Introduction to FISMA Compliance with CorreLog Mainframe SIEM Solutions

This Executive Summary from CorreLog provides CXOs and InfoSec managers a brief overview of NIST guidelines for maintaining FISMA compliance with best-practice Security Information and Event Management (SIEM)

The origins of the National Institute of Standards and Technology or NIST date back to the early 1900s to a U.S. agency known as the National Bureau of Standards (NBS). The NBS became NIST in 1988 and is now responsible for supplying Government, Industry and Academia with hundreds of Standard Reference Materials (SRMs) for anything from National calibration standards for measuring equipment, to special publications for the handling of information stored by Federal agencies.

This guide will provide a brief overview of NIST mandates for organizations covered by The Federal Information Security Management Act (FISMA), including NIST Special Publications (SPs) and Federal Information Processing Standards (FIPS) publications, and how CorreLog's mainframe SIEM solutions help organizations maintain FISMA compliance, with special consideration for mainframe system data and dataset accesses.

The combined total pages of the NIST SPs and FIPS publications that will be referenced in this executive summary exceeds 750 pages. This executive summary provides an overview of the SPs that need to be on your radar as CXO, and a sample of CorreLog's in-depth rubric on FISMA compliance in its whitepaper titled *"FISMA Compliance with CorreLog Mainframe SIEM Solutions,"* available for downloaded at CorreLog.com/library.

NIST

> "…Through the process of risk management, leaders must consider risk to U.S. interests from adversaries using cyberspace to their advantage and from our own efforts to employ the global nature of cyberspace to achieve objectives in military, intelligence, and business operations…"
>
> -- THE NATIONAL STRATEGY FOR CYBERSPACE OPERATIONS, OFFICE OF THE CHAIRMAN, JOINT CHIEFS OF STAFF U.S. DEPARTMENT OF DEFENSE 2006

FIPS 199 and 200 were the first NIST publications categorizing and establishing federal standards for digital data governance. These and subsequent applicable standards are listed below, including summaries outlining organizational responsibilities for FISMA compliance. (Complete standard and publications list available at NIST.gov). Following the NIST list will be a list of CorreLog functions that assist with maintaining FISMA compliance.

NIST FIPS Publication 199 - *Standards for Security Categorization of Federal Information and Information Systems*

- Lists the standards to be used by all federal agencies for the categorization of information systems and appropriate levels of InfoSec relative to risk

continued.....

NIST FIPS Publication 200 - *Minimum Security Requirements for Federal Information and Information Systems*

- Lists the minimum security requirements for 17 security-related areas for protecting the confidentiality, integrity, and availability of federal information systems and the information processed, stored, and transmitted by those systems.
- Covers access control (authentication), awareness and training, auditing and accountability, and more areas that must be incorporated into a minimum InfoSec process.

NIST SP 800-37 - *Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*

- Lists requirements for integrating an organization-wide IT risk management framework, establishing security controls, and monitoring security controls
- Outlines management of cyber-security risks for mitigation and well-informed risk-based decisions for organizations' mission/business strategies

NIST SP 800-39 - *Managing Information Security Risk Organization, Mission, and Information System View*

- Lays out process for identifying, assessing, monitoring, and responding to risk throughout all three tiers of the organization: 1) the organization itself, 2) mission/business processes, and 3) information systems
- Provides effective governance of risk management best practices in order to achieve mission/business success

NIST SP 800-53 - *Security and Privacy Controls for Federal Information Systems and Organizations*

- Establishes requirements for IT security control structures, baselines, and designations
- Provides guidelines for selecting security control baselines, tailoring baselines, and creating a framework for security control processes with possible "overlays" per sector.

NIST SP 800-137 - *InfoSec Continuous Monitoring for Federal Information Systems and Organizations*

- Outlines InfoSec continuous monitoring (ISCM) for risk-based decision-making by maintaining visibility over all IT assets, monitoring for changes to IT infrastructure, and maintained awareness for the nature of dynamic threats/vulnerabilities with "near real-time" capabilities.
- Lists requirements for defining ISCM strategy, establishing and implementing a program, assessing efficacy, and updating the strategy/program as necessary.

FISMA Compliance Leveraging CorreLog SIEM Solutions

zDefender™ Visualizer, zDefender™ for z/OS, and dbDefender™ for DB2 are designed for security in the context of compliance with FISMA on the mainframe and other data management standards.

Examples:

NIST FIPS Publication 200 and 199 – categorize information systems and implement security controls in areas such as authentication, auditing, accountability, etc.

- **CorreLog Response:** zDefender™ Visualizer, zDefender™ for z/OS, and dbDefender™ for DB2 monitor root and privileged user accesses, audit z/OS facilities such as RACF, CA-ACF2, CA-Top Secret, TCP/IP, IND$FILE, FTP, and others, and deliver real-time security notifications to your SOC in preferred formats.

NIST SP 800-37 – integrate all three tiers of the organization – Organizational Governance & Strategy, Business Processes, and Information System Operating Environment – into a six-step Risk Management Framework (RMF) to continually improve InfoSec and risk-based decision-making

- **CorreLog Response:** zDefender™ Visualizer, zDefender™ for z/OS, and dbDefender™ for DB2 all enable real-time z/OS security inclusion for a complete RMF – delivering continuous monitoring across all mainframe subsystems for informed, risk-based decision-making.

NIST SP 800-39 – defines the components of an ongoing risk management improvement strategy, including response to risk once determined and monitoring risk on an ongoing basis for continuous risk management strategy improvement.

- **CorreLog Response:** zDefender™ Visualizer facilitates continuous monitoring for z/OS security and operational events in real-time in a browser-based SIEM. zDefender™ for z/OS and dbDefender™ for DB2 forward real-time z/OS events to any name-brand WIN-/UNIX-based SIEM for up-to-the-second security notifications in preferred formats.

NIST SP 800-53 – addresses "overlays" for specialized requirements per industry, organization, and/or agency.

- **CorreLog Response:** zDefender™ Visualizer, zDefender™ for z/OS, and dbDefender™ for DB2 can be tailored for security requirements in financial services/banking, healthcare, U.S. Government, and other verticals; compliance with FISMA, PCI DSS, SOX, GLBA, IRS Pub. 1075, GDPR and more.

NIST SP 800-137 – continuous InfoSec monitoring with automated security controls for log management and "near real-time" notifications.

- **CorreLog Response:** Real-time z Systems monitoring and alerts with zDefender™ Visualizer, zDefender™ for z/OS, and dbDefender™ for DB2.

CorreLog's Consultative Approach – Leveraging Existing IT Investments for World-Class InfoSec

CorreLog seeks to gain a full understanding of client policies of governance and organizational strategy, and then work with senior management to understand business processes that help establish security and compliance initiatives. We then work with clients to deploy solutions that meet these governance objectives within the information systems operating environment(s).

CorreLog's roots in mainframe computing date back to the 1970s and we have a fundamental understanding of the mainframe as an operational tool to serve the business side of enterprise organizations. With this understanding we have developed operationally sound and highly functional mainframe security tools to assist with FISMA mandates and other compliance standards such as PCI DSS, HIPAA, SOX, IRS Pub. 1075, GLBA, GDPR, etc.

In Summary

This executive summary is an introduction to CorreLog's more detailed whitepaper, titled *"FISMA Compliance with CorreLog Mainframe SIEM Solutions,"* written to help senior managers understand the origins of FISMA, how NIST details FISMA compliance, and some of the functionality within CorreLog mainframe SIEM tools that can help maintain your FISMA compliance.

Visit CorreLog.com/library to download the FISMA compliance whitepaper and other CorreLog security, compliance and auditing documents.

CORRELOG®

CorreLog.com
info@CorreLog.com • 1-877-CorreLog