David Perez

Professor Barbara Brough

IST-4610

February 5, 2022

# An Overarching Law and Security Standards

In an era where data security is paramount, the Federal Information Security Modernization Act (FISMA) stands as a crucial regulation ensuring the protection of federal information systems. FISMA is a law that was created in 2002 to address several issues directly related to agency operations; It requires government agencies to follow a security approach when handling federal information systems. Every agency working with the federal government must have security infrastructure to address confidentiality, integrity, and availability for the information processes being conducted. As the standard of security, FISMA demands that organizations, contractors, institutions, and other sources working directly and indirectly with federal government data implement a risk-based framework (NIST, 2016). Examples of organizations and institutions include Medicare, Medicaid, student loans, and Cal State Universities; however, these are by no means exhaustive.

One of the advantages of FISMA is that private organizations that want to contract with the federal government can do so by complying with the security standard as well. Consequently, FISMA provides a unified security standard applicable to both public and private sectors, which facilitate organizations’ efforts to comply with federal requirements. Additionally, compliance with the security standard can enhance public perception of an organization, compared to those that are not compliant. An example of a private organization that works with the federal government but also provides services to other private companies is Deloitte. Deloitte is FISMA compliant thus provides the federal government with various services that often require federal data processing; however, it also works with Morgan Stanley, Walmart, and Pfizer. The specific risk-based framework that the National Institute of Standards and Technology (NIST) created is referred to as the Risk Management Framework (RMF).

FISMA requirements are met by the RMF created by NIST which outlines a series of steps that can be followed methodically to ensure systems controls continue to be effective as time goes on. It is important to understand that the RMF is not intended to be a list of tasks that one can simply check off to be compliant with FISMA. Unlike FISMA which provides a high-level overview, RMF provides a system and organizational level approach (SP 800-37r2, 2018, p. 3). The RMF classifies organization systems and applies risk management techniques to allow for specific controls to be implemented according to the need of the organization. NIST created the RMF to comply with the law and to reflect its mission to encourage industrial competitiveness, making cost-effectiveness an essential component of the RMF (NIST, 2009, Mission). The RMF suggests controls to address risk while at the same time achieving effectiveness and efficiency. Afterall, there is no point in seeking a cost-effective approach if it means prioritizing low cost in every area and jeopardizing the overall security structure.

Additionally, the RMF identifies systems based on a hierarchical methodology, specifically based on each system's value to the organization. For example, a healthcare provider might prioritize its electronic health record (EHR) system due to its critical role in patient care and data sensitivity. Meanwhile, a financial institution might prioritize its transaction processing system for its importance in daily operations and regulatory compliance. Moreover, some of the key elements that the RMF addresses in an organization are design and strategy. For instance, a university might use RMF to strategically secure its research data repositories, ensuring compliance with funding agency requirements. After implementing the RMF, the organization's information systems structure will be positioned in a way that interconnects with security control catalog SP 800-53 and other such NIST publications. Ultimately, ensuring RMF is properly followed will allow efficient use of security controls, providing easier implementation to rapidly address areas of the organization more effectively.

There are seven steps overall in the RMF, the first three of which are prepare, categorize, and select. The RMF can work on any organization size and on any technology or system. When deploying the RMF, the first step is to prepare, which ensures the proper classification of organizational assets. In the prepare step the organization must identify essential systems and assets of high value which will make certain that resources equal to their respective priority level are allocated. The process of identifying systems can be augmented by the SP 800-37 task table E-1. Following the task table operations will provide the organization with a list of system types and their respective responsibilities and roles which the next step will require to categorize said systems. After the prepare step, the organization can choose to follow the RMF steps in sequence or choose a non-sequential approach, however, all organizations are expected to complete every step of the RMF.

In the categorize step, systems are assigned an impact value—low, moderate, or high—based on the information they store and the potential disruption to the organization, as determined in the prepare step. An example of a high impact asset would be a server storing sensitive information such as social security and passwords or a backup electrical system essential for business continuity. A special publication that assists in the task of categorization is the Standards for Security Categorization of Federal Information and Systems (FIPS) 199. The next step of the RMF is the select step, each of these steps build upon the other, to categorize one first must prepare, and to select one should first categorize. In the select step, the organization determines what controls to use based on the categorization of the system. Security controls can be found in the NIST SP 800-53 control publication to satisfy RMF and other established standards for organizational and system requirements (NIST, 2016).

The last four steps of the RMF are implement, assess, authorize and monitor. After selecting the controls, the next step is to implement them to safeguard organizational assets. The system owner and/or common control provider must handle the implementation step, planning and documenting the implementations. By documenting the implementation of the security controls chosen in the select step any issues that arise can be traced back and properly addressed. Changes by their very nature can come with unforeseen events. It is possible that selected controls do not fully meet the security and privacy requirements of the organization and when implemented increase risks to the systems or infrastructure. Similarly, it is also possible that selected controls do not meet the specified intent based on security configurations. As an example, risk may increase from implementing certain controls such as CM-6 Configuration Settings control ‘b” from SP 800-53 which allows the organization to implement the configurations. Implementing the control with certain settings may negatively impact a system thus create risk (NIST, 2021).

Because there is risk in implementing the wrong controls with the wrong configurations, an assessment process is required by a third party to discover, document, recommend and if need be, request remediation actions. The organization must select a third-party independent assessment team or assessor that is familiar with the controls that were selected and implemented. Thus, the assessing step evaluates the security controls implemented by the system owner or common controls provider for accuracy and usefulness.

Moreover, when all the previous steps of the RMF have been initiated the common control provider or the system owner must seek authorization before becoming operational. In the authorize step an authorization package must be compiled, and it must contain the following information: assessment reports, security and privacy plans, plan of action, milestones, and an executive summary. The authorization package must be reviewed by an Authorizing Official (AO). The AO is a senior federal official who will assume the risk of operation based on the agreed upon security controls. However, before approving (or not) the Authority to Operate (ATO) the authorization package will be assessed by a security team to determine the risk, security, and privacy posture. If the risk is not accepted, then the AO will issue a Denial of Authorization to Operate (DATO). The next step after being authorized is continual monitoring of the system, on-going assessments, and upkeep throughout the systems life cycle. Monitoring requires continual updates to the authorize package based on each new change implemented (NIST, 2016).

Selecting controls is based on FIPS 199, which categorizes systems according to their impact level. To properly implement controls that would address specific information or information systems there first must be classification of information types and potential impacts. Potential impacts are measured against the security objectives of FISMA which are confidentiality, integrity, and availability. Low potential impact is decided if the impact of an event will have limited repercussions to the individuals or organization. Consequently, moderate impact is decided if an event will have serious effects limited to financial losses or tangible material assets. High impact is decided if severe or catastrophic effects including loss of life can be expected from a breach of confidentiality, integrity, and availability. A detail explanation of each categorization is provided in FIPS PUB 199.

A categorization example can be the potential impact of an organization being rendered offline due to a natural disaster wherein the area power grid has been damaged. In this scenario, the organization must determine the potential impact on the CIA Triad. The potential impact of confidentiality in this specific scenario would not apply since there was no unauthorize access nor information disclosed. However, the integrity impact would be high, and availability would also be high because of the clear disruption of both. A power outage on the organization can potentially cause corruption to data and affect its integrity as well as the overall availability and those issues must be addressed. Therefore, security controls can be suggested that address the systems with high impact concerns. For instance, the organization would then suggest controls that address single points of failure, business continuity management controls such as moving their operations to the cloud and adding database redundancy measures. The importance of categorizing information and information systems correlates and works in tandem with selecting controls that best fit and address priority assets (NIST, 2004).

After fulfilling all FISMA requirements agencies will have a security infrastructure and be positioned in a way that allows for the handling of federal information. With the help of frameworks such as RMF agencies will be able to determine how to implement controls to meet the baseline security in an efficient and cost-effective way. Furthermore, whether in the public or private sector, this standard ensures that organizations have the best security policies in place to process sensitive data with security and privacy in mind.

# References

National Institute of Standards and Technology. (2016, November 30). *Federal Information Security Modernization Act (FISMA) Background*. NIST. Retrieved February 10, 2022, from https://csrc.nist.gov/Projects/risk-management/fisma-background

Cybersecurity and Infrastructure Security Agency. *Federal Information Security Modernization Act*. CISA. Retrieved February 10, 2022, from https://www.cisa.gov/federal-information-security-modernization-act

National Institute of Standards and Technology. (2016, November 30). *About the RMF - NIST risk management framework: CSRC*. NIST. Retrieved February 10, 2022, from https://csrc.nist.gov/Projects/risk-management/about-rmf

National Institute of Standards and Technology. (2016, November 30). *SP 800-53 comment site FAQ*. NIST. Retrieved February 10, 2022, from https://csrc.nist.gov/Projects/risk-management/sp800-53-controls/public-comments-home/faq

National Institute of Standards and Technology (2018) Risk Management Framework for Information Systems and Organizations. (Department of Commerce, Washington, D.C), National Institute of Standards and Technology Special Publication (SP) 800-37 Rev 2, December 2018. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf

National Institute of Standards and Technology (2004) Standards for Security Categorization of Federal Information and Information Systems (Department of Commerce, Washington, D.C), Federal Information Processing Standards Publication (FIPS) 199, February 2004. https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf

National Institute of Standards and Technology. (2009, July 10). *About NIST*. NIST. Retrieved February 16, 2022, from https://www.nist.gov/about-nist

National Institute of Standards and Technology. (2021, March 11). *NIST Risk Management Framework (RMF) Implement Step*. NIST. Retrieved March 31, 2022, from https://csrc.nist.gov/CSRC/media/Projects/risk-management/documents/04-Implement%20Step/NIST%20RMF%20Implement%20Step-FAQs.pdf