SecureFLO Governance Risk Compliance Practice (GRC)
Federal Information security management assessment (FISMA)

WHAT IS IT?

The Federal Information Security Management Act of 2002 ("FISMA", 44 U.S.C. § 3541, et seq.) is a United States federal law enacted in 2002 as Title III of the E-Government Act of 2002 (Pub.L-107–347, 116 Stat. 2899). The act recognized the importance of information security to the economic and national security interests of the United States.[1] The act requires each federal agency to develop, document, and implement an agency-wide 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.

SCOPE

FISMA has brought attention within the federal government to cyber security and explicitly emphasized a "risk-based policy for cost-effective security. FISMA assigns specific responsibilities to federal agencies, the National Institute of Standards and Technology (NIST) and the Office of Management and Budget (OMB) in order to strengthen information security systems. In accordance with FISMA,

AREAS TO CONSIDER

Risk Management is about reducing the risk to sensitive data managed and owned by Federal government entities. Risk management for FISMA readiness service includes but not limited to

- Inventory of information systems
- Data Classification based on risk (High, Medrate, Low)
- Security Controls
- Risk Assessment
- Systems Security Plan
- Certification and Accreditation
- Continuous Monitoring
- Third Party Risk

Performance of Major Federal Agencies by Cybersecurity Area

Cybersecurity Program Area	Program in place		Program not in place	
	FY 2012	%	FY 2012	%
Continuous monitoring	17	71	7	29
Configuration management	18	75	6	25
Identity and access management	20	83	4	17
Incident response and reporting	20	83	4	17
Risk management	18	75	6	25
Security training	22	92	2	8
POA&M	19	79	5	21
Remote access management	20	83	4	17
Contingency planning	18	75	6	25
Contractor systems	18	75	6	25
Security capital planning	19	79	5	21

Source: Office of Management and Budget

For further details, visit us on the Web or email us.

SecureFLO GRC Difference

SecureFLO GRC program is established to develop a strategy that is based on industry standards. SecureFLO understands that Risk management is variable by industry vertical

SecureFLO is unique in its approach: We focus on data lifecycle; Manage Business Use Cases; Develop a Risk Program on Standards; Compare to industry peers; Assure Continuous Compliance

In short, SecureFLO GRC (Governance Risk Compliance) program is about Prevent Detect and Contain your threats. Develop a holistic program that is defensible and manageable with existing resources.

Our Experience extends to the following services:

- Risk Management Program Development
- GDPR Assessment & Readiness
- ISO27001/2 Readiness
- FISMA Readiness
- HIPAA Assessment
- PCI Assessment
- SSAE16 Certification
- DFS Assessment
- SOX Assessment
- NERC-CIP Assessment
- Development of a GRC reporting Dashboard
- Automation of the GRC Process using open source
- Penetration Testing and Ethical Hacking

Listen, Learn, Innovate!