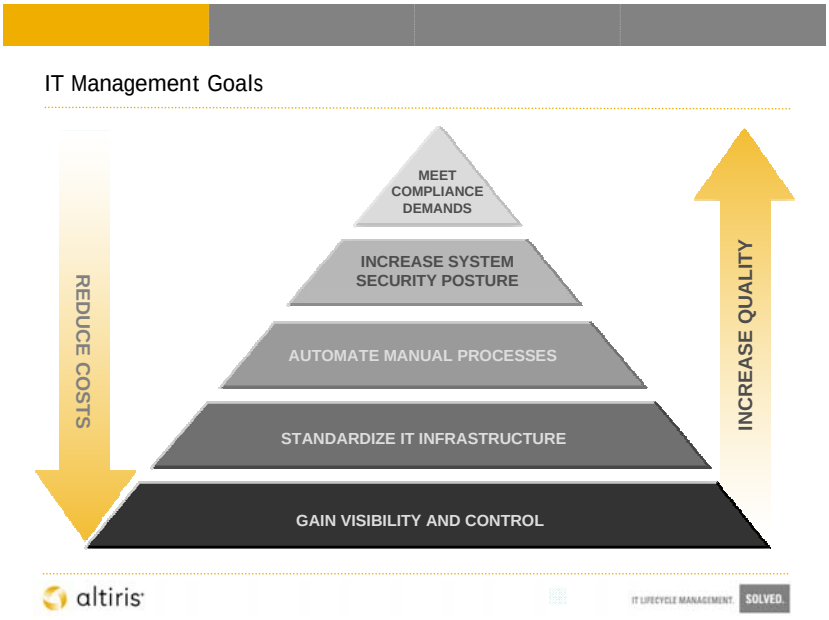


Figure 2

The goals of proactive IT management is to lock down data, comply with FISMA, control costs, and enhance the contribution of IT to the agency's mission.

THE CRITICAL FIRST STEP: MANAGEMENT BUY-IN

As a rule, agencies with the highest compliance ratings have made IT security a high-priority item and have assigned responsibility for FISMA to the chief information officer (CIO). Having senior-level management in charge of FISMA compliance helps drive cooperation throughout the agency.

How can the agency official responsible for FISMA get organizational buy-in? Sociologists have observed that a majority of both individuals and groups of people are resistant to change.

While a few people view changes as healthy, most see change as an impediment to their current way of accomplishing daily tasks or, in more extreme cases, as a criticism of their organization's performance.

The most effective way to identify current processes and implement new processes is to make the entire organization, divisions, and individuals feel vested in the initiative. For example:

The Environmental Protection Agency (EPA) was able to take its FISMA compliance percentage from 36 percent to 94 percent. According to the EPA's Deputy CIO, Mark Day, this was largely the result of a concerted culture change.

To help ensure that EPA personnel care about FISMA and recognize the importance of IT security, CIO Day created a system of easy-to-understand red, yellow, and green "score cards" demonstrating each group's compliance.

Senior management can quickly identify FISMA compliance status for the EPA and each of its sub-agencies: Full compliance (green), making progress (yellow), and requiring further attention (red). Mid-level management in those organizations uses the system to validate their efforts.

At the staff level, work is quantified in a way that can be easily understood and rewarded. While there are numerous other factors involved, the EPA was able to get to 94 percent FISMA compliance due in large part to top-to-bottom organizational "buy-in" to the new IT security processes.

GETTING A PASSING GRADE: THE IT INVENTORY

What provides the best baseline to start FISMA compliance? According to Bob Dix, staff director of the U.S. House of Representatives subcommittee that oversees IT systems security for federal agencies, the most basic requirement of FISMA is the creation of a hardware and software inventory.

An IT inventory is a database with a complete list of all IT assets. It includes a description of the asset, manufacturer, model number, date purchased, date of last upgrade, and a record of service, maintenance, customization, and ultimately disposition.

Since 1998, the federal government has required all of its agencies to have a complete IT inventory. But a Congressional report issued in 2003 found that only five federal agencies had such an inventory.

Dix cited a high correlation between a complete inventory and FISMA compliance: If you don't know what IT assets you own, your claims of a high percentage of security certification and accreditation are easily discredited.

Industry experts speculate that a complete inventory of IT assets alone may be enough to earn an agency a grade of "C" during a FISMA evaluation.

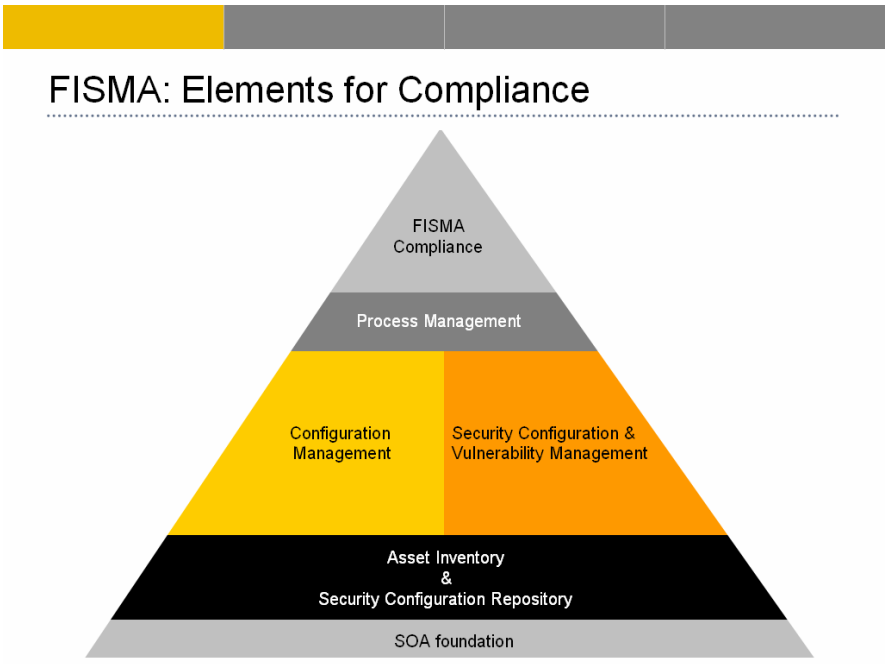


Figure 3

Taking complete IT inventory is a good starting point for your FISMA compliance efforts.

MANAGING RISK UNDER FISMA

FISMA is not intended to eliminate IT risk entirely. Rather, its goal is to achieve the right balance between data security and data access.

When implementing FISMA requirements, responsible agency officials must walk the fine line of risk management. They need to balance the potential harm from the unauthorized exposure of agency data with the ability of IT systems to provide data access to the public in fulfillment of its mission requirements.

The security of IT systems and the ability to conduct daily activities do not have to be an either/or proposition. Making IT security part of the organizational fabric, without interfering with the ability to execute on an agency's missions and goals, can be achieved with the proper balance of processes, organizational buy-in, and tools that execute on the agency's FISMA plan.

IT LIFECYCLE MANAGEMENT

A step beyond merely taking an IT inventory is to implement a system of IT lifecycle management. Simply put, lifecycle management helps you manage your IT assets in an organized manner, with comprehensive record-keeping providing an audit trail.

The lifecycle stages of a piece of IT equipment can include:

1. Purchase or lease
2. Deployment
3. Systems integration
4. Customization or modification
5. Maintenance and repair
6. Upgrades
7. Disposition (recycling, disposal, resale, or redeployment)

An IT lifecycle management program can include establishing a secure configuration management baseline, active asset inventory, identification and remediation of vulnerabilities, and cost control. By implementing IT lifecycle management, you can get maximum productivity out of IT assets while extending each asset's useful life.

In addition, IT lifecycle management gives you a "snapshot" of all IT systems and their configurations. This view includes data security devices and software, enabling you to validate FISMA compliance.

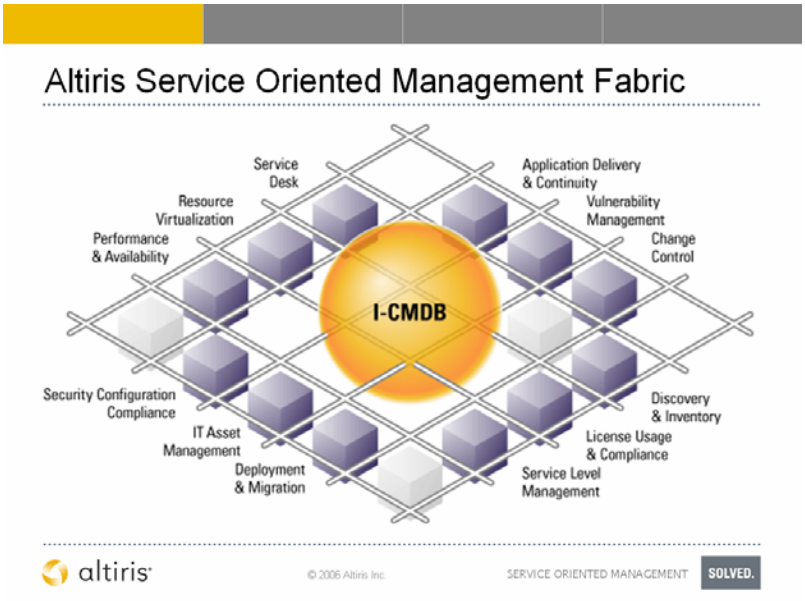


Figure 4

IT lifecycle management gives you greater control over IT assets and their security.

COBIT

There is a close correlation between COBIT and the NIST IT security requirements. By adhering to COBIT guidelines in your IT quality control system, you can more closely align control objectives with NIST standards.

However, while COBIT focuses on providing IT with security and quality control practices, it does not specify how to align IT resources to meet the COBIT critical success factors or the NIST standards. A second strategy that focuses on aligning your IT resources must be considered as a part of your overall FISMA approach.

This is where the Information Technology Infrastructure Library (ITIL) comes in. Focusing on the security controls of COBIT combined with the infrastructure processes of ITIL provides an effective framework for FISMA compliance.

IDENTIFYING AND MANAGING PROCESSES: ITIL

Before you can comply with FISMA, the right processes and organizational visibility of those processes need to be put in place. Without accurate understanding and documentation of key business processes, gaining FISMA compliance becomes both difficult and costly.

At their core, the security mandates of FISMA are business initiatives, not technical requirements. Therefore, proper identification and implementation of processes, a complete inventory of these processes, and senior-level management involvement can help you develop a security plan to manage security risks.

The NIST standards provide some guidance, but not a formula or boilerplate plan to follow, for identifying and managing key business processes. However, there is a boilerplate methodology—ITIL—that enables you to identify, define, and develop processes that support COBIT for FISMA compliance.

Conceived in response to increased dependency on IT and the need for process standardization, ITIL is a set of detailed process guidelines. Presented in a series of books, ITIL contains recommended global best practices, workflow, templates, and terminology. Today ITIL has become a worldwide de facto standard for IT management process implementation.

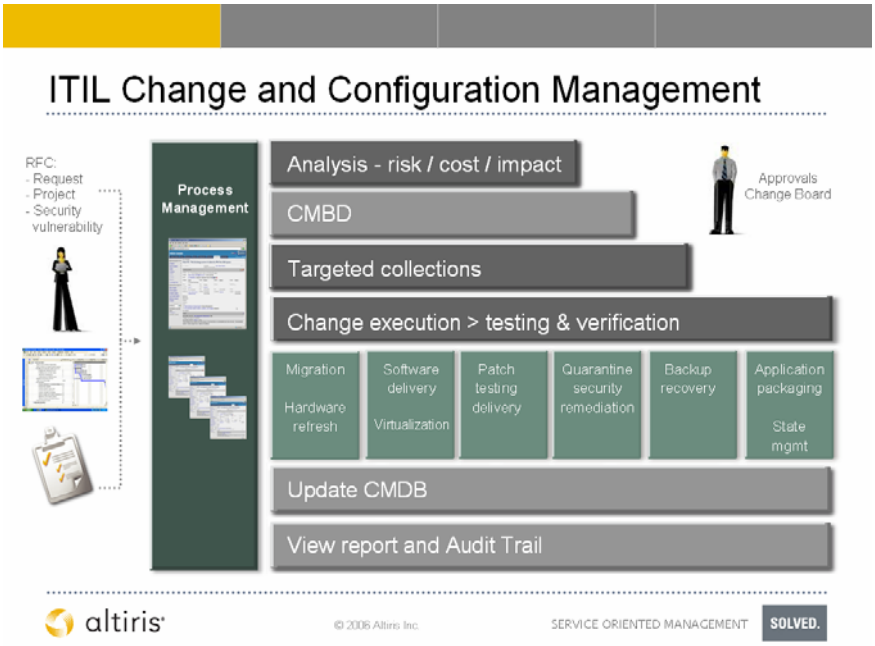


Figure 5

ITIL provides a framework to aid in FISMA compliance.

TOOLS

Once everything else is in place and the security plan is complete, proper tool selection becomes critical for execution. In a survey of 25 federal agency chief information security officers, more than 85 percent said that commercial software for compliance reporting would be “very helpful.”

There are two different approaches to proper tool selection for FISMA compliance. The first approach is to find the single best-of-breed tool to address each FISMA compliance area.

Although this “one tool for one job” approach may address compliance in each individual area, it has numerous drawbacks. These negatives include piecemeal systems, lack of a central database, poor reporting, excessive training requirements, and high system integration and maintenance costs.

The second approach is to find a vendor with multi-product toolsets that address as many FISMA mandates as possible. This “single vendor with a comprehensive tool set” (see appendix A) approach can cost-effectively reduce IT security risks to an acceptable level while reducing implementation, training, and support costs.

FISMA'S TWIN REQUIREMENTS: SECURITY AND REPORTING

FISMA has two primary objectives:

1. Keep federal agency IT systems secure while providing the electronic access for the public mandated by the E-Government Act of 2002.

In essence, FISMA is about letting the public see what they should on your systems—and preventing them from seeing what they should not. A low FISMA score means you are at risk for releasing information that is private and sensitive.

2. Maintain an audit trail of system activity and provide reports that document compliance.

From a macro perspective, an agency's FISMA certification is simply a huge reporting challenge. The two biggest issues in report production are the gathering of data and then its compilation.

The importance of the tools used in the gathering of data and ongoing security maintenance are described in the previous section. Most agency data is typically gathered and stored on different systems in a number of different locations, commonly referred to as "stovepipe systems."

Storing both IT inventory and security data stored in a centralized database enables an agency to produce consistent reports much more easily. There is a direct correlation between consistent report production and higher compliance percentages.

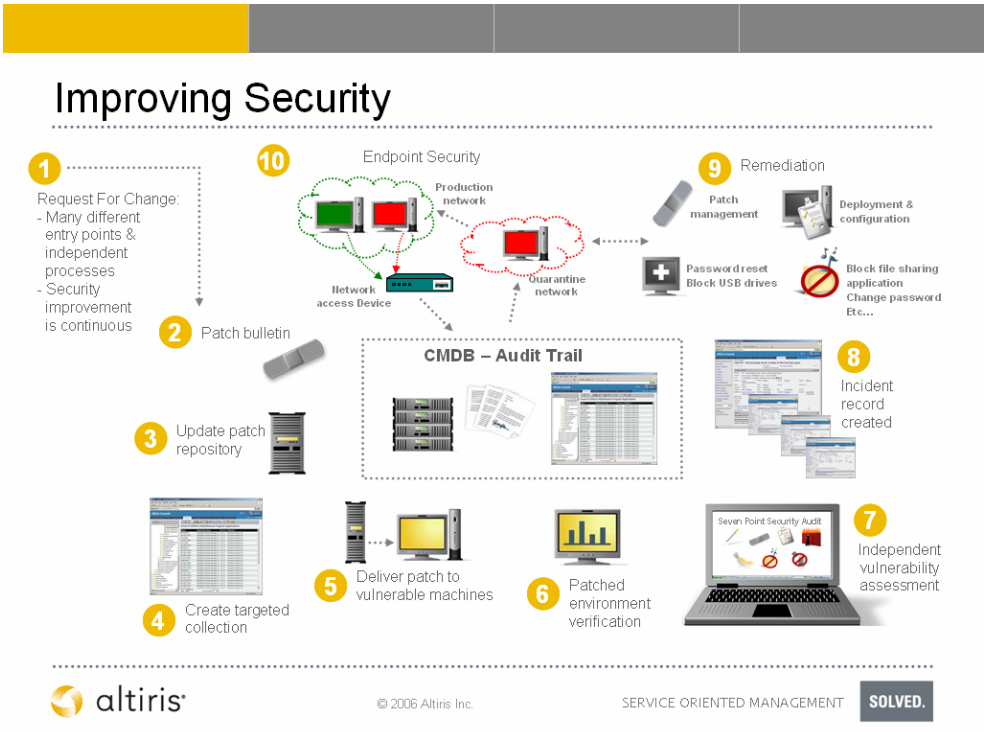


Figure 6

A Centralized Configuration Management Database (CMDB) creates the basis for managing IT security.

SUMMARY AND CONCLUSIONS

1. FISMA compliance is mandatory, not optional, for all federal agencies and any contractors or other organizations supporting that agency's mission.

2. IT security for every federal agency is evaluated annually and reported to the OMB, which makes your grade available to both the public and the press.

3. The penalties for a low or failing FISMA grade include censure by Congress, negative publicity for the agency, and reduced funding for agency initiatives. It may also put your job at risk.

4. Key steps you can take to improve your FISMA compliance rating include making an IT inventory, implementing IT lifecycle management, following NIST standards, building an IT infrastructure library, and using an integrated toolset to manage IT systems security.

5. A reactive approach to FISMA compliance—fixing IT security only when obvious problems arise and scrambling to compile the needed reports at audit time—places a tremendous burden on IT staff and often results in a lower FISMA grade.

6. An ongoing, proactive FISMA compliance program can keep your agency FISMA rating high while reducing the time and burden of reporting, freeing your IT staff to focus on core issues. The OMB states that "all agencies must continually work to ensure that they are FISMA compliant."

APPENDIX A: ALTIRIS TOOLS FOR ACHIEVING FISMA COMPLIANCE

Altiris currently offers a suite of more than 65 solutions that enable government organizations to reach FIMSA compliance.

The core Altiris infrastructure provides customers a Web-based modular console. The console enables them to move away from framework, giving them the flexibility to purchase what they need now and easily add solutions over time.

The following is a sampling and brief description of the Altiris solutions most frequently associated with FIMSA compliance:

Asset Control Solution™—Tracks non-discoverable fixed assets and computers throughout any environment. For each asset, the software tracks location, contact information, cost, and any custom data.

Asset Control Solution manages all fixed assets including desktops, cell phones, pagers, chairs, monitors, fax machines, and so on. IT administrators can import data from Microsoft Active Directory and analyze the data with numerous pre-defined Web reports.

AuditExpress™—Audits Windows, UNIX, and Linux desktops, notebooks, and servers. Audit results are summarized in easy to understand Smart Reports, enabling you to quickly take action on identified system security vulnerabilities. The system checks for antivirus status, operating system security patch status, industry-known vulnerabilities, personal firewall software, system security configuration settings, and unauthorized software and hardware.

Carbon Copy® Solution—Provides remote access from a Web browser. Powerful management features give you the tools you need to remotely administer your corporate environment. Integrated client deployment and configuration simplify distribution. Reports and notification policies track client installations and remote sessions.

Connector Solution™—Integrates Altiris solutions with your organization's third-party systems. You can leverage user and organizational data from your HR system, cost information from your financial system, and other pertinent data from your critical business systems. This solution is a powerful way to connect information systems and provide overall visibility into your organization.

Contract Management Solution™—Tracks the contracts associated with desktops, servers, fixed assets, and service agreements anywhere in your organization. Comprehensive Web reports provide in-depth details of the objects under contract by correlating the contract data with actual system inventory, contact and location information, and associated costs. Tracking contracts saves time and money by centrally managing each corporate contract and avoiding costly penalties.

Deployment Solution™—An easy-to-use, integrated solution that enables you to establish a uniform configuration baseline. The software provides operating system deployment, configuration, computer "personality" migrations, and software deployment across multiple hardware platforms and operating systems. This can help get rid of security vulnerabilities while reducing the cost of deploying and managing servers, desktops, notebooks, and handheld devices.

Deployment Solution™ for Network Devices—Enables you to manage virtual local area network (VLAN) configurations on network devices across vendors. The solution models the physical connectivity of the network and can automatically assign devices to preconfigured VLANs. The software can help you proactively isolating rogue devices on your network before they cause harm.

Helpdesk Solution™—A powerful Incident Management (IM) tool that allows you to raise service levels while reducing costs. Designed for quick implementation, the software is built on the Altiris Notification Server™ architecture. That means you can directly leverage other Altiris components, such as remote control and Web-based administration tools, to provide immediate incident resolution.

Inventory Solution®—Helps administrators manage their multi-platform hardware and software environment from the convenience of a Web browser. You can control what is captured and how it is reported throughout your LAN, WAN, and dial-up enterprise. The software leverages zero-footprint technology and Altiris' built-in Web reports to provide quick ROI. It supports heterogeneous environments that can include Windows, UNIX, Linux, handheld devices, network devices, and Macintosh.

Patch Management Solution™—Permits you to proactively manage patches and software updates by automating the collection, analysis, and delivery of patches across your enterprise. The software, which can be integrated with Altiris Recovery Solution for stable-state rollback, can significantly help you decrease the costs involved in delivering patches throughout your enterprise.

PC Transplant® Solution—Allows you to transfer a PC's files and settings to a new PC quickly and intuitively. The solution allows you to migrate to new desktops and platforms at lower cost, with no loss of settings or data. The software provides cross-version support for more than 60 applications, with automated application installation. Multiple profiles from a single computer can be captured in one automated operation. You can track status and validate successful migrations with comprehensive Web reporting.

Protect™—Enables you to easily maintain the desired state of your PCs. Protect can also allow users to have their own unique configurations, independent of the approved baseline configuration or other user configurations on the system. Changes made during a user session are preserved for that user's next session, but a reset mode gives you the option to delete the changes made during the session when the user logs off.

Recovery Solution™—Protects your organization's servers and computers with scheduled backups, allowing you to recover lost data or roll back to a known good state. Protection is automatic and doesn't require user intervention. Patented technology minimizes bandwidth usage, making Recovery Solution an excellent choice for protecting remote and disconnected users. For those environments without LAN-based connectivity, the software can back up to a local hidden partition.

SecurityExpressions™—An audit and compliance software solution for Windows, UNIX, and Linux desktops, notebooks, and servers, the software audits the seven major areas of system security audit: antivirus status, operating system security patch status, industry-known vulnerabilities, personal firewall software status, system security configuration settings, unauthorized software, and unauthorized hardware. You can audit any networked desktop or server from a centralized management console, enabling you to maintain corporate and regulatory compliance across all systems. The software supports all popular industry standard best-practices system security policies including NIST.

Software Virtualization Solution™ (SVS)—Provides for faster, simpler, and more manageable deployment of desktop applications. SVS isolates applications and data, allowing you to instantly add or remove applications to a Windows workstation. Conflicts between applications or even between different versions of the same application are eliminated.

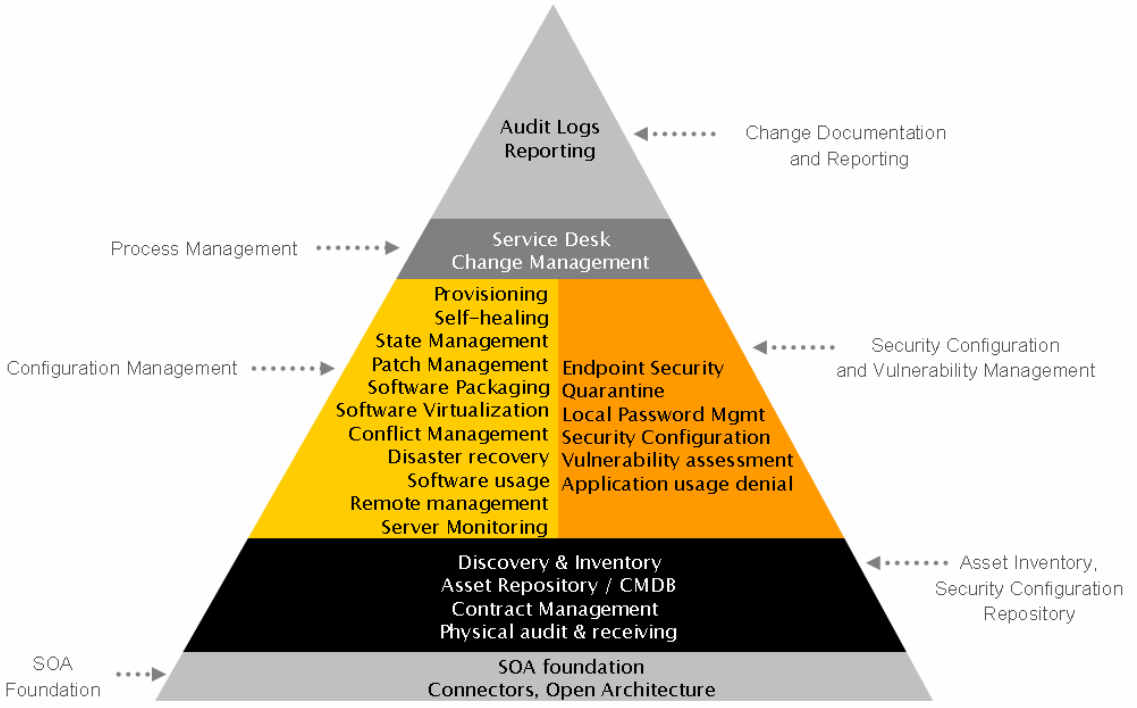
TCO Management Solution™—Helps you track the total cost of ownership (TCO) of your computers, reporting on assets throughout the entire enterprise. Assets can be tracked by cost centers, location, domain, and in many other ways.

Wise Package Studio®—Provides functionality for creating and customizing packages and managing and eliminating application conflicts. Based on a structured, best-practice process called enterprise software packaging, the software enables you to do conflict analysis and a virtual pre-flight on an existing production system.

Altiris offers a comprehensive approach to organizations of any size. Altiris solutions address all aspects of FISMA compliance and are targeted at solving immediate problems while helping you build a roadmap for the future.

Figure 7

Look for a single vendor who can provide a comprehensive suite of solutions that address all aspects of FISMA compliance.



APPENDIX B: ADDITIONAL RESOURCES

- **Office of Management and Budget (OMB)**—For more information, visit www.whitehouse.gov/omb/.
- **FISMA Implementation Project (NIST)**—For more information, visit csrc.nist.gov/sec-cert/.
- **2004 FISMA Report to Congress**—For more information, visit www.whitehouse.gov/omb/inforeg/2004_fisma_report.pdf.
- **IT Governance Institute (ITGI)**—ITGI was established in 1998 to advance international thinking and standards in directing and controlling an enterprise's information technology. For more information, visit www.itgi.org.
- **Information Systems Audit and Control Association (ISACA)**—Founded in 1969, ISACA is a recognized worldwide leader in IT governance, control, security and assurance. For more information, visit www.isaca.org.