SiGMA TECHNOLOGY

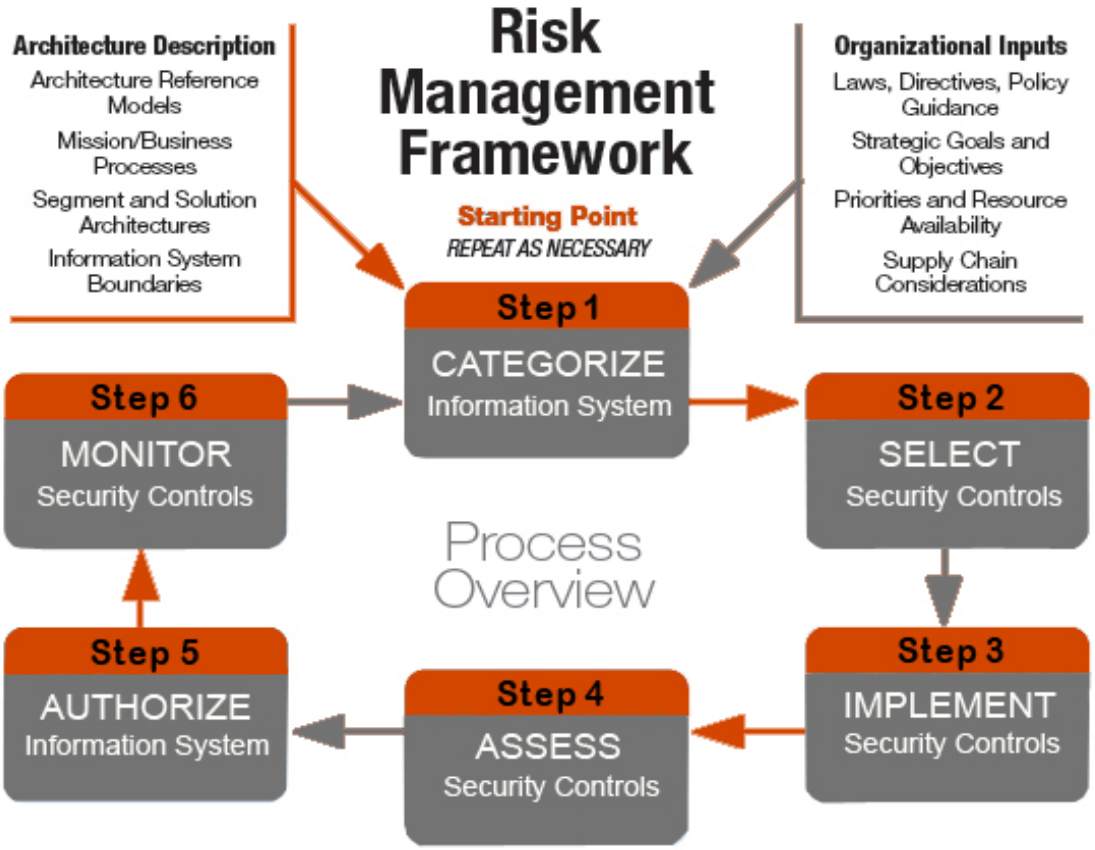
Solutions that Matter

FISMA Compliance Services

Compliance | Risk Management | IT Governance | Assurance

Sigma Technology offers a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support federal operations and assets.

Our framework creates a cycle of risk management activities necessary for an effective security.



Risk Management Framework

Sigma Technology's FISMA compliance program covers the entire spectrum of IT under the guidelines of NIST. Our assessment of Management, Operational and Technical Security controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.

We 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.

We facilitate more consistent, comparable and repeatable approach for selecting and specifying security controls for information systems. Our program is designed in accordance with FIPS 199, FIPS 200, SP 800-53 and other NIST's Special Publications, OMB directives, GAO FISCAM, and agencies specific directives and federal mandates.

Sigma Technology's ST&E is an examination and analysis of both technical and nontechnical security safeguards of IT resources as they have been applied in an operational environment. The ST&E process includes developing an ST&E Plan, executing the ST&E plan, and developing the ST&E report. The ST&E report will serve as input to the Certification Authority (CA) and Designated Approving Authority (DAA) to help them make the accreditation decision for agencies GSSs (General Support Systems) and MAs (Major Applications).

Sigma Technology 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.
- Compliance through automated tools with U.S Government Configuration Baseline (USGCB) and FDCC (Federal Desktop Core Configuration).
- FISMA C&A (Certification and Accreditation) and Compliance audit engagements are assigned to highly skilled CISA/CISSP and CPA partners.

Streamlined Methodology

- Testing and Assessment of Controls as per NIST's and OMB guidelines
- Vulnerability Assessments
- Penetration Testing
- Review of Policies, Guidelines, Departmental Directives and Federal Mandates
- Certification and Accreditation documentation
- Refinement of policies, procedures and SOP's by preparing amendments or revisions
- Post C&A assistance – Continuous Monitoring, Periodic Assessment, POA&M Management and Reaccreditations

FISMA Compliance Following Risk Management Framework (RMF)

Sigma Technology's Risk Management Framework provides a disciplined and structured process that integrates information security and risk management activities into the system development life cycle.

Our RMF steps include:

- **Categorize** the information system and the information processed, stored, and transmitted by that system based on an impact analysis.
- **Select** an initial set of baseline security controls for the information system based on the security categorization; tailoring and supplementing the security control baseline as needed based on an organizational assessment of risk and local conditions.
- **Implement** the security controls and describe how the controls are employed within the information system and its environment of operation.
- **Assess** the security controls using appropriate assessment procedures to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.
- **Authorize** information system operation based on a determination of the risk to organizational operations and assets, individuals, other organizations, and the Nation resulting from the operation of the information sys tem and the decision that this risk is acceptable.
- **Monitor** the security controls in the information system on an ongoing basis including assessing control effectiveness, documenting changes to the system or its environment of operation, conducting security impact analyses of the associated changes, and reporting the security state of the system to designated organizational officials.

Sigma Technology's Continuous Monitoring Framework

The objective of a continuous monitoring program is to determine if the complete set of planned, required, and deployed security controls within an information system or inherited by the system continue to be effective over time in light of the inevitable changes that occur.

- Continuous monitoring determines the security impact of proposed or actual changes to the information system and its environment of operation.
- A disciplined and structured approach to managing, controlling, and documenting changes to an information system or its environment of operation is an essential element of an effective security control monitoring program.
- Security controls that are modified, enhanced, or added during the continuous monitoring process are reassessed by the assessor to ensure that appropriate corrective actions are taken to eliminate weaknesses or deficiencies or to mitigate the identified risk.
- To facilitate the near real-time management of risk associated with the operation and use of the information system, the organization updates the security plan, security assessment report, and plan of action and milestones on an ongoing basis.

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

T (202) 263 1150
F (202) 263 1160

info@sigmatechllc.com
www.sigmatechllc.com