ITL BULLETIN FEBRUARY 2019

The Next Generation Risk Management Framework (RMF 2.0): A Holistic Methodology to Manage Information Security, Privacy and Supply Chain Risk

Victoria Yan Pillitteri
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
U.S. Department of Commerce

NIST SP 800-37 Revision 2 describes the Risk Management Framework (RMF) and provides guidelines for applying the RMF to information systems and organizations. The RMF provides a disciplined, structured, and flexible process for managing security and privacy risk that includes information security categorization; control selection, implementation, and assessment; system and common control authorizations; and continuous monitoring. The RMF also includes activities to prepare organizations to execute the framework at appropriate risk management levels.

Introduction

In today's dynamic ecosystem of interconnected systems and devices in conjunction with the pervasive nature and value of the information from those systems and devices, it is critical to understand and manage the security and privacy risks (including supply chain risks) to organizations, systems, and individuals. It is no longer adequate to treat security and privacy separately as the two disciplines are unequivocally tied together in modern systems; without adequate security, there cannot be adequate privacy and vice versa. NIST Special Publication (SP) 800-37, Revision 2, is the first NIST publication to address security and privacy risk management in an integrated, robust, and flexible methodology applicable to any sector, organization, or type of system.

NIST SP 800-37 Revision 2 develops the next-generation Risk Management Framework (RMF) for systems, organizations, and individuals. The updates include an alignment with the constructs in the NIST Cybersecurity Framework; the integration of privacy risk management processes; an alignment with system life cycle security engineering processes; and the incorporation of supply chain risk management processes.

The Risk Management Framework

The RMF emphasizes risk management by promoting the development of security and privacy capabilities into systems throughout the system development life cycle (SDLC). Implementing the RMF allows organizations to maintain situational awareness of the security and privacy posture by providing near real-time information to facilitate decisions regarding the acceptance of risk to organizational operations and assets, individuals, and other organizations from the use and operation of their systems.

The RMF:

- Provides a repeatable process designed to promote the protection of information and systems commensurate with risk;
- Emphasizes organization-wide preparation necessary to manage security and privacy risks;
- Facilitates the categorization of information and systems, the selection, implementation, assessment, and monitoring of controls, and the authorization of information systems and common controls;
- Promotes the use of automation for near real-time risk management through the implementation of continuous monitoring processes;
- Encourages the use of correct and timely metrics to provide senior leaders with the necessary information to make cost-effective, risk-based decisions;
- Facilitates the integration of security and privacy requirements and controls into enterprise architecture, the SDLC, acquisition processes, and systems engineering processes;
- Connects risk management processes at all levels of the organization (organization, mission/business process and system level); and
- Establishes responsibility and accountability for controls implemented within systems and inherited by those systems.

The RMF is purposefully designed to be technology neutral so that the methodology can be applied to any type of system without modification. While the specific controls selected, control implementation details, and control assessment methods and objects may vary with different types of IT resources, there is no need to adjust the RMF process to accommodate specific technologies.

Figure 1, below, provides an overview of the RMF Steps and other NIST publications that provide implementation guidance and additional information. The seven RMF steps include a new preparatory step to ensure that organizations are ready to execute the process and the other six steps, unchanged from Revision 1 of the RMF. All seven steps are essential for the successful execution of the RMF. The steps are:

- **Prepare** to execute the RMF from an organization-level and a system-level perspective by establishing a context and priorities for managing security and privacy risk.

- **Categorize** the system and the information processed, stored, and transmitted by the system based on an analysis of the impact of loss.
- **Select** an initial set of controls for the system and tailor the controls as needed to reduce risk to an acceptable level based on an assessment of risk.
- **Implement** the controls and describe how the controls are employed within the system and its environment of operation.
- **Assess** the controls to determine if the controls are implemented correctly, operating as intended, and producing the desired outcomes with respect to satisfying the security and privacy requirements.
- **Authorize** the system or common controls based on a determination that the risk to organizational operations and assets, individuals, other organizations, and the Nation is acceptable.
- **Monitor** the system and the associated controls on an ongoing basis to include assessing control effectiveness, documenting changes to the system and environment of operation, conducting risk assessments and impact analyses, and reporting the security and privacy posture of the system.

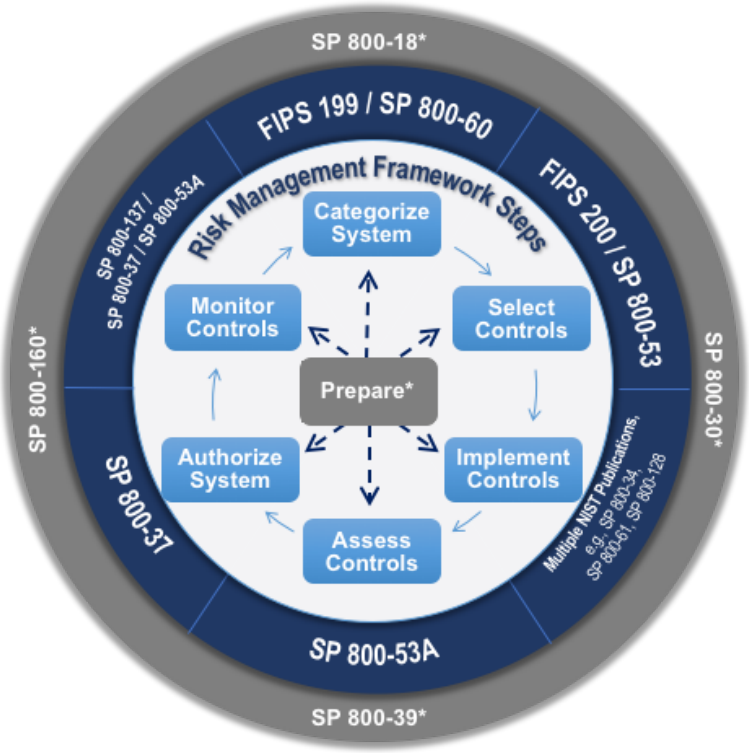

Figure 1. The Risk Management Framework and Supporting Resources for Implementation

Overview of Significant Updates to the RMF

RMF 2.0 is the first NIST publication to include full integration of privacy risk management into the existing information security risk management processes. The update also includes direct references to the Cybersecurity Framework, demonstrating how organizations that implement the RMF also achieve the outcomes of the Cybersecurity Framework.

The addition of the Prepare step is one of the key changes to the RMF—incorporated to achieve more effective, efficient, and cost-effective security and privacy risk management processes. The guidance in the Prepare step was previously part of other existing NIST Special Publications (e.g., SP 800-18, 800-30, 800-39, 800-47, and 800-160), but by incorporating Prepare step tasks into the RMF, organizations have a single, focal resource and methodology to manage security and privacy risk. The Prepare step institutionalizes organization-level and system-level preparation to implement the RMF by facilitating communication across the organizational risk management levels, encouraging organization-wide identification of common controls and the development of organizationally-tailored control baselines, reducing complexity of the IT infrastructure and providing additional methods to identify, prioritize and focus resources on high value assets commensurate with risk.

RMF 2.0 also includes updated guidance on:

- Authorization boundaries, including guidance on authorization boundaries for complex systems and software applications;
- Types of system and control authorizations, to include incorporation of guidance on ongoing authorization (previously published as a white paper), and introduction of the ***authorization to use***, which encourages reciprocity and reuse of existing authorizations;
- Use of automation (where feasible) to increase speed, effectiveness, and efficiency; and
- System life cycle considerations.

Changes to existing RMF steps (Categorize, Select, Implement, Assess, Authorize, and Monitor) were not significant. Additional discussion was added to tasks to address privacy integration and to facilitate implementation. Tasks that were added to existing steps were previously implied in SP 800-37 Rev 1 or other NIST guidance, but are now explicitly identified.

The **seven major objectives** for the RMF 2.0 update:

1. Provide closer linkage and communication between the risk management processes/activities at the C-suite level and the individuals, processes, and activities at the system and operational level;
2. Institutionalize critical risk management preparatory activities;
3. Demonstrate how the **NIST Cybersecurity Framework** can be aligned with the RMF and implemented using established NIST risk management processes;
4. Integrate privacy risk management processes into the RMF to better support the privacy protection needs;
5. Promote the development of trustworthy secure software and systems by aligning with life cycle-based systems engineering processes in **NIST SP 800-160 Volume 1**;
6. Integrate security-related, supply chain risk management (SCRM) concepts into the RMF; and
7. Allow for an organization-generated control selection approach to complement the traditional baseline control selection approach and support the use of the consolidated control catalog in **NIST**

RMF 2.0 Webcast

On Thursday, February 28, 2019, NIST hosted a webcast on NIST Special Publication (SP) 800-37, Revision 2. The webcast featured an overview of the updates in SP 800-37, Revision 2, followed by a deep dive into the Steps and Tasks of the Risk Management Framework, and concluded with a question and answer session. For more information and to access the webcast recording and presentation slides, please visit: https://go.usa.gov/xENcs.

Conclusion

The RMF 2.0 marks the inaugural document in the suite of risk management publications that holistically address managing both security and privacy risk. The updates to the RMF are intended to increase the effectiveness, efficiency, and cost-effectiveness of the RMF by establishing a closer connection to the organization's missions and business functions and improving the communications among senior leaders, managers, and operational personnel. NIST SP 800-37 Revision 2 encourages facilitating a common organization-wide foundation for managing risk, reducing the complexity of the IT

infrastructure using Enterprise Architecture concepts and eliminating unnecessary functions that do not address security and privacy risk, and helps to identify, prioritize, and focus resources on the organization's high value assets commensurate with risk. The fundamental principles described in NIST SP 800-37 Revision 2 result in simplified RMF execution, encourage organizations to identify and use innovative approaches to manage risk, and promote an increase in the level of automation to carry out specific tasks.

Additional Resources

https://csrc.nist.gov/Projects/Risk-Management

ITL Bulletin Publisher: Katherine Green
Information Technology Laboratory
National Institute of Standards and Technology
katherine.green@nist.gov