Cybersecurity Risk Management

Choosing the Right Approach to Get the Job Done

During the past two decades, the National Institute of Standards and Technology (NIST) has developed a suite of cybersecurity standards and guidelines to help federal agencies manage risk and comply with the Federal Information Security Modernization Act (FISMA) [1].[1] One of NIST's flagship risk management publications, Special Publication (SP) 800-37, *Risk Management Framework for Information Systems and Organizations* [3], has been used by federal agencies to develop and implement their information security programs and to satisfy federal information security requirements. Many federal systems and components are procured "off-the shelf" from the commercial marketplace. For these types of systems, components, and enterprise solutions, the Risk Management Framework (RMF) works extremely well and provides the type of information necessary for federal officials to make credible, risk-based decisions supporting the Authorization to Operate (ATO)[2] process.

Although the NIST RMF and its supporting standards and guidelines are successfully serving the cybersecurity needs of federal agencies for relatively stable enterprise information technology systems, the emergence and growing complexity of cyber-physical systems[3] (e.g., National Aeronautics and Space Administration [NASA] space flight systems), requires an approach in which cybersecurity is tightly integrated into the systems engineering process, as part of the system development life cycle. A "secure-by-design" systems engineering-based approach ensures that there is (1) comprehensive coverage for the full spectrum of cyber-threats to and cyber-attacks against organizational missions; (2) seamless alignment of missions to the engineering lifecycle; and (3) the appropriate context to achieve mission success.

[1] NIST standards and guidelines are referenced in Office of Management and Budget (OMB) *Circular A-130* [2], the overarching governmentwide policy for protecting federal information and information systems.

[2] The ATO is the official management decision given by a senior Federal official or officials to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of controls.

[3] This includes technology components such as Field-Programmable Gate Arrays (FPGA), Application Specific Integrated Circuits (ASIC), Programmable Logic Controllers (PLC), and actuators.

To address this need, NIST developed SP 800-160, Volume 1, *Engineering Trustworthy Secure Systems* [4]. This publication focuses on system life cycle-based security engineering practices and is based on a widely adopted international systems and software engineering standard (ISO/IEC/IEEE 15288) [5]. SP 800-160, Volume 1 includes over four decades of foundational security design principles that are necessary to protect critical systems from hostile adversaries and to ensure those principles have been incorporated early and throughout the system development life cycle. In a similar manner to using the RMF for enterprise systems, the execution of the system life cycle processes described in SP 800-160, Volume 1, can produce the essential information needed by senior Federal officials to make credible, risk-based decisions to authorize the operation of the engineered systems—explicitly accepting the risk to the organization's operations (including missions, functions, image, and reputation), organizational assets, individuals, and the Nation.

There is a need for a process that allows federal agencies to address their cybersecurity requirements and manage risk as part of the system development life cycle process—a process that is understood and implementable by systems engineers and systems security engineers supporting critical organizational missions.

Table 1 provides a high-level comparison of the steps in the NIST RMF and the equivalent system development life cycle processes in NIST SP 800-160, Volume 1. It should be noted that not all system life cycle processes are executed sequentially and some processes (e.g., the System Analysis, Verification, and Validation processes) are carried out numerous times as needed at various stages in the life cycle.

Table 1: Comparison of RMF Steps and System Life Cycle (SLC) Processes

Risk Management Framework NIST SP 800-37	Systems Security Engineering NIST SP 800-160, Volume 1
RMF Step 1: Preparation	**SLC Process: Mission or Business Analysis**
RMF Step 2: Categorize System	**SLC Process: Stakeholder Needs and Requirements Definition**
RMF Step 3: Select Controls	**SLC Process: System Requirements Definition** **SLC Process: System Architecture Definition** **SLC Process: Design Definition** **SLC Process: System Analysis** **SLC Process: Verification** **SLC Process: Validation**
RMF Step 4: Implement Controls	**SLC Process: Implementation** **SLC Process: Integration** **SLC Process: System Analysis** **SLC Process: Verification** **SLC Process: Validation**
RMF Step 5: Assess Controls	**SLC Process: Verification** **SLC Process: Transition** **SLC Process: Validation** **SLC Process: System Analysis**
RMF Step 6: Authorize System	**SLC Process: System Analysis**
RMF Step 7: Monitor System	**SLC Process: Operation** **SLC Process: Maintenance** **SLC Process: System Analysis** **SLC Process: Disposal**

Since systems engineers address cybersecurity problems as part of the overarching mission requirements and reflect security solutions at the system architecture and design level of detail, the information generated during the execution of the life cycle processes, in many cases, can provide additional and more detailed information for authorizing officials. This can also increase the fundamental assurance or trustworthiness in the systems supporting critical organizational missions.

Choosing the right risk management approach and supporting tools is important to ensure that systems are adequately protected, implementors understand how to achieve security solutions in their respective operational environments, and senior officials have sufficient information to make credible risk-based decisions and manage their cybersecurity risks.

REFERENCES

[1] Federal Information Security Modernization Act (P.L. 113-283), December 2014. Available at https://www.govinfo.gov/app/details/PLAW-113publ283

[2] Office of Management and Budget Circular A-130, Managing Information as a Strategic Resource, July 2016. Available at https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/circulars/A130/a130revised.pdf

[3] Joint Task Force (2018) Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-37, Rev. 2. https://doi.org/10.6028/NIST.SP.800-37r2

[4] Ross R, Winstead M, McEvilley M (2022) Engineering Trustworthy Secure Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-160, Vol. 1, Rev. 1. https://doi.org/10.6028/NIST.SP.800-160v1r1

[5] International Organization for Standardization/International Electrotechnical Commission/Institute of Electrical and Electronics Engineers (2023) ISO/IEC/IEEE 15288:2023 – Systems and software engineering – Systems life cycle processes. https://www.iso.org/standard/81702.html