

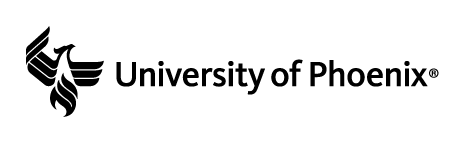
Risk Management Framework



July 13, 2020

Shane Ẽire Byrne

CYB407



**Week 1:Risk Management Framework**

|  |  |  |  |
| --- | --- | --- | --- |
| **NIST Risk Management Framework Step** | **What is the key NIST Special Publication that guides this step?** | **What are the typically deliverables for this step??** | **Who typically works on the deliverables for this step??** |
| **Step 1 : Categorize Information Systems** | •NIST Special Publication 800-30 •NIST Special Publication 800-39 •NIST Special Publication 800-59 •NIST Special Publication 800-60 (Tipton, 2019) | •NIST Special Publication 800-30 provides guidance for conducting risk assessments of federal information systems and organizations (NIST, 2012). •NIST Special Publication 800-30 establishes information on threat sources, threat events, vulnerabilities, and predisposing conditions thus allowing organizations to use such information to categorize information and information systems based on the knowledge of known and potential threats. (NIST, 2012) •NIST Special Publication 800-39 Helps in the establishment and implementation of governance structures that are consistent with strategic goals and objectives of organizations. (NIST, 2011) •NIST Special Publication 800-59 establishes the classification of the system; whether it is to be used in intelligence activities, national security, military, weapons development, or handling of classified information, and if it is applicable to any (Barker, 2003). •NIST Special Publication 800-60 helps in the establishment of the security categorization process, as well as tying it in to agency mission, security programs, IT Management, the role in system development lifecycles, as well as certification and accreditation processes. (Stine, Kissel, Baker, Fahlsing, Gulick, 2008). | •Information security program officer •CISO •Enterprise architects •Individuals involved in capital planning and investment control •Cross-organizational stakeholders •Technical operations personnel CIO |
| **Step 2: Select Security Controls** | •NIST Special Publication 800-30 •NIST Special Publication 800-53 •NIST Special Publication 800-53A (Tipton, 2019) | •NIST Special Publication 800-30 establishment of risk assessment allow for the application of a tailored guidance to adjust the security controls based on the specific mission/business requirements, assumptions, constraints, priorities, trade-offs, or other threat information (NIST, 2012). •NIST Special Publication 800-53 establishes security control identifiers and family names (NIST, 2013). •NIST Special Publication 800-53A establishes that all appropriate policies covering security, privacy control assessments, and any prior steps in the RMF are successfully completed (NIST, 2014). | •Information security program officer. •Enterprise architects •Technical operations personnel •Cross-Organizational Stakeholders. |
| **Step 3: Implement Security Controls** | •NIST Special Publication 800-30 •NIST Special Publication 800-53 •NIST Special Publication 800-53A (Tipton, 2019) | •NIST Special Publication 800-30 establishes risk assessment results to identify alternative implementations of selected security controls. Information technology products, system components, or architectural configuration could possibly be more susceptible to certain types of threat sources, these susceptibilities are address during security control development and implementation (NIST, 2012). •NIST Special Publication 800-53 establishes the designations (common, system-specific-or hybrid) related to said security controls. Also, the scope of applicability for said control, the shared nature of said control, and the responsibility for control development (NIST, 2013). •NIST Special Publication 800-53A address the determination of the assessment team and results of security control assessments as well as privacy control assessments (NIST, 2014).  •NIST Special Publication 800-53 if security controls are assessed to be adequate enough, security-relevant entity will have a predictable manner when satisfying a defined set of security requirements under specified conditions/circumstances and while subjected to disruptions, human errors, component faults, and failures, as well as purposeful attacks that may occur in the environment of operation, a means of trust can be established with the system if it meets expectations for performance (NIST, 2013). | •Information security program officer. •Enterprise architects. •Technical operations personnel. •Cross-Organization Stakeholders. •CISO. |
| **Step 4: Assess Security Controls** | •NIST Special Publication 800-30 •NIST Special Publication 800-53A •NIST Special Publication 800-70 (Tipton, 2019) | •NIST Special Publication 800-30 allows for results from security control assess (documents in security assessment reports) to information risk assessments. Identification of vulnerabilities in organization information systems and the environments in which said systems operate is brought possible through security control assessment (NIST, 2012). •NIST Special Publication 800-53A analyses assessment report results, this being results of security control assessments and privacy control assessments and how they ultimately influence control implementations, the content of security plans, and privacy plans as well as the respective plans of action and milestones (NIST, 2014). •NIST Special Publication 800-70 helps to identify system needs. These being functional needs (what the product of service does for the end user), possible threats and vulnerabilities that can affect the end user, and security needs this being all the controls needed to minimize or eliminate of a threat exercise a vulnerability within the end product (Quinn, Souppaya, Cook, Scarfone, 2018). | •Information security program officer. •Enterprise architects •Technical operations personnel •Cross-Organizational Stakeholders. •CISO. |
| **Step 5: Authorize Information System** | •NIST Special Publication 800-30 •NIST Special Publication 800-39 •NIST Special Publication 800-70 (Tipton, 2019) | •NIST Special Publication 800-30 risk assessment can be presented to authorizing officials; risk responses carried out by the organization based off the risk assessments will establish a security posture of organizational information systems and environments of operation (NIST, 2012). •NIST Special Publication 800-70 establishes security configuration checklists (or lockdown guide, hardening guide, security guide, or security technical implementation guide (STIG) which deals with configuration files, documentation that guides the checklist user to manually configure an IT product, documentation that explains the recommended methods to securely install and configure a device, and the policy or programmatic documents that set fourth guidelines for auditing authentication mechanisms, and perimeter security (Quinn, Souppaya, Cook, Scarfone, 2018). | •Information security program officer. •Enterprise architects •Technical operations personnel •Cross-Organizational Stakeholders. •CISO. •CIO |
| **Step 6: Monitor Security Controls** | •NIST Special Publication 800-30 •NIST Special Publication 800-39 •NIST Special Publication 800-53 •NIST Special Publication 800-137 (Tipton, 2019) | •NIST Special Publication 800-30 leads to the effectiveness of security controls, changes to information systems, and environments of operations as well as compliance with federal legislation, regulations, directives, polices, standards, and guidance when monitoring processes are established (NIST, 2012). •NIST Special Publication 800-53 in conjunction with FIPS Publication 199 allows for the security controls in the information system and environment of operation to be monitored in order to determine control effectiveness, changes to the system/environment, and compliance to legislation, Executive Orders, directives, policies, regulations, and standards (NIST, 2013). •NIST Special Publication 800-39 establishment of risk monitoring provides organizations a means to verify compliance, determine ongoing effectiveness or risk response measures, identify risk-impacting changes to organizational information systems, and environments of operation (NIST, 2011). •NIST Special Publication 800-137 helps to establish an Information Security Continuous Monitoring (ISCM) program. This program is sufficient to inform risk-based decisions and maintain operations within establish risk tolerances. Goals developed include detection of anomalies and changes within the organization's environments of operations and information’s systems, visibility into assets, and awareness of vulnerabilities, knowledge of threats, and frequencies determined to ensure the information needed to manage risk to within organizational risk tolerances is available (Dempsey, Chawla, Johnson, Johnson, Orebaugh, Scholl, Stine, 2011). | •Information security program officer. •Enterprise architects •Technical operations personnel •Cross-Organizational Stakeholders. •CISO. •CIO. |

**References**

Barker, W. (August 2003) Guide for Identifying an Information System as a National Security System

Retrieved from <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-59.pdf>

Center for Development of Security Excellence (CDSE) (2020) Risk Management Framework Retrieved from <https://www.cdse.edu/documents/student-guides/CS102-guide.pdf>

Dempsey, K., Chawla, N., Johnson, A., Johnson, R., Jones, A., Orebaugh, A., Scholl, M., Stine, K. (September 2011) Information Security Continuous Monitoring (ISCM)

for Federal Information Systems and Organizations Retrieved from <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-137.pdf>

EC-Council. (2020 ). CYB/405 (Domain 1) - Governance and Risk Management, 3rd Edition. [[VitalSource Bookshelf version]]. Retrieved from vbk://9781635674064

EC-Council. (2020 ). CYB/407 (Domain 2) - Information Security Controls, Compliance, and Audit Management, 3rd Edition. [[VitalSource Bookshelf version]].

Retrieved from vbk://9781635674071

National Institute of Standards and Technology (NIST) (April 2013) Security and Privacy Controls for Federal Information Systems and Organizations

Retrieved from <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf>

National Institute of Standards and Technology (NIST) (December 2014) Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building

Effective Assessment Plans Retrieved from <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf>

National Institute of Standards and Technology (NIST) (March 2011) Managing information Security Risk: Organization, Mission, and Information System

View Retrieved from <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf>

National Institute of Standards and Technology (NIST) (March 2011) Managing information security Risks: Organization, Mission, and Information System View

Retrieved from <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf>

National Institute of Standards and Technology (NIST) (September 2012) Guide for Conducting Risk Assessments

Retrieved from <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf>

Quinn, S., Souppaya, M., Cook, M., Scarfone, K. (February 2018) National Checklist Program for IT Products—Guidelines for Checklist Users and Developers

Retrieved from <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-70r4.pdf>

Rogers, B. E., Dunkerley, D. (2015). CRISC Certified in Risk and Information Systems Control All-in-One Exam Guide. [[VitalSource Bookshelf version]].

Retrieved from vbk://1260118088

Shanthamurthy, D. (Aug 05, 2011) NIST SP800-30 standard for technical risk assessment: An evaluation

Retrieved from <https://www.computerweekly.com/tip/NIST-SP-800-30-standard-for-technical-risk-assessment-An-evaluation>

Stine, K., Kissel, R., Barker, W., Fahlsing, J., Gulick, J (August 2008) Guide for Mapping Types of Information and Information Systems to Security Categories

Retrieved from <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-60v1r1.pdf>

Tipton, S. (Dec 10, 2019) How to Apply the Risk Management Framework (RMF)

Retrieved from <https://www.tripwire.com/state-of-security/featured/applying-risk-management-framework/>