**FISMA (Federal Information Security Management Act 2002)**

* + Amended by FISMA 2014

**The Federal Information Security Modernization Act of 2014 (FISMA)**

* Highlights the importance of information security to the economic and national security interests of the United States
* FISMA 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.
* 1. Information system inventory
* An inventory of all the information systems in use within the organization need to be maintained by every federal agency and entities working in collaboration with the government. In addition, the agencies also need to maintain an inventory of the interdependencies between the systems and interdependencies between internal systems and systems not under the control of the agency.
* 2. Risk categorization
* All the systems handling sensitive information must be protected with the highest level of security. For this, agencies need to categorize information systems based on risk levels. A high-impact system that stores sensitive information wherein a breach could lead to grave consequences should be categorized as high-risk so appropriate security measures can be implemented. Each information system needs to be placed in appropriate risk categories.
* 3. System security plan
* Every agency is required to create, maintain and update security plans from time to time. The security plan should outline the plan of action and security controls that have already been deployed within the organization.
* 4. Security controls
* There are multiple security controls recommended for FISMA compliance. However, agencies need not implement all the security controls. They need to assess the security requirements of their organization and accordingly implement the appropriate security controls relevant to their organization. The organizations also need to document the chosen security controls in the system security plan.
* 5. Risk assessments
* Risk assessment is one of the most important prerequisites for FISMA compliance. The NIST guidelines suggest agencies conduct three-tiered risk assessments to detect risks at all levels such as organizational level, business process level and the information system level.
* 6. Certification and Accreditation
* Agencies need to go through a four-phased process to achieve certification and accreditation. The four phases are initiation, planning, certification, accreditation and monitoring. Agencies must identify weaknesses, change existing security practices and implement new security measures as a part of the certification process. After certification, the information system can proceed with accreditation.
* 7. Continuous monitoring
* Achieving compliance isn’t a one-time event. There has to be continuous monitoring of systems to identify weaknesses and vulnerabilities and assess security controls. Organizations should maintain compliance throughout.

## \*\*FedRAMP (Federal Risk and Authorization Management Program)

FedRAMP is a government program organized under the General Services Administration (GSA) to provide oversight and direction to federal agencies and commercial cloud service providers (CSP) on how cloud-based services are evaluated for security and ultimately authorized for use within federal agencies.

Systems evaluated under FedRAMP are commercial cloud-based (IaaS, PaaS, SaaS) systems and can support the general business processes of government agencies and commercial companies alike.

Systems that fall under FISMA are traditionally on-premise (e.g. in a government data center) systems that were designed to address the business processes of a specific federal agency. These systems generally aren’t leveraged by multiple federal agencies either.