Risk Management Framework (RMF): An Overview

The Risk Management Framework is a set of criteria for securing US Government IT Systems. In this guide, we'll explain the RMF and how to implement it.

Michael Buckbee 6 min read Last updated October 6, 2023

Contents

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 independ processes and systems. It requires that firms implement secure data governance systems and perform threat modeling to identify cyber risk areas.

In this guide, we'll take you through everything you need to know about the RMF. We'll break dowr the components of the framework in several sections:

What Comprises the Risk Management Framework?

The general concept of "risk management" and the "risk management framework" might appear to quite similar, but it is important to understand the distinction between the two. The risk manageme 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-s 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 800-3 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 cond 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

When getting started with the RMF, it can be useful to break the risk management requirements in different categories. These categories provide a way of working toward an effective risk managem system, from identifying the most critical risks you face to how you will mitigate them.

Risk Identification

The first, and arguably the most important, part of the RMF is to perform risk identification. NIST s “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 syste and then prioritize them using different factors:

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 b 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 specif 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.

Risk Measurement and Assessment

Once you have identified the threats, vulnerabilities, impact, likelihood, and predisposing condition you can calculate and rank the risks your organization needs to address.

Risk Mitigation

Organizations take the previous ranked list and start to figure out how to mitigate the threats from t greatest to the least. At some point in the list, the organization can decide that risks below this leve are not worth addressing, either because there is little likelihood of that threat getting exploited, or there are too many greater threats to manage immediately to fit the low threats into the work plan.

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.

Risk Governance

Finally, 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 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 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.

References: FIPS Publication 199, Standards for Security Categorization of Federal Information a Information Systems; Special Publication 800-60 Rev. 1 (Volume 1, Volume 2), Guide for Mapping Types of Information and Information Systems to Security Categorie

2. Select Security Controls

Select the appropriate security controls from the NIST publication 800-53 to "facilitate a more consistent, comparable, and repeatable approach for selecting and specifying security controls for systems."

References: Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations ed. note the updated version of 800-53 goes into effect on September 2021. Stay tuned for details.

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.

References: Multiple publications provide best practices to implement security controls. Check out this page to search for them.

4. Assess Security Controls

Make sure the security controls you implemented are working the way they need to so you can lim 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 that system is authorized! Congrats!

References: Special Publication 800-37 Rev. 2 Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy

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 analy and report security controls' status to your designated officials.

References: Special Publication 800-37 Rev. 2 Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy

How Can An Effective Risk Management Framework Benefit A Business?

Though the RMF is a requirement for businesses working with the US Government, implementing 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-spect 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. Consumers in the US are increasingly aware of data privacy's importance, not just because US privacy laws are becoming increasingly strict. A data breach will damage your busines reputation. An effective risk management framework can help companies quickly analyze gaps in enterprise-level controls and develop a roadmap to reduce or avoid reputational risks.

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, distribut 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, a this – in itself – can give you a competitive advantage over your peers.

How Can Varonis Help You Be Compliant?

NIST regulation and the RMF (in fact, many of the data security standards and compliance regulations) have three areas in common:

- Identify your sensitive and at risk data and systems (including users, permissions, folders, etc.);
- Protect that data, manage access, and minimize the risk surface;
- Monitor and detect what's happening on that data, who's accessing it, and identify when there is suspicious behavior or unusual file activity.

The Varonis Data Security Platform enables federal agencies to manage (and automate) many of t recommendations and requirements in the RMF.

DatAdvantage and Data Classification Engine identifies sensitive data on core data stores, and ma user, group, and folder permissions so that you can identify where your sensitive data is and who c access it. Knowing who has access to your data is a key component of the risk assessment phase defined in NIST SP 800-53.

Data security analytics helps meet the NIST SP 800-53 requirement to constantly monitor your dat Varonis analyzes billions of events from data access activity, VPN, DNS, and proxy activity, and Active Directory and automatically builds behavioral profiles for each user and device. Machine-learning-powered threat models proactively identify abnormal behavior and potential threats like ransomware, malware, brute force attacks, and, insider threats.

NIST SP 800-137 establishes guidelines to protect your data and requires that the agency meet a least-privilege model. DatAdvantage surfaces where users have access that they might no longe need based. Automation Engine can clean up permissions and remove global access groups automatically. DataPrivilege streamlines permissions and access management by designating dat owners and automating entitlement reviews.

While the Risk Management Framework is complex on the surface, ultimately it's a no-nonsense a logical approach to good data security practices– see how Varonis can help you meet the NIST SP 800-37 RMF guidelines today.