# Final Project

Veeraiah Nannapaneni

University of San Diego

CSOL 530 Cyber Security Risk Management

Summer 2019

## Table of Contents

In this white paper, I will discuss how the Risk Management Framework (RMF) is used to secure the Supply Chain Management (SCM) system by applying each of the RMF steps – categorize, select, implement, assess, authorize, and monitor.

## Risk Management Framework

### Categorize

Security categorization is the first step in the RMF. “The purpose of the Categorize step is to inform organizational risk management processes and tasks by determining the adverse impact to organizational operations and assets, individuals, other organizations, and the Nation with respect to the loss of confidentiality, integrity, and availability of organizational systems and the information processed, stored, transmitted by those systems.” (“Risk Management Framework,” 2018).

The SCM system involves the purchasing, tracking, and overall management of goods and services by external providers to carry out missions and business functions (Stine, Kissel, Barker, Lee, & Fahlsing, 2018).

**Information types for the SCM system**. The SCM system consists of four information types.

- Goods acquisition deals with the procurement of physical goods, products, and capital assets to be used by the Federal government.
- Inventory control refers to the tracking of information related to procured assets and resources with regards to quantity, quality and location.
- Logistic management involves the planning and tracking of personnel and their resources in relation to their availability and location.
- Service acquisition involves the oversight and/or management of contractors and service providers from the private sectors (Stine et al., 2008).

**Provisional Impact Level.** To establish an appropriate security category of an information type essentially requires determining the potential impact for each security objective (i.e., Confidentiality, Integrity and Availability) associate with the SCM system information types (“FIPS PUB 199,” 2004).

$SC_{\text{goods acquisition}}$ = {(confidentiality, LOW), (integrity, LOW), (availability, LOW)}.

$SC_{\text{inventory control}}$ = {(confidentiality, LOW), (integrity, LOW), (availability, LOW)}.

$SC_{\text{logistic management}}$ = {(confidentiality, LOW), (integrity, LOW), (availability, LOW)}.

$SC_{\text{service acquisition}}$ = {(confidentiality, LOW), (integrity, LOW), (availability, LOW)}.

**Security categorization applied to information system.** The security categorization of the SCM information system is the high water mark of the provisional impact levels of each information type (“FIPS PUB 199,” 2004).

$SC_{\text{supply chain management system}}$ = {(confidentiality, LOW), (integrity, LOW), (availability, LOW)}.

**Justification.** My justification for the impact is as follows.

***Confidentiality.*** The effect of unauthorized disclosure of the information types of the system; goods acquisition information, inventory control information, logistics management information, and services acquisition information are likely to have a limited adverse effect on agency operations, agency assets or individuals. The recommended provisional impact level for all four information types of the confidentiality security objective is low (Stine et al., 2008).

***Integrity.*** The effect of unauthorized modification or destruction of information effecting external publication of goods acquisition information, inventory control information, logistics management information, and services acquisition (e.g. web pages, and electronic mail) may adversely affect public confidence in the agency. However, damage to the mission would usually be limited. The recommended provisional impact level for all four information types is low (Stine et al., 2008).

***Availability.*** The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish access to goods acquisition information, inventory control information, logistics management information, and services acquisition information. Functions and processes supported by most of the four information types are tolerant of delays. Typically, disruption of access to the four information types will have a limited adverse effect on agency operations, agency assets, or individuals. There are some special factors affecting availability impact determination. One example is when there are delays in goods procurement or distribution of materials necessary to support disasters. The result of this may be loss of life. In such cases, the impact level for goods acquisition, and inventory control information needed to respond to emergencies will be high. The provisional impact level of the availability security objective for all four information types is low (Stine et al., 2008).

## Select

Security control selection is the second step in the RMF. I will discuss the security controls selection for the SCM system by selecting and tailoring a set of baseline controls based on the security categorization impact levels of each security objective: confidentiality, integrity, and availability of organizational systems and the information processed, stored, and transmitted by those systems (“Risk Management Framework,” 2018). I will then provide my justification for each of the security controls.

The NIST SP 800-53 discusses three types of security and privacy controls; a) common controls; (b) system-specific controls; and (c) hybrid controls. The control types determine the extent of applicability of the control, the common nature or inheritability of the control, and the accountability for control development, implementation, assessment, and authorization ("Security and Privacy Controls," 2017).

The SCM system is classified as a low-impact system.  According to the NIST SP 800-53 Rev. 4, a low-impact system has 115 security controls belonging to following security control families: Access Control (AC), Awareness and Training (AT), Audit and Accountability (AU), Security Assessment and Authorization (CA), Configuration Management (CM), Contingency Planning (CP), Identification and Authentication (IA), Incident Response (IR), Maintenance (MA), Media Protection (MP), Physical and Environmental Protection (PE), Planning (PL), Personnel Security (PS), Risk Assessment (RA), System and Services Acquisition (SA), System and Communications Protection (SC), and System and Information Integrity (SI) ("NIST Special Publication 800-53 (Rev.4)," n.d). For this paper I am limiting my discussion to three control families.

**Security controls.** According to the NIST SP 800-37 Risk Management Framework, "The purpose of the Select step is to select, tailor, and document the controls necessary to protect the information system and organization commensurate with risk to organizational operations and assets, individuals, other organizations, and the Nation." ("Risk Management Framework," 2018).

***Access* controls *(AC).*** Only authorized users are required to have access to an information system that contains programs, processes or other systems. The reason for selecting the AC family is to control access to the information system's resources ("FIPS PUB 200," 2006).

***Identification and* authentication (IA).** The SCM system should appropriately identify information system users, processes operating on behalf of users or devices, and authenticate the identities of those users, processes, or devices, as a prerequisite to allowing access to the SCM system ("FIPS PUB 200," 2006). IA has 11 controls associated with it, but only seven controls are related to the low-impact system ("Security and Privacy Controls," 2017. pp. 336, 337).

***Physical and Environmental Protection (PE).*** PE controls access to physical systems and buildings where the information systems are stored. Security controls within the PE family can control the intensity, frequency, and randomness of security checks to decrease the risk associated with exfiltration ("FIPS PUB 200," 2006).

**Justification.** Since the SCM system is a low-impact system, there is no need for any tailored baseline controls. My justification for choosing the above security controls is as follows.

***Confidentiality.*** The effect of unauthorized access or disclosure of goods acquisition, inventory control, logistics management, and services acquisition information systems can have a limited adverse effect ("FIPS Pub 199," 2004). In order to mitigate the risk, I selected the baseline security controls that are appropriate to control, identify and authenticate users and devices to the SCM system.

***Integrity.*** Unauthorized modification or destruction of information may result in limited disruption of procurement and operations ("FIPS Pub 199," 2004). In order to mitigate the risk, I selected access control, configuration management, and system and information integrity security controls.

***Availability.*** The impact on availability of the SCM system does not always have the same level of impact as confidentiality and integrity since there are some cases where delays in goods procurement or distribution of materials are necessary to support disasters. Since this is a low-impact system, the baseline controls are all that are needed to mitigate the risk.

## Implement

Security control implementation is the third step in the RMF. "The purpose of the Implement step is to implement the controls in the security and privacy plans for the system and for the organization and to document in a baseline configuration, the specific details of the control implementation." ("Risk Management Framework," 2018).

The three security control families from the RMF I will discuss are Access Controls (AC), Identification and Authentication (IA), and Physical and Environmental Protection (PE). I will select security controls from each control family and explain how they are to be implemented.

**Access controls (AC).** To control access to the information system the following security controls need to be implemented:

***AC-2 account management.***

- Establish and document the types of system accounts allowed for use within the system in support of organizational missions and business functions;
- Require approvals by appropriate organizational personnel for requests to create system accounts;
- Identify authorized users of the system, group and role membership, and access authorizations and other attributes for each account;
- Create, enable, modify, disable, and eliminate system accounts following organizations policy and procedures.
- Advise account managers when (a) accounts are no longer required; (b) users are terminated or transferred; (c) system usage changes for an individual ("Security and Privacy Controls," 2017).

*Implementation***.** System owners, the business owner, or the chief information security officer are responsible for approving the request for administrative privileges on system accounts. Accounts created for the temporary or emergency purpose should be intended for short-term use. Accounts that are no longer in use or when the individuals are terminated need to be deactivated or removed from the systems ("Security and Privacy Controls," 2017).

***Identification and authentication (IA).*** To identify and authenticate the users or devices, the following security controls need to be implemented.

***IA-2 identification and authentication (organizational users).***

- Implement multifactor authentication for access to privileged and non-privileged accounts.
- Provide a single sign-on capability for system accounts and services.

*Implementation.* Identification and authentication are achieved by using passwords, physical authenticators, or biometrics. Single sign-on enables users to access multiple resources without prompting authentication for each system. It will also allow adding multifactor authentication to improve system security ("Security and Privacy Controls," 2017).

***IA-3 device identification and authentication.***

- Authenticate devices before establishing a connection using bidirectional authentication that is cryptographically based.
- Identify and authenticate devices based on its configuration and known operating state.

*Implementation.* Device identification and authentication on local and wide area networks can be achieved by using IEEE 802.1x and Extensible Authentication Protocol (EAP), RADIUS server with EAP-Transport Layer Security (TLS) authentication, and Kerberos ("Security and Privacy Controls," 2017).

**Physical and environmental protection (PE).** To control access to physical systems and buildings, the following security controls need to be implemented.

***PE-2 physical access authorizations.***

- Develop, adopt, and maintain a list of people with authorized access to the facility where the system resides;
- Remove individuals from the facility access list when access is no longer needed.

*Implementation***.** Physical access authorization includes badges, identification cards, and smart cards. The strength of authorization credentials is based on organizational policies and standards. PE-2 control applies only to the areas within facilities that are not designated as publicly accessible (“Security and Privacy Controls,” 2017).

***PE-3 physical access control.***

- Verify personal access authorization before granting access to the facility.
- Maintain physical access audit logs for entry/exit points.
- Escort visitors and monitor visitor activity.
- Secure keys, combinations, and other physical access devices.

*Implementation***.** The PE-3 control applies to employees and visitors. Physical access control is implemented per organizational policies and standards. Organizations have flexibility in implementing the type of audit logs, and these can be procedural, automated or some combination thereof (“Security and Privacy Controls,” 2017).

## Assess

Security control assessment is the fourth step in the RMF. “The purpose of the Assess step is to determine if the controls selected for implementation are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security and privacy requirements for the system and the organization.” (“Risk Management Framework,” 2018).

In this step I will assess the security controls from each control family that were implemented on the SCM system. They are AC-2 account management, IA-2 identification and authentication (organizational users) and PE-3 physical access control. And provide a plan of action and milestones for any remediation of noncompliant security controls that are required.

**AC-2 account management.** Identify authorized users of the system, group and role membership, and access authorizations and other attributes for each account ("Security and Privacy Controls," 2017).

***Assessment.*** The assessment objective of the control is to determine if the organization has the following specifics for each account: (a) authorized users of the information systems; (b) group and role membership; and (c) access authorizations such as privileges ("Joint Task Force Transformation Initiative," 2014, pp. F-5, F-6). I used the examine assessment method to assess the control and chose basic examination for both depth and coverage attributes. The following objects were examined: (a) list of active system accounts along with the name of the individual associated with each account; (b) list of conditions for group and role membership; (c) access authorization records; (d) notifications or records of recently transferred, separated, or terminated employees ("Joint Task Force Transformation Initiative," 2014, p. F-6).

As a result of the assessment, I found one noncompliant security control which is related to authorized access to the SCM system. A user account had access to the system for more than a week after the employee was terminated. To remediate and to make sure this type of mistake does not happen again in the future, the employee exit procedure has been updated to ensure that all the user accounts belonging to a terminated employee are disabled.

**IA-2 identification and authentication (organizational users).** Implement multifactor authentication for access to privileged and non-privileged accounts ("Security and Privacy Controls," 2017).

***Assessment.*** The assessment objective of the control is to "determine if the information system implements multi-factor authentication for network access to privileged and non-privilege accounts" (Joint Task Force Transformation Initiative, 2014, p. F-149). I used the examine method to assess the control, and for the attributes, I used the basic examination for both depth and coverage. The objects I examined are: (a) identification and authentication policy; (b) procedures addressing user identification and authentication; (c) information system design documentation; (d) information system configuration settings and associated documentation; (e) information system audit records (Joint Task Force Transformation Initiative, 2014, p. F-149). The result of the assessment found that the control is in compliance.

**PE-3 physical access control.** Verify individual access authorization before granting access to the facility ("Security and Privacy Controls," 2017).

***Assessment.*** The assessment objective of the control is to determine if the organization enforces physical access authorizations at each entry/exit points to the facility where the information system lives. (Joint Task Force Transformation Initiative, 2014, p. F-216). I used the examine method to assess the control, and for the attributes, I used the basic examination for both depth and coverage. The objects I examined are: (a) physical access control logs or records; (b) inventory records of physical access control devices; (c) list of security safeguards controlling access to designated publicly accessible areas within the facility. As a result of the assessment, I found that the security control is in compliance.

**Plan of actions & milestones (POA&M).** The initial remediation plan for AC-2 is to revoke the access of user accounts which are inactive or that belong to terminated or transferred employees to be completed within two days. The long-term plan is to review the employee exit and transfer procedures and update them is necessary to ensure user accounts are deactivated or updated with appropriate access controls to be completed within three weeks. Once the initial and long-term remediation plan is completed, the AC-2 control will be reassessed.

## Authorize

Security control authorization is the fifth step in RMF. "The purpose of the Authorize step is to provide organizational accountability by requiring a senior management official to determine if the security and privacy risk (including supply chain risk) to organizational operations and assets, individuals, other organizations, or the Nation based on the operation of a system or the use of common controls, is acceptable." ("Risk Management Framework," 2018).

In the assessment step of the RMF, I discussed how the security controls are assessed, and now I will provide a plan of action and milestones (POA&M) for any initial and long-term remediation of noncompliant security controls. I will then provide my recommendation for an authorization decision.

**Plan of actions & milestones.** The initial remediation plan for AC-2 is to revoke the access of user accounts which are inactive or that belong to terminated or transferred employees. This was completed within the five-day timeline. The long-term plan is to review the employee exit and transfer procedures and update them if necessary, to ensure user accounts are deactivated or updated with appropriate access controls. The long-term plan was completed within the three-week timeline. The AC-2 control was then reassessed, and it was determined that it was in compliance.

**Recommendation for Authorization Decision.** The initial and long-term remediation plans have been completed, and the AC-2 control has been determined to be in compliance. I have determined that the risk to the SCM system's operations, assets, and individuals is acceptable. As the Authorizing Official (AO), I recommend an authorization to operate (ATO).

## Monitor

Information security continuous monitoring (ISCM) is the sixth step in the RMF. "The purpose of the Monitor step is to maintain an ongoing situational awareness about the security and privacy posture of the information system and the organization in support of risk management decisions." ("Risk Management Framework," 2018).

Continuous monitoring addresses the security impacts on the SCM system resulting from changes to the hardware, software, firmware, or the operational environment. The goal is to determine if the security controls implemented in the system remain to be effective over time in light of the unavoidable changes that occur in the system as well as in the environment in which the system operates (“CSOL 530 Cyber Security Risk Management,” n.d).

Information systems and its environment of operation are in a constant state of change with changes to technology or machine elements, human elements, and physical or environmental elements. Therefore, we need a process to constantly assess the security controls that impact the security and privacy posture of the system and update the security and privacy plans, security and privacy assessment plans, and POA&M. An effective continuous monitoring process includes:

- Monitor the information system and its environment of operation for changes that impact the security and privacy posture of the system.
- Ongoing assessment of the control effectiveness is part of the continuous monitoring activity, after an initial system or common control authorization. Each control may have its own monitoring frequency based on a continuous monitoring strategy.
- Respond to risk based on the results of ongoing monitoring activities, risk assessments, and outstanding items in POA&M.
- Update plans, assessment reports, and POA&M based on the results of the continuous monitoring process
- The results of monitoring activities are documented and reported to the authoring official and other selected organizational officials on an ongoing basis following the organizational continuous monitoring strategy.

- To employ an ongoing authorization approach, review the organization-level and system-level continuous monitoring process to assess implemented controls on an ongoing basis.
- When a system is removed from operation, execute necessary actions that are implemented in the system disposal strategy ("Risk Management Framework," 2018).

## References

CSOL 530 Cyber Security Risk Management. (n.d). Retrieved from https://learn-us-east-1-prod-fleet01-xythos.s3.us-east-1.amazonaws.com/5c2103143e6a3/1020322?response-content-disposition=inline%3B%20filename%2A%3DUTF-8%27%27Continuous_Monitoring.pdf&response-content-type=application%2Fpdf&X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Date=20190826T041036Z&X-Amz-SignedHeaders=host&X-Amz-Expires=21600&X-Amz-Credential=AKIAIBGJ7RCS23L3LEJQ%2F20190826%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Signature=02a066a0bed4254cc7bbe04fc131f341e8faafad3e7fd5a4f3ee99b80e81da8e

FIPS Pub 199: Standards for Security Categorization of Federal Information and Information Systems. (2004, February). Retrieved from https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf

FIPS PUB 200. Minimum Security Requirements for Federal Information and information Systems. (2006, March). Retrieved from https://csrc.nist.gov/csrc/media/publications/fips/200/final/documents/fips-200-final-march.pdf

Joint Task Force Transformation Initiative. (2014, December). NIST Special Publication 800-53A Revision 4, Assessing Security and Privacy Controls in Federal Information Systems and Organizations. Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf

NIST Special Publication 800-53 (Rev.4). (n.d). Retrieved from https://nvd.nist.gov/800-53/Rev4/impact/low

Risk Management Framework for information Systems and Organizations. (2018, December).

Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf

Security and Privacy Controls for Information Systems and Organizations. (2017, August). Retrieved from https://csrc.nist.gov/CSRC/media//Publications/sp/800-53/rev-5/draft/documents/sp800-53r5-draft.pdf

Stine, K., Kissel, R., Barker, W., Lee, A., & Fahlsing, J. (2018, August). Volme II: Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories. Retrieved from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-60v2r1.pdf