Compliance **Risk Management** **IT Governance** **Assurance**

Introduction to Federal Information Security Management Act (FISMA)

Without proper safeguards, federal agencies' computer systems and networks are vulnerable to intrusions by individuals and groups who have malicious intentions and can obtain sensitive information, commit fraud, disrupt operations, or launch attacks against other computer systems and networks. Concerned by reports of significant weaknesses in federal systems, Congress passed the Federal Information Security Management Act (FISMA), which permanently authorized and strengthened information security program, evaluation, and annual reporting requirements for federal agencies. FISMA was enacted as title III, E-Government Act of 2002.

FISMA sets forth a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support federal operations and assets. Its framework creates a cycle of risk management activities necessary for an effective security program; these activities are similar to the principles noted in our study of the risk management activities of leading private sector organizations—assessing risk, establishing a central management focal point, implementing appropriate policies and procedures, promoting awareness, and monitoring and evaluating policy and control effectiveness.

FISMA assigns specific responsibilities to agency heads, chief information officers, Inspectors general and the National Institute for Science and Technology (NIST). It also assigns responsibilities to Office of Management and Budget (OMB), which include developing and overseeing the implementation of policies, principles, standards, and guidelines on information security and reviewing, at least annually, and approving or disapproving, agency information security programs.

FISMA Highlights:

- Federal agencies heads are required to report annually the results of their independent evaluations to OMB;
- Each federal agency shall develop, document, and implement an agency-wide information security 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;
- Federal Information Processing Standards are mandatory and non-waiver able under the provisions of FISMA;
- Periodic testing and evaluation of the effectiveness of information security policies, procedures, practices, and security controls to be performed with a frequency depending on risk, but no less than annually;
- Policies and procedures that are based on risk assessments, cost-effectively reduce information security risks to an acceptable level, and ensure that information security is addressed throughout the life cycle of each agency information system.

Introduction and role of National Institute Of Standards and Technology (NIST):

NIST is required to provide standards and guidance to agencies on information security. In addition, NIST is tasked with developing a definition of and guidelines for detection and handling of information security incidents as well as guidelines developed in conjunction with the Department of Defense and the National

Security Agency for identifying an information system as a national security system. NIST has issued guidance through its FISMA Implementation Project and has expanded its work through other security activities.

NIST FISMA Implementation Project:

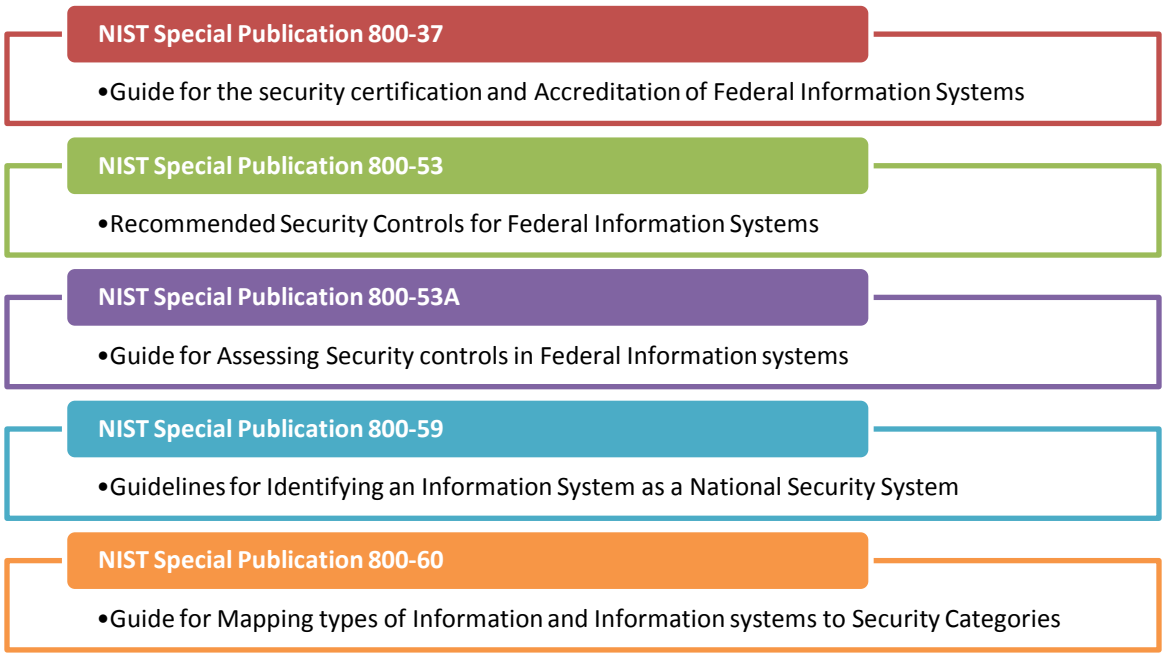
To promote the development of key security standards and guidelines to support the implementation of and compliance with the Federal Information Security Management Act including:

- Standards for categorizing information and information systems by mission impact
- Standards for minimum security requirements for information and information systems
- Guidance for selecting appropriate security controls for information systems
- Guidance for assessing security controls in information systems and determining security control effectiveness
- Guidance for certifying and accrediting information systems

NIST has development two major security standards:

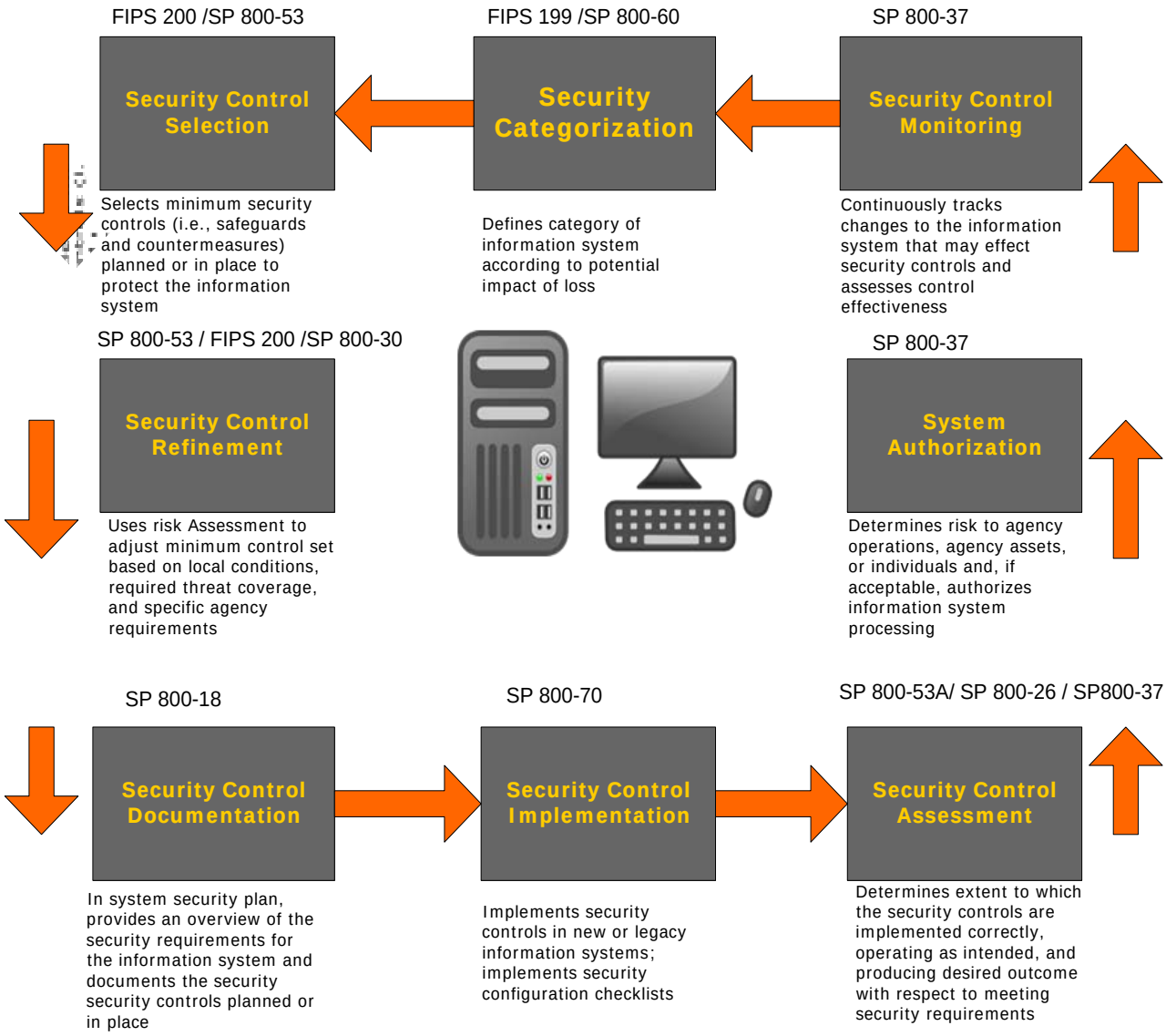
Federal Information Processing Standard
FIPS 199, Standards for security categorization of Federal Information and Information Systems
Federal Information Processing Standard
FIPS 200, Minimum Security Requirements for Federal Information and Information Systems.

NIST has also developed five security guidance documents, supporting FISMA compliance:



Information Security Life Cycle

The Risk Framework



Sigma Technology Partners

Sigma's Risk Framework – Complexity out of FISMA Compliance

Sigma Technology methodology applies key strategies for successful FISMA compliance and facilitates:

- The development of comprehensive information in security programs for federal agencies.
- Employs a security life cycle approach that can be integrated directly into the System Development Life cycle for Federal information systems.
- Integrates NIST Federal Information Processing Standards and Special Publications to maximize their effectiveness and utility for federal agencies.
- Provides a cost-effective approach to managing risk to enterprise operations and assets.

Sigma's FISMA Compliance program covers the entire spectrum of IT under the guidelines of NIST:

Risk Assessment
Security Planning
Security policies and procedures
Contingency Planning
Incident response planning
Security awareness and training
Physical security
Personnel security
Certification, accreditation, and
Security assessments

Access Control mechanisms
Identification & Authentication mechanisms
(biometrics, token, passwords)
Audit mechanisms
Encryption mechanisms
Firewall and network mechanisms
Intrusion detection systems
Security configuration settings
Anti-viral software
Smart cards

Sigma Risk-based framework includes agency-wide security planning, accountability, configuration, implementation and testing assessment and measure, remedial action and a continuous improvement process.

Sigma can assist agencies in selecting and specifying security controls for information systems supporting the agency's mission. The security controls apply to all components of information systems that process, store, or transmit federal information. Our methodology has been developed to help achieve more secure information systems within the federal government by:

- Facilitating more consistent, comparable and repeatable approach for selecting and specifying security controls for information systems.
- Program is designed in accordance with FIPS 199, FIPS 200, SP 800-53 and other NIST's Special Publications.
- Detailed evaluation of the agency's compliance performance and a prioritized roadmap of recommendations for implementing security program and compliance reporting improvements.
- FISMA C&A (Certification and Accreditation) and Compliance audit engagements are assigned to highly skilled CISA/CISSP and CPA partners.

About

Sigma Technology Partners

Sigma Technology Partners is an enterprise technology and business solutions firm delivering quality service to both government and private sector. We provide wide range of IT consulting and business process services. Sigma offers solutions and resources for Security Certification and Accreditation, Federal Information Security Management Act (FISMA) compliance, DoD Information Assurance Certification and Accreditation Process (DIACAP), SAS 70, IT systems Validation for SOX and Regularity Compliance, and Financial and Business Solutions (FABS).

For more information contact us at:

Sigma Technology Partners, LLC
3200 Briggs Chaney Rd,
Silver Spring, MD 20904

Main	202-263-1150
Fax	202-263-1160
Email	info@sigmatechllc.com
Web	http://www.sigmatechllc.com