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.

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

Disclaimer: Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by NIST nor does it imply that the products mentioned are necessarily the best available for the purpose.