Christine Jimenez

Professor Demirel

CYSE 495

6 October 2024

Risk Management Framework for Information Systems and Organizations

The Risk Management Framework for Information Systems and Organizations contains updates that more closely align with the NIST Framework. It integrates the usage of privacy risk management processes. This document serves as a comprehensive guide for organizations, particularly within the federal sector, in managing risks associated with information systems throughout their life cycle. This review will include an overview of the document, by examining the six steps within RMF, and identifying areas for improvement to better address current security and privacy needs.

NIST SP 800-37 Revision 2 provides to aim and assist organizations in implementing effective risk management practices that are tailored to their specific environments.The primary objectives of the document are guiding organizations in the selection, implementation, and the maintenance of their appropriate security and privacy controls. Furthermore, integrating these practices into the system development process. The extent to which this publication relates to are federal agencies, contractors, and other entities that operate using federal information systems. It emphasizes the need for a more comprehensive approach at managing security and privacy risks. The revision of this document provides a detailed and organized description of the several sections that are being used to help implement the framework. This structured approach of the

document enables all entities utilizing the document to understand and apply the risk management practices.

RMF or the Risk Management Framework were developed through the help of the National Institute of Standards and Technology. Like previously mentioned, this document provides a common baseline for organizations. Firstly, I will provide an overview of the six steps: categorize information systems, select security controls, implement security controls, assess security controls, authorize information systems, and monitor security controls. The first step involves categorizing information systems based on the types of information that they process and the potential impact of a security breach. The Federal Information Processing Standards (FIPS) 199 guides organizations to determine impact levels (low, moderate, or high) in accordance with the confidentiality, integrity, and availability of information. Categorizing information systems helps to understand the potential risks that can be associated with the system and ensures the practice of risk management processes.

The second step in the process is to select security controls. This has to do with organizations selecting the appropriate security controls from NIST SP 800-53, tailoring it to the system's impact level. This step takes into consideration the organizational risk tolerance, mission needs, as well as, compliance requirements. This step in the process ensures that the chosen controls are effective in mitigating any risks present, while also considering the operational context of the information system.

The third step in the risk management framework is implementing security measures and controls. This process is crucial as it focuses on deploying the security measures necessary to the operational environment. Organizations are required to document their implementation processes. This might include documenting configurations and system settings, this provides

transparency. This step in the process ensures that sensitive information is being protected with practical security measures.

The fourth step is assessing security controls, the assessment of security controls involves the evaluation of effectiveness through rigorous testing and also evaluation. This step requires organizations to document their findings and vulnerabilities that may be identified. This step helps to provide any potential recommendations for remediation in the event of an attack to the system. The assessment process is vital because it ensures that the controls are functional and provides assurance that the system's security postures are functioning as they should.

The fifth step is authorizing information systems, this is followed after the security controls are assessed. The authorizing official accepts the risk that is presented within the information system. It includes a comprehensive review of the security assessment results, the security posture present, and any remaining risks. Organizations are required to develop and implement continuous monitoring plans to ensure that there are ongoing risk management processes always in place.

The sixth and final place is monitoring security controls. This step includes continuous monitoring of computer systems and security controls. This requires organizations to assess and track performance controls. This process is essential in adapting the risk management strategy against evolving risks and maintaining a robust security posture. All in all, while there are six steps in this framework there is no singular step that is more important than the other. Each of these steps help to maintain and strengthen systems and are all equally important and must be implemented to mitigate and control any possible vulnerabilities.

While this framework has already been revised and it is quite comprehensive as is, NIST SP 800-37 Revision 2 can benefit from updates to better address more current security and

privacy needs. With anything in the digital world, constant updates will always be beneficial as technology is constantly evolving and advancing. One area for improvement that I believe will deem as beneficial is the inclusion of guidance on emerging threats and technologies. This can include, but is not limited to ransomware, artificial intelligence vulnerabilities, and even supply chain risks. As the possibilities of risk evolve, the Risk Management Framework should provide organizations with more strategies to help mitigate these risks effectively. So it would simply involve adding on to what has already been provided in this framework. Another big area for important might be enhancing the integration of privacy considerations throughout the RMF steps. Because there is an increasing importance of data protection and privacy laws, there should be a specific area that explicitly addresses privacy controls and assessments. This can help organizations to navigate complexities of compliance while also protecting their sensitive information. Another potential improvement that would make RMF better is aligning it with other already established frameworks or even international standards. This can help in terms of collaboration across multiple organizations and sectors, which will help to further strengthen all security resilience.

In conclusion the NIST Risk Management Framework provides a very structured approach for organizations to manage security and privacy risks effectively. By focusing and following the six steps that have been outlined in NIST SP 800-37 Revision 2, organizations are able to establish a comprehensive risk management strategy that helps to safeguard their information systems. While it is an amazing review, periodic reviews and updates are necessary to keep up with the pace of evolving technological landscape and emerging threats. By addressing these areas for improvement, NIST can continue to support so many organizations in their efforts to protect sensitive information while also complying with federal regulations.

References

National Institute of Standards and Technology. (2018). Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy (NIST Special Publication 800-37 Rev. 2). Retrieved from NIST.