Security Frameworks: FISMA

Levi Overstreet

University of Advancing Technology: NTS435

Security Frameworks: FISMA

The Federal Information Security Modernization Act of 2014 amended the Security Management act of 2002. Its goal was to establish oversight from the Director of Office Management and Budget and set forth authority for the Secretary of Homeland Security to administer the implementation of policies and practices for information systems (Congress, 2014). However, a significant piece of the legislation required federal agencies to report any major data breaches or other information security issues to Congress, not only as they occur but also as an annual report. This change added new reporting requirements for federal agencies to comply with when a major information security incident occurred. Standards were set within the NIST risk management framework that protected critical information within technology-driven agency operations. It also required an increased level of reporting and communication from federal agencies.

Controls and Sub controls

The FISMA framework identifies over 17 control areas and 249 sub controls within its framework (NIST, 2022). The purpose of these controls is to secure and protect the data during storage and transmission. The controls were established to provide guidelines for federal agencies to specify the minimum level of governance required to protect the organization's data. NIST supports state, local and tribunal governments employing the FISMA framework to their information security platform (NIST, 2019). The guidelines were also established with a degree of flexibility to allow for the changing technology landscape. A few of the topic areas covered in these controls are Risk Assessment, Security Planning, Awareness and Training, Access Control, and Accountability and Audit. The controls are assigned a priority code based upon their importance in the plan for the organization (NIST, 2019).

Additional Framework

The FISMA framework was built per FIPS 199 (NIST, 2019). FIPS 199 addresses the need to create a standard for the categorization of federal information systems. The purpose of the categorization is to address the level of risk these systems pose to the confidentiality and integrity of the data. Like the FISMA control families, FIPS 199 maintains controls such as audit and accountability and risk assessment. A framework also used in conjunction with FISMA is the Cyber Supply Chain Risk Management. Its purpose is to identify, assess, and mitigate risk associated with the interconnected nature of IT/OT product and service supply chains (NIST, 2019). The Cyber Supply chain represents nonfederal agencies with access to information and other assets within the Federal government framework. Risk must be evaluated at all levels of design, manufacture, distribute, deploy, maintain, and manage IT/OT products and services.

Authorization and Accreditation process of FISMA

The security accreditation process is structured around the acceptance and management of risk to the agency, its assets the operation, or the individuals within the organization. Authorizing officials are required to determine the risk to operations, assets, or individuals and accept the responsibility of this risk as it pertains to the mission or business needs of the agency as well as evaluate appropriate factors to decide to accept or reject the risk to the agency (NIST, 2018). A certification walks the agency through a series of assessments to determine if current security controls are adequate or if changes to the current operation need to be made. Certification does not include a determination of risk because this requires a broader view of the organization. Accreditation, while an ongoing process, reflects operation for a specific point in time, thus requiring continuous monitoring and reinforcement of procedures (NIST, 2018).

Risk Management as applied to FISMA

The Risk Management framework was designed to be neutral, allowing it to apply itself to any information system. Risk Management Framework, as identified within the FISMA compliance, identifies systems through its identification, protection, and management of assets. A traditional RMF process makes use of the steps to prepare and categorize. These steps would be identified in the Identify step of FISMA. Identification is meant to perform a risk management assessment and in turn, create the management system. Select and Implement correspond to Detect step, whose requirements are to put controls into place and provide necessary training to the organization. Assess and Authorize are Respond, the Risk Management framework looks at the selected controls to ensure they are working as desired. Respond requires analysis, mitigation, and improvement, responding to whether the controls that were put in place are working properly. Finally, monitor is equivalent to Recover. This last step's purpose is to create resilience, continue to monitor activity, make improvements as necessary and create a recovery plan (NIST, 2019).

FISMA is one of the more important regulations in the Electronic Government Act since it brought forth a method to reduce federal data security risks while emphasizing cost-effectiveness. FISMA compliance can help organizations reduce risk and keep data safer, which in turn reduces the financial risks associated with data breach recovery thus underlining the benefits of compliance to this framework.

References

Congress. (2014). S.2521 - Federal Information Security Modernization Act of 2014. Retrieved from https://www.congress.gov/bill/113th-congress/senate-bill/2521

NIST. (2019). FISMA Implementation Project. Retrieved from https://csrc.nist.gov/Projects/risk-management/rmf-overview

NIST. (2018). SP 800-37 Rev. 2 Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy. Retrieved from https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final

NIST. (2022). SP 800-53 Rev. 5 Security and Privacy Controls for Information Systems and Organizations. Retrieved from https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final