

CorreLog for FISMA

In 2002, Congress passed and the President signed the E-Government Act, within which is Title III, the Federal Information Security Management Act (FISMA). This law requires federal agencies – and the foundations, educational institutions, and organizations that receive federal funds, as well as the contractors that do business with them – to develop, document, and implement information security programs to protect the confidentiality, integrity and availability of the data and systems that support agency operations, assets and mission.

In meeting compliance, agencies face a dual responsibility: First, is to meet the specific requirements established by NIST in support of the FISMA requirements; and second, is to provide a risk-appropriate level of assurance that critical information security controls are operationally effective and producing intended outcomes. Agency officials are concerned that change management and configuration control are handled in a consistent and enforced manner to reduce vulnerabilities. According to the 2005 White House Office of Management and Budget (OMB) Annual Report to Congress on Implementation of FISMA, uneven implementation of security measures across the federal government leaves weaknesses that must be corrected.

Above all, FISMA matters because in becoming compliant, agencies also become more efficient in their operations, and most importantly, more secure.

Q: Is Correlog limited to only technical NIST controls?

A: CorreLog 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. CorreLog can produce some or all of the required evidence of operational effectiveness for FIPS-199 Moderate-level systems in a mechanized and automated way

Background facts

FISMA was enacted in December 2002.

Compliance for legacy systems was required as of February 2006; for new systems under development, immediate compliance with the National Institute of Standards and Technology (NIST) guidelines for FISMA is expected.

Companies and industries impacted

FISMA applies to all U.S. government agencies, federal contractors and those working on behalf of a U.S. government agency.

Penalties and fines for non-compliance

Specifically, federal agencies are required to develop an agency-wide security program, and to implement and adhere to security configuration standards developed by the National Institute of Standards and Technology (NIST). Agencies must identify and resolve risks, and perform ongoing assessment and testing. They must also conduct annual reviews on the effectiveness of the agency's information security and privacy programs and report the results annually to the OMB that can delay or deny funding requests if agencies score poorly on FISMA evaluations. Also, Congress publishes the annual "scorecard" — grading agencies on their FISMA compliance.

Ship's Log: True Tales of FISMA

1. Your agency is accused of data negligence.

- a) CorreLog provides a clear record of security violations, and supports an over-arching security policy that incorporates all types of platforms, network devices and application programs.
- b) Tamper-proof archives, with encrypted *checksums*, provide clear evidence of security breaches (or the absence of security breaches).
- c) Correlog monitors thousands of security points within your enterprise and provides a clear audit trail — demonstrating your commitment to security and data privacy.
- d) If a breach does occur, immediate assessment of the actual severity can be obtained, as opposed to your customer or client assuming the worst-case scenario.

2. An agency contractor uses the password of a government employee to enter your private system.

- a) CorreLog keeps track of user activity on your system, automatically tracking when users have logged into the system and what changes they have made to critical data items.
- b) You can quickly see when a user has accessed an invalid machine, perhaps during odd hours, and be notified of suspicious behaviors, such as clearing log files, installing software, or simply running an editor or application.
- c) You are notified of the event via e-mail, pager, or some other method — so you can take immediate action to block unauthorized access.
- d) A permanent log of all activity is saved, allowing you to investigate further.

CorreLog at the Helm of FISMA Compliance

CorreLog will guide you through FISMA compliance. CorreLog configuration audit and control software detects every change made to the IT system, alerts when an unauthorized change is made, and assesses each change is within policy. CorreLog facilitates compliance with many NIST controls, particularly operational and technical controls. By using CorreLog, federal agencies and their associated organizations can achieve and maintain a known and trusted state across their IT infrastructure. The CorreLog system monitors thousands of security points; logging all activity on your system (in excess of ten-million events each day) and correlating this data into alerts and actionable data – more clear and detailed than any other technology today. In general, CorreLog:

- Centralizes all logs on a single system
- Provides clear, detailed visibility into logs globally

Navigate Your Way to Compliance — CorreLog for FISMA



- Reduces time and resources spent demonstrating effectiveness of IT controls. CorreLog provides the empirical proof to verify compliance with a single audit trail. CorreLog provides detailed, automated reporting to compliment audits. Correlog dramatically reduces the resources required to prepare audits.
- Maintains compliance automatically — Correlog expose unauthorized changes through reconciliation with expected changes and allows IT staff to immediately identify any exceptions and trigger remediation of configurations that do not conform to policy — helping to meet the continuous monitoring requirements of FISMA.
- Minimizes security risks — Correlog monitors and reports on every change made across the enterprise regardless of source, detecting unauthorized change and non-conforming configurations to proactively discover and manage security and compliance position.

Correlog incorporates a sophisticated, indexed search engine to furnish extremely fast, interactive searching — saving your organization man hours and reducing expertise requirements. With CorreLog, businesses can reach FISMA compliance. Below, please find out how CorreLog addresses FISMA regulations:

Configuration Assessment.

With configuration assessment, CorreLog Enterprise can proactively test and assess a server environment against pre-configured, out-of-the-box policies, helping to enable a minimal deployment window. CorreLog leverages industry standards, specifically benchmarks from the Center for Internet Security (CIS), the National Institute of Standards and Technology (NIST), as well as the Defense Information Systems Agency (DISA). These benchmarks include tens of thousands of configuration assessments enabling automatic sustainable policy compliance testing for FISMA.

Change Detection and Reporting.

CorreLog monitors file integrity and file structures on information systems, including hardware, software, network, and security infrastructure. It then provides detailed change audit information to enable agency staff to quickly pinpoint, analyze, and recover from any undesirable change. CorreLog delivers assurance that authorized changes are completed, and that unauthorized or ad hoc changes that circumvented policy are detected and immediately reported. With a verifiable audit trail, staff can then document every step to auditors or assessors and provide them with detailed reports that demonstrate changes made to information systems can be detected, corrections verified, and anomalies explained. The path from data to information to knowledge is quick and responsive.

Combination for Achieving and Maintaining Automated Compliance.

By combining change detection and reporting with configuration assessment, CorreLog assesses every change as authorized, within policy and compliant, ensuring systems achieve a known and trusted state. CorreLog then helps maintain that known and trusted state by establishing a secure baseline to measure change against, and then monitors against that baseline through ongoing, tunable change detection and reporting.

Enforce FISMA policy for online and offline data transfer.

Monitor and control transfer of federal agency data from all desktops and laptops—regardless of where users and data go, and even when users are not connected to the corporate network.

Control the transfer of federal agency data to removable media.

Regulate how users copy federal agency data to removable USB drives, CDs, DVDs and other external storage devices.

Navigate Your Way to Compliance — CorreLog for FISMA

Control the transfer of federal agency data through the network.

Direct whether and how users may access, print, and send federal agency data over the network via email, peer-to-peer (P2P) applications, IM, HTTP, HTTPS, FTP, Wi-Fi, or other means. Ensure that data only goes to authorized recipients such as contractors or other agencies.

Educate and train end users

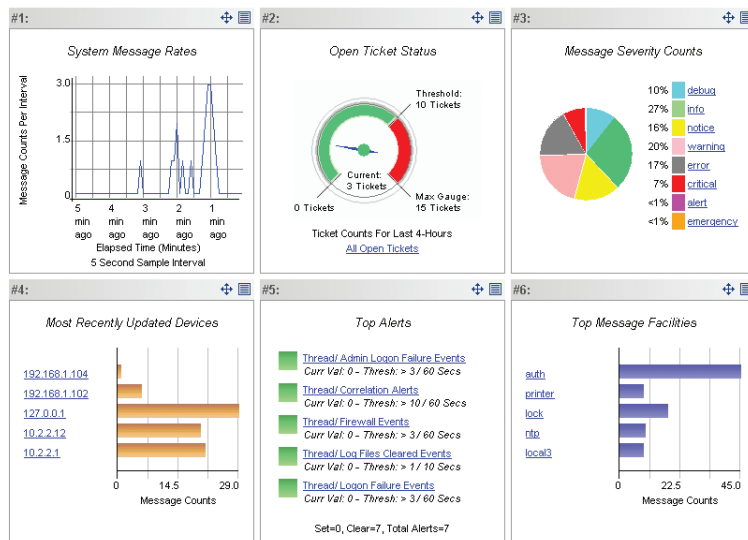
Improve user awareness and reinforce appropriate behavior with custom and automatic notifications, which help maintain the information security policy that FISMA requires.

Prove internal controls

Support compliance with FISMA and NIST 800-53 guidelines by demonstrating security measures to auditors, board members and other stakeholders.

Restrict physical access to agency data.

CorreLog detects when systems are restarted (via a cold-start trap or via syslog messages) indicating that physical access may be breached — and systems may have been tampered with. This includes detection of USB and computer driver activity; indicating that somebody may have physical access to a restricted machine. CorreLog monitors the creation, deletion and modification of user accounts and groups so it can detect when access has been given to a user to a particular system. Additionally, CorreLog keeps track of user logins to these systems, including by time of day, so that “after hours” unauthorized access is easily detected.



Sample of CorreLog Custom Dashboard Reporting

Track and monitor all access to network resources and cardholder data and support audits with detailed visibility.

This is the main role of CorreLog as a security monitor. It provides visibility into who is logging into what areas of the enterprise and keeps track of what users are doing on the system. This is achieved through monitoring log messages and mapping activity back to security protocol. This correlation is presented in detailed event reports like the one above.

Regularly test security systems and processes.

CorreLog schedules periodic tests of network integrity and verifies that certain messages are logged, indicating successful tests. CorreLog interfaces easily with common, security-test software, including port scanners, to verify that CorreLog is successfully monitoring system security. CorreLog has a self-test associated with AES encryption that permits users to verify that CorreLog encryption is working.

Maintain a policy that addresses information security.

An organization cannot claim to have a comprehensive information security policy without monitoring the security message being constantly logged on platforms within your enterprise. An enterprise that installs CorreLog, with no other action, takes a major step forward in creating and maintaining an enterprise security policy.

Develop and maintain secure systems and applications.

CorreLog furnishes ability to make Windows platforms more secure (using the CorreLog Windows agent). For UNIX and other platforms, CorreLog leverages the existing native agent (i.e. the syslog process) to make the managed system more secure. CorreLog is a substantial “development component” of an enterprise-wide security system that incorporates a standards-based, easy-to-use API to allow you to extend your security to any streaming log file or home-grown application.

Navigate Your Way to FISMA Compliance Today

Meet several NIST 800-53A requirements with the ability to assess security protocol configurations and detect and audit change within the IT infrastructure. CorreLog helps you achieve and maintain the integrity of all IT security configurations.

For more information about CorreLog and FISMA compliance, visit www.correlog.com.

To learn more about how CorreLog can help, contact CorreLog toll-free in the US at 877-CorreLog or 239-514-3331.

About CorreLog, Inc.

CorreLog, Inc. delivers security information and event management (SIEM) combined with deep correlation functions. CorreLog’s flagship product, the CorreLog Security Correlation Server, combines log management, Syslog, Syslog-NG, SNMP, auto-learning functions, neural network technology, proprietary semantic correlation techniques and highly interoperable ticketing and reporting functions into a unique security solution. CorreLog furnishes an essential viewpoint on the activity of users, devices, and applications to proactively meet regulatory requirements, and provide verifiable information security. CorreLog automatically identifies and responds to network attacks, suspicious behavior and policy violations by collecting, indexing and correlating user activity and event data to pinpoint security threats, allowing organizations to respond quickly to compliance violations, policy breaches, cyber attacks and insider threats. CorreLog provides auditing and forensic capabilities for organizations concerned with meeting SIEM requirements set forth by PCI/DSS, HIPAA, SOX, FISMA, GLBA, NCUA, and others. Maximize the efficiency of existing compliance tools through CorreLog’s investigative prowess and detailed, automated compliance reporting. CorreLog markets its solutions directly and through partners. Visit www.correlog.com for more information.

1004 Collier Center Way, Suite 103 · Naples, Florida 34110 · 1-877-CorreLog · 239-514-3331 · info@correlog.com