
Complying with the Federal Information Security Management Act

How Tripwire Change Auditing Solutions Help

page 2	Introduction
page 3	Exercising Due Diligence
page 3	Parallels with Sarbanes-Oxley Compliance
page 3	Similar Requirements for Deploying, Maintaining and Auditing Controls
page 4	Help is on the Way – Through FISMA Compliance
page 4	Meeting FISMA Requirements with Change Auditing Solutions
page 5	NIST Defines Security Controls and Expands its Focus to Include Auditing
page 5	Tripwire Change Auditing Solutions Meet Requirements
page 6	Delivering Evidence of Effectiveness
page 6	Tripwire Professional Services
page 7	Tripwire and Specific NIST Controls

In the aftermath of September 11, 2001, Congress passed, and the President signed, the E-Government Act, which formally recognized the importance of information security to the United States' economic and national security interests. Title III of that act, the Federal Information Security Management Act (FISMA), requires federal agencies to develop, document, and implement agency-wide information security programs to protect the confidentiality, integrity, and availability of information and systems that support the operations and assets of the agency. FISMA's scope includes securing an agency's operations and assets that are provided or managed by another agency, contractor, or other source.

Compliance with FISMA is not just a good idea, it's the law. FISMA is codified in FIPS199, Standards for Security Categorization of Federal Information and Information Systems, which was signed into law December, 2003. FIPS199 defined the requirements to be used by Federal agencies in categorizing information and information systems in order to provide appropriate levels of information security, according to a range of risk levels. This standard established three levels of risk—low, moderate, and high—for each of the security objectives of confidentiality, integrity, and availability.

Implemented in March, 2006, FIPS200, Minimum Security Requirements for Federal Information and Information Systems, takes the next step. In applying the provisions of FIPS200, agencies will categorize their systems as required by FIPS199, and then select an appropriate set of security controls from technical guidance documents developed by the National Institute of Standards and Technology (NIST). Specifically, agencies must select security controls from NIST Special Publication (SP) 800-53, Recommended Security Controls for Federal Information Systems. NIST SP800-53 provides federal agencies with a foundation for understanding security controls and their use within an information security program. Information covered by NIST SP800-53 includes:

- Structural components of controls
- Organization of controls into classes of operational, management, and technical controls
- How controls are used to support information security programs
- Steps to follow to determine which controls are needed and how to assure and maintain their effectiveness
- Categorization of security controls for graduated levels of security requirements
- A catalog of security controls

NIST SP800-53 is designed to help federal agencies more easily comply with FISMA. Together, the FISMA requirements and NIST technical guidance documents are emerging as a world-class framework for implementing information security governance. They set forth clearly defined roles and responsibilities, data-driven risk classification, and the concept of unambiguous personal accountability for agency residual risk. As a result, the NIST framework is being closely scrutinized by agency Chief Information Security Officers (CISOs), Inspector Generals (IGs), the Office of Management and Budget (OMB) and Congress.

Exercising Due Diligence

Information security is a top priority. It is considered to be so important that the Department of Homeland Security recently promoted the Cyber Security position to an Assistant Secretary level. This sense of urgency within the Federal sector to comply with FISMA is also being felt at state, regional, and local levels of government. Agencies increasingly must demonstrate compliance due diligence by using a risk-based framework, like NIST SP800-53, that maximizes the use of limited resources to protect the most critical assets. Due diligence is not limited to existing information systems and data—it also applies to all new technology purchases.

An interim rule recently published by the Civilian Agency Acquisition Council and the Defense Acquisition Regulations Council specifies new steps that IT procurement workers at federal agencies must take to ensure that information security considerations are an integral part of all technology purchases. The rule essentially incorporates the IT security provisions defined by FISMA into the Federal Acquisition Regulation (FAR).

Parallels with Sarbanes-Oxley Compliance

Thanks to several years spent in creating the NIST framework, federal agency CIOs and CISOs have at their fingertips a robust information security governance framework, tailored for their unique environments. The same framework can be easily extended to other government entities. Training is available. Certifications are emerging. Best practices derived from real-world use are entering knowledge repositories.

In the private sector, compliance issues have not been so clear-cut. Corporate Chief Financial Officers (CFOs) were challenged to comply with Sarbanes-Oxley (SOX) Section 302, which requires internal controls over financial reporting, at the same time that corporate Chief Information Officers (CIOs) were required to comply with SOX Section 404, which requires IT controls on systems related to financial reporting. The result has been confusion and scrambling to meet requirements that, at best, are open to interpretation.

Similar Requirements for Deploying, Maintaining, and Auditing Controls

Federal CFOs are similarly being asked to demonstrate the effectiveness of internal financial controls, per revised Circular A-123. This circular emphasizes the importance of proper stewardship of federal resources, and places accountability on agency managers and staff. A series of related acts serves to reinforce Circular A-123:

- Specific requirements for management controls are articulated in The Federal Managers' Financial Integrity Act (P.L. 97-255). Under this act, agency heads must establish controls that reasonably ensure that obligations and costs comply with applicable law; assets are safeguarded against waste, loss, unauthorized use or misappropriation; and revenues and expenditures are properly recorded and accounted for. Agency heads also evaluate and report annually on their control and financial systems that protect the integrity of Federal programs. Thus, management controls should be an integral part of the entire cycle of planning, budgeting, management, accounting, and auditing.
- The Chief Financial Officers Act requires the preparation and audit of financial statements for 24 Federal agencies. In this process, auditors report on internal controls and compliance with laws and regulations.
- The Inspector General Act provides for independent reviews of agency programs and operations. Offices of Inspectors General (OIGs) and other external audit organizations frequently cite specific deficiencies in management controls and recommend opportunities for improvements. Agency managers are required by the Act to follow up on audit recommendations, correcting problems resulting from inadequate, excessive, or poorly designed controls, and building appropriate controls into new programs.

Help is on the Way—Through FISMA Compliance

The OMB will soon issue a list of best practices designed to help agencies implement internal controls for financial reporting information. The OMB also will begin to provide feedback to agencies on their plans for instituting internal controls, as required by Circular A-123.

The OMB has stated that controls that have been proven effective for FISMA compliance will be acceptable for Circular A-123 compliance. Efficient agency heads can effectively use their FISMA compliance measures to greatly simplify their Circular A-123 compliance efforts.

Meeting FISMA Requirements with Change Auditing Solutions

NIST SP800-37 provides a clearly defined framework for achieving FISMA compliance. NIST SP800-53A is targeted for final publication in late 2006 and establishes methods and procedures to assess security controls. Agency heads can use the framework as a guide to select and specify security controls in their environments.

The NIST framework:

- Facilitates a consistent, comparable, and repeatable approach for selecting and specifying security controls
- Provides a recommendation for minimum-security controls for information systems categorized according to FIPS199
- Promotes a dynamic, extensible catalog of security controls for information systems to meet the demands of changing requirements and technologies
- Creates a foundation for the development of assessment methods and procedures for determining security control effectiveness

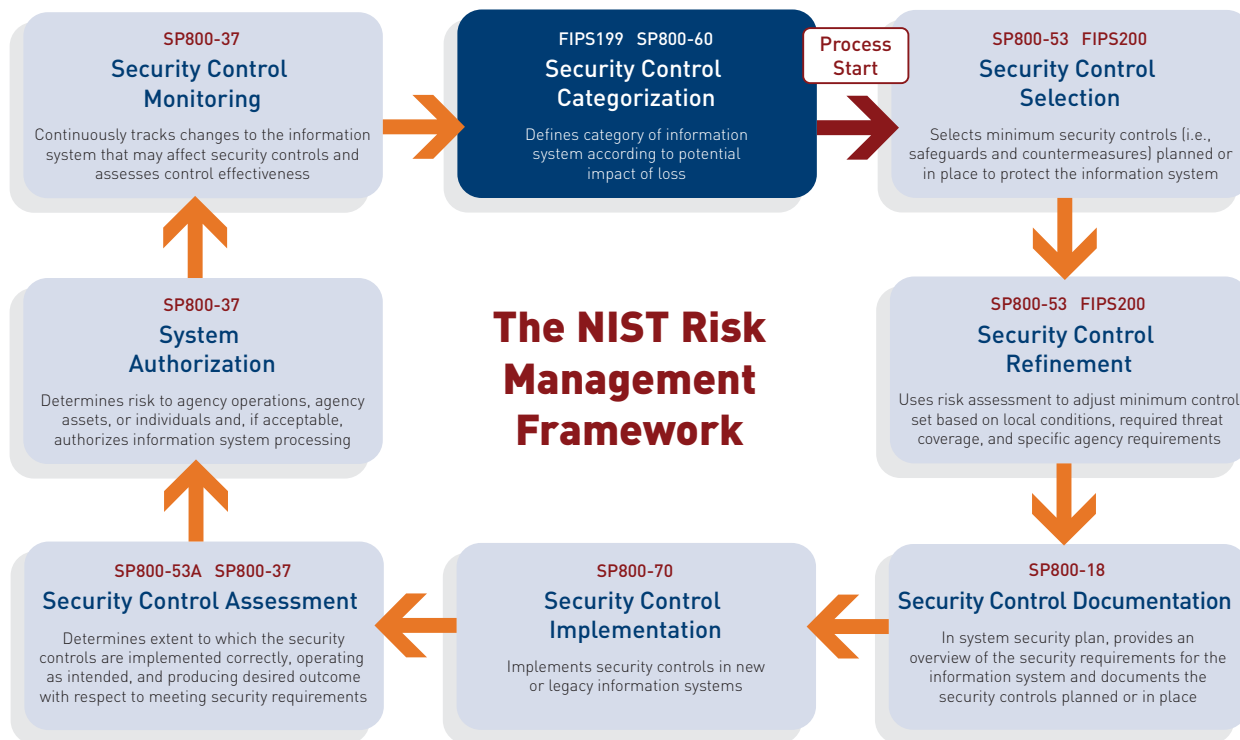


Figure 1: The NIST Risk Management Framework provides agencies with guidelines on assessing, choosing, monitoring, and documenting controls on information systems.

NIST Defines Security Controls and Expands its Focus to Include Auditing

Within the framework, NIST SP800-53 categorizes security controls into three broad classes: Management, Operational, and Technical. These three classes are further divided into 17 families of controls.

The upcoming NIST SP800-53A document will expand NIST guidelines to include guidelines for auditing control effectiveness and achieving full compliance with FISMA.

As highlighted by NIST in SP800-53A:

“Since many of the security controls required to protect organizational information systems will use commercial off-the-shelf information technology products, organizations are encouraged, whenever possible, to take advantage of the assessment results and associated assessment-related documentation and evidence available from independent, third-party product evaluations and validations. Once the information system component product responsible for providing a particular security capability is identified and associated with a particular security control in NIST Special Publication 800-53, the evidence produced during a product evaluation and validation process can be used... to build an effective assurance argument that the security control is effective in its application.”

Tripwire Change Auditing Solutions Meet Requirements

More than 400 government agencies have already adopted Tripwire change auditing solutions to meet a wide range of security and compliance requirements. Tripwire change auditing solutions work with other security measures recommended in various regulators' guidelines, such as personnel policies, administrative procedures, password controls and firewalls, anti-virus tools and authentication software. In fact, Tripwire will monitor the integrity of layered security products themselves. Tripwire change auditing solutions deliver three critical compliance requirements.

Detection

Tripwire change auditing software monitors file integrity and file structures on information systems, including hardware, software, network, and security infrastructure. Tripwire instantly detects unauthorized changes—including changes that would normally be undetected—and enables rapid rollback to a known and trusted state. Change detection and verification are automated, failsafe, and non-intrusive on IT resources, which makes it easy to maintain system integrity and enforce change management policies. With Tripwire, systems do not change without knowledge or authorization.

Audit Control

Tripwire provides detailed change audit information for use in incident investigation, computer forensics, and root cause analysis. Tripwire enables agency staff to quickly pinpoint, analyze, and recover from any undesirable change and, most importantly, document every step to regulators. Only Tripwire delivers assurance that authorized changes are completed, and that unauthorized or ad hoc changes that circumvented policy are detected and immediately reported.

Reporting and Proof

Complete documentation of each change is provided in detailed reports. Tripwire change audit information demonstrates to regulators that changes to information systems can be detected, corrections verified, and changes explained—even if those changes are made outside of authorized change processes. Tripwire proves that security policies are in place, and enables unequivocal enforcement.

Delivering Evidence of Effectiveness

Tripwire can provide evidence about the application of Tripwire products and services in federal agencies. Tripwire can help system owners, authorizing officials, agency and system security officers, and certification agents (internal or external) understand how the deployment of a comprehensive, next-generation file integrity monitor can be reflected in their system security plans, security assessment reports, and plans of action and milestones.

System Classification (per FIPS199 criteria)	
Low	The assessor determines if the mechanism exists and is operational within the information system
Low	The assessor determines if the mechanism is consistent with the functional requirements in the security control statement
Moderate	The assessor determines if the mechanism is implemented correctly (including installation) and operating as intended in accordance with developer/implementer specifications and defined procedures
Moderate	The assessor determines if the mechanism includes an assignment of responsibilities and specific actions to ensure the mechanism is being effectively employed and meets its required function or purpose consistently on an ongoing basis
High	The assessor determines if the mechanism includes a means to support the continuous improvement in its effectiveness

Figure 2: Tripwire is especially helpful in providing the stringent control effectiveness assurance requirements spelled out in NIST SP800-53A for moderate and high-risk systems.

Tripwire Professional Services

Ensuring that IT systems are controlled requires expertise and deep knowledge of data, infrastructure devices, and the dynamics of change—in addition to software. Tripwire Professional Services contributes the knowledge, experience, and change auditing solutions required for maximizing control effectiveness and simplifying FISMA compliance. From initial network discovery to policy file writing and customization, Tripwire’s experienced consultants work efficiently to accelerate the effectiveness of a new change auditing deployment.

Aligning agencies’ information controls to support FISMA compliance is only one benefit. Tripwire also delivers consulting services that help build an integrated, stable, and effective IT environment. This includes implementing solutions for securing data assets and developing strategies for using change monitoring and analysis to maximize IS uptime. Tripwire and its network of certified partners have a proven history of delivering results and enabling agencies to achieve security, compliance, and system availability objectives.

Tripwire and Specific NIST Controls

Tripwire can facilitate compliance with many NIST controls, especially operational and technical controls, by assuring that file system and registry objects and network device configurations do not change unexpectedly. The table below identifies specific NIST controls that Tripwire change auditing solutions can help implement, maintain, and provide auditing proof:

Control Number	Control Name	How Tripwire Addresses Control
AC-2	Account Management	Detects and provides an audit trail of new user IDs, and the modification or deletion of existing user IDs.
AC-3	Access Enforcement	Monitors changes in access controls, especially in network perimeter (firewalls). Can identify that file system and registry object access rights do not change unexpectedly.
AC-5	Separation of Duties	Provides security-related information on user accounts, user roles, user groups, and/or access controls to ensure authorized individuals are performing the appropriate duties.
AC-13	Supervision and Review: Access Control	Provides audit trails on changes made to nodes, showing what changes were made, when they were made, and by whom.
AC-17	Remote Access	Fulfills the "monitor and control" portion of the control by reporting on changes to remote access servers and infrastructure.
AU-2	Auditable Events	Directly addresses both Control Enhancements for audit record aggregation and central management of audit event selection.
AU-3	Content of Audit Records	Provides a single control point for auditing changes across the entire IT infrastructure as well as an archived audit trail of all changes to specified assets.
AU-6	Audit Monitoring, Analysis & Reporting	Able to integrate system audit information with changes in file system and registry objects.
AU-7	Audit Reduction & Report Generation	Provides the capability outlined in Control Enhancement 1, relative to automated mechanisms for audit integrity management.
AU-8	Time Stamps	Provides time stamps for all changes to files. Within the Tripwire GUI, users are able to view when changes are made to nodes, what changes were made, and by whom.
AU-9	Protection of Audit Information	Protects itself from compromise by monitoring and cryptographically protecting its own files. User actions conducted within Tripwire are recorded in a separate audit log, which can be used to identify specific actions performed within the Tripwire application.
AU-10	Non-Repudiation	Evidence of who (or what process) executed events are captured to protect against an individual's subsequent false claims of not having taken a specific action.
CA-2	Security Assessments	Supplies independent verification that agency security controls are working as intended in preventing unexpected changes in network perimeter, file systems, and Windows registries.
CA-7	Continuous Monitoring	Periodically and automatically detects certain configuration changes.

Table continued on following page

Control Number	Control Name	How Tripwire Addresses Control
CM-2	Baseline Configuration & System Component Inventory	Verifies that systems in a baseline configuration do not change, and can confirm that similar types of systems are configured identically.
CM-3	Configuration Change Control	Tracks which changes originated in a Change Control system and which were emergency changes. APIs are provided to allow building of automatic interrogation of change control systems.
CM-4	Monitoring Configuration Changes	Specifically identifies changes to information systems. From change reports, appropriate impact analyses can be launched.
CM-5	Access Restrictions For Change	Independent change detection is a critical component of change management policies that deter and restrict access to systems that may result in changes to those systems.
CM-6	Configuration Settings	Provides the capability outlined in Control Enhancement 1, relative to automated mechanisms to manage and verify configuration settings.
CP-10	Information System Recovery & Reconstitution	Able to verify that production system cold and hot backups are configured identically, and to verify that restore procedures produced an identically configured system.
IR-5	Incident Monitoring	Detects systems changes resulting security events not prevented by security controls.
IR-7	Incident Response Assistance	Strong reporting provides the capabilities outlined in Control Enhancement 1, relative to automated mechanisms to increase the availability of incident response-related information.
SA-10	Developer Configuration Management	Can be used as an important component of an information system developer's configuration management plan.
SI-4	Intrusion Detection Tools and Techniques	Able to rapidly and accurately identify changes not prevented by other intrusion detection tools.
SI-7	Software and Information Integrity	Employs the same checks recommended to automatically monitor software integrity.

To Learn More

For additional information on change and configuration management and change auditing solutions as they relate to IT auditing, regulatory compliance, the IIA and GTAG, the ITPI, the ITGI, and best practices such as ITIL/Visible Ops and COBIT, please visit www.tripwire.com/solutions.



www.tripwire.com
 US TOLL FREE: 1.800.TRIPWIRE MAIN: 503.276.7500 FAX: 503.223.0182
 326 SW Broadway, 3rd Floor Portland, OR 97205 USA

www.tripwire.com/europe
 TRIPWIRE UK: +44 207 618 6512 FAX: +44 207 618 8001
 78 Cannon Street London EC4N 6NQ UK