**Understanding FISMA and its compliance requirement**

Federal Information Security Management Act , or FISMA, is a global standard for financial services organizations that aims to improve the quality of their financial services by providing customers with more information about their financial products and services. It was developed by the Financial Services Industry Association (FSIA) and the International Organization for Standardization (ISO). This standard has been adopted by many countries around the world including Australia, Canada, China, France, Germany, India, Japan, Korea, Malaysia, Mexico, New Zealand, Singapore, South Africa, Switzerland, the United Kingdom, and the United States.

FISMA relies on security categorizations and definitions provided by the federal information processing standards 199 and 200. To fulfill its goal of ensuring confidentiality, integrity, and availability of federal information. The introduction of FISMA gave the National Institute of Standards and Technology the authority to develop the necessary guidelines to create programs that ensure acceptable information security and risk management. In 2014, a physical was emitted by the public law 113-283 which made the secretary of the Department of Homeland Security responsible for administering and implementing the programs that ensure federal information security. The amendment to the law also requires that agencies notify congress of major security incidents within seven days of discovering them. Under the interim rule issued in December 2015, present and future DoD contractors must adhere to two basic cyber security requirements.

**Why was it created?**

The purpose behind creating FISMA was to require each agency to build, document, and implement a finished and complete information security plan to give protection and support to the operations of the agency. FISMA recognizes the importance and significance of information security in terms of the economic and national interests of the United States (US).

**What are FISMA Compliance Requirements?**

FISMA creates a network that is used for managing information security which is followed by all information systems which is operated by the US federal government agency in executive branches and by third-party vendors. There are mainly seven FISMA Compliance Requirements. These are as follows.

1)Agencies and third-party vendors are required by FISMA to maintain an inventory of information systems and recognition of any point of interaction between a particular system or network including those which are not operated by the agency.

2) All the sensitive and confidential data and information systems are categorized. This categorization is based on the required information security according to a range of risk levels. FIPS 199 and NIST SP 800-60provide guidelines on categorization. The primary thing to understand about FISMA is that it implements the high water mark for its impact rating.

3)As defined in FIPS 200, the information system must meet an eligibility requirement. NIST provides various security control measurements and requirements. Agencies should implement only those controls which are required by them and avoid unnecessary ones.

4) The foundation level of all the agency's risk management framework is formed and maintained by the collaboration and combination of NIST and FIPS. Risk assessment checks whether the present security measurements are up to the mark and if any new and updated management is required. It also identifies the different forms of cyber attacks and threats. After determining the risk, the final goal is to give an optimized risk assessment with all the risks calculated.

5)All the systems under FISMA must be checked from time to time to check for all the security controls and recertify if there are any major changes. Continuous evaluation and monitoring should be performed.

6)After completion of the risk assessment and the security plan, reviews should be given on the security controls to make sure that the security risk controls are enough and up to the mark. This review is a four-step process.

7)NIST brought the idea of a system security plan into reality, consisting of plans, modifications, and reviews regarding the system. This plan is one of the major inputs into the process of security certification and accreditation.

**References**

1.<https://www.techtarget.com/searchsecurity/definition/Federal-Information-Security-Management-Act>

2.<https://www.varonis.com/blog/fisma-compliance>

3.<https://www.upguard.com/blog/fisma>

4.<https://www.solarwinds.com/federal-government/solution/fisma-compliance-requirements>

5.<https://digitalguardian.com/blog/what-fisma-compliance-fisma-definition-requirements-penalties-and-more>

6.<https://www.titania.com/resources/guides/what-is-fisma-compliance/>

7.<https://www.algosec.com/resources/fisma-compliance/>