Risk Management Framework 1O1

By itsmecevi.github.io

The Risk Management Framework (RMF) is a set of criteria that dictate how the United States government IT systems must be architected, secured, and monitored.

Originally developed by the Department of Defense (DoD), the RMF was adopted by the rest of the US federal information systems in 2010. Today, the National Institute of Standards and Technology (NIST) maintains NIST and provides a solid foundation for any data security strategy.

The RMF builds on several previous risk management frameworks and includes several independent processes and systems. It requires that firms implement secure data governance systems and perform threat modeling to identify cyber risk areas.

Agenda:

1. What Comprises the Risk Management Framework?
2. The 5 Risk Management Components
3. The 6 Risk Management Framework (RMF) Steps
4. How Can An Effective Risk Management Framework Benefit A Business?

⇨ What Comprises the Risk Management Framework?

- The risk management process is specifically detailed by NIST in several subsidiary frameworks.
- The most important is the elegantly titled "NIST SP 800-37 Rev.1", which defines the RMF as a 6-step process to architect and engineer a data security process for new IT systems, and suggests best practices and procedures each federal agency must follow when enabling a new system
- In addition to the primary document SP 800-37, the RMF uses supplemental documents SP 800-30, SP 800-53, SP 800-53A, and SP 800-137:
  - NIST SP 800-30, entitled Guide for Conducting Risk Assessments, provides an overview of how risk management fits into the system development life cycle (SDLC) and describes how to conduct risk assessments and how to mitigate risks
  - NIST SP 800-37 discusses the risk management framework itself and contains much of the information we'll cover in the remainder of this guide.
  - Finally, NIST SP 800-39, titled Managing Information Security Risk, defines the multi-tiered, organization-wide approach to risk management crucial for reaching compliance with the RMF.

⇨ The 5 Risk Management Components

The first, and arguably the most important, part of the RMF is to perform risk identification. NIST says, "the typical risk factors include threat, vulnerability, impact, likelihood, and predisposing condition." During this step, you will brainstorm all the possible risks you can imagine across all of your systems and then prioritize them using different factors:

- 1-Risk Identification:
  - Threats are events that could potentially harm the organization by intrusion, destruction, or disclosure.
  - Vulnerabilities are weaknesses in the IT systems, security, procedures, and controls that can be exploited by bad actors (internal or external).
  - Impact is a measurement of how severe the harm to the organization would be if a particular vulnerability or threat is compromised.
  - Likelihood is a measurement of the risk factor based on the probability of an attack on a specific vulnerability.
  - Predisposing conditions are a specific factor inside the organization that either increases or decreases the impact or likelihood that a vulnerability will come into play.

- 2-Risk Measurement and Assessment: Once you have identified the threats, vulnerabilities, impact, likelihood, and predisposing conditions, you can calculate and rank the risks your organization needs to address.
- 3-Risk Mitigation:
  - Eliminate
  - Reduce
  - Transfer
  - Retain/accept
- 4-Risk Reporting and Monitoring:
  - The RMF requires that organizations maintain a list of known risks and monitor known risks for compliance with the policies.
  - Statistics on data breaches indicate that many companies still do not report all of the successful attacks they are exposed to, which could impact their peers
  - Data breaches (see the data breaches slide)
- 5-Risk Governance: All of the steps above should be codified into a risk governance system.

⇨ The 6 Risk Management Framework (RMF) Steps

At the broadest level, RMF requires companies to identify which system and data risks (see the data risk slide) they are exposed to and implement reasonable measures to mitigate them. The RMF breaks down these objectives into six interconnected but separate stages.

- 1-Categorize Information Systems
  - Use NIST standards (see the NIST standard slide) to categorize information and systems so you can provide an accurate risk assessment of those systems.
  - NIST tells you what kinds of systems and information you should include.
  - And what level of security you need to implement based on the categorization.

- 2-Select Security Controls
  Select the appropriate security controls (see the security control slide) from the NIST publication 800-53 to "facilitate a more consistent, comparable, and repeatable approach for selecting and specifying security controls for systems."

- 3-Implement Security Controls
  Put the controls you selected in the previous step in place and document all the processes and procedures you need to maintain their operation.

- 4-Assess Security Controls
  Make sure the security controls you implemented are working the way they need to so you can limit the risks to your operation and data.

- 5-Authorize Information Systems
  Are the security controls working correctly to reduce the risk to the organization? Then that control on that system is authorized! Congrats!

- 6-Monitor Security Controls
  Continuously monitor and assess the security controls for effectiveness and make changes during operation to ensure those systems' efficacy. Document any changes,

conduct regular impact analysis, and report security controls' status to your designated officials.

⇨ How Can An Effective Risk Management Framework Benefit A Business?

Though the RMF is a requirement for businesses working with the US Government, implementing an effective risk management system can benefit any companies. The ultimate goal of working toward RMF compliance is the creation of a data and asset governance system that will provide full-spectrum protection against all the cyber risks you face.

More specifically, developing a practical risk management framework will provide a company with several specific benefits:

- Asset Protection:

  An effective risk management framework will prioritize understanding the risks that your business faces to take the necessary steps to protect your assets and your business. This means that a comprehensive risk management framework will help you protect your data and your assets.

- Reputation Management:

  Reputation management is an essential part of modern business practices, and limiting the detrimental consequences of cyber attacks is an integral part of ensuring that your reputation is protected.

- IP Protection:

  Almost every company has intellectual property that must be protected, and a risk management framework applies just as much to this property as your data and assets. If you sell, offer, distribute, or provide a product or service that gives you a competitive edge, you are exposed to potential Intellectual Property theft. A risk management framework helps protect against potential losses of competitive advantage, business opportunities, and even legal risks.

- Competitor Analysis:

  Finally, developing a risk management framework can have beneficial impacts on the fundamental operation of your business. By cataloging the risks you face and taking measures to mitigate them, you will also be gathering a wealth of valuable information on the market that you operate within, and this – in itself – can give you a competitive advantage over your peers.