RMF Implement Step

Student Guide

May 2023

Center for Development of Security Excellence

Table of Contents

Course Introduction

Introduction

Welcome to the Risk Management Framework, or RMF, Implement Step.

This course focuses on the Implement Step, and by the end of the course, you will be able to define the Implement 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.

Objectives

Before you begin, consider the following course learning objectives.

- Identify Policies and guidelines for the Implement Step in the RMF
- Identify the two tasks and associated inputs, outputs, roles and responsibilities in the Implement Step.

Lessons:

The course is divided into two lessons:

Lesson 1: Policies and Guidelines

Lesson 2: Tasks, Potential Inputs & Expected Outputs, Roles and Responsibilities

Lesson 1: Introduction to Policies and Guidelines

Lesson Introduction

The RMF was developed as a result of a partnership between the National Institute of Standards and Technology, or NIST, the Department of Defense, or DOD, the Office of the Director of National Intelligence, or ODNI, and the Committee on National Security Systems.

In this lesson, you will learn the defining aspects of the Implement Step, and the associated policies and guidelines.

NIST Special Publication (SP) 800-37 Revision 2, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, describes the RMF and provides guidelines for managing security and privacy risks and applying the RMF to information systems and organizations.

DODI 8510.01: **Risk Management Framework (RMF) for DOD Information Technology (IT)** establishes the use of the RMF, an integrated enterprise and integrates DOD mission areas, or MAs, in accordance with Department of Defense Directive (DODD) 8115.01.

NIST SP 800-53 Rev 5: **Security and Privacy Controls for Information Systems and Organizations** establishes controls for systems and organizations. The controls can be implemented within any organization or system that processes, stores, or transmits information. The use of these controls is mandatory for federal information systems in accordance with Office of Management and Budget Circular A-one hundred thirty or OMB A-130, and the provisions of the Federal Information Security Modernization Act, or FISMA, which requires the implementation of minimum controls to protect federal information and information systems.

NIST SP 800-160 Volume 1 Revision 1: Engineering Trustworthy Secure Systems

The purpose of this publication is:

- To provide a basis to formalize a discipline for systems security engineering in terms of its principles, concepts, and activities.
- To foster a common mindset to deliver security for any system regardless of its scope, size, complexity, or stage of the system life cycle
- to provide considerations and to demonstrate how systems security engineering principles, concepts, and activities can be effectively applied to systems engineering activities
- To advance the field of systems security engineering by promoting it as a discipline that can be applied and studied

- To serve as a basis for the development of educational and training programs, including the development of individual certifications and other professional assessment criteria.

NIST SP 800-30 Revision 1: **Guide for Conducting Risk Assessments**

The purpose of Special Publication 800-30 is to provide guidance for conducting risk assessments of federal information systems and organizations, amplifying the guidance in Special Publication 800-39.

Risk assessments, carried out at all three tiers in the risk management hierarchy, are part of an overall risk management process—providing senior leaders and executives with the information needed to determine appropriate courses of action in response to identified risks. In particular, this document provides guidance for carrying out each of the steps in the risk assessment process (i.e., preparing for the assessment, conducting the assessment, communicating the results of the assessment, and maintaining the assessment) and how risk assessments and other organizational risk management processes complement and inform each other.

Special Publication 800-30 also provides guidance to organizations on identifying specific risk factors to monitor on an ongoing basis so that organizations can determine whether risks have increased to unacceptable levels (i.e., exceeding organizational risk tolerance) and whether different courses of action should be taken.

Review Activity

Knowledge Check 1

Select all that apply.

Which document establishes controls for systems and organizations?

○ a) NIST SP 800-53 Rev 5 - Security and Privacy Controls for Information Systems and Organizations

○ b) FIPS 199 – Standards for Security Categorization of Federal Information and Information Systems

○ c) NIST SP 800-60v2 Rev 1 Guide for Mapping types of Information and Information systems to Security Categories: Appendices

○ d) OMB FEA – Federal Enterprise Architecture

Lesson 1 Conclusion

Lesson Conclusion

You have completed this lesson. You should now be able to define Policy and Guidelines associated with the Implement Step.

Lesson 2: Tasks, Inputs and Outputs, Roles and Responsibilities

Introduction of Tasks

In this lesson, we will look at the Tasks, Inputs and Outputs, Roles and Responsibilities outlined in the Implement. The Implement Step includes two Tasks that have an alpha designator of **"I"** preceding the task number.

Task I-1: Control Implementation

Task I-2: Update Control Implementation Information

Each task contains a set of inputs that are required to implement the tasks, inputs, and a set of expected outputs as a result.

The first Implement Step to be discussed is Task I-1.

Task I-1: Control Implementation

Organizations implement the controls as described in the security and privacy plans.

The control implementation is consistent with the organization's enterprise architecture, associated security, and privacy architectures.

Organizations use best practices when implementing controls, including systems security and privacy engineering methodologies, concepts, and principles.

Task I-1 Risk Assessments

Risk assessments guide and inform decisions regarding the cost, benefit, and risk trade-offs in using different technologies or policies for control implementation.

Risk assessments may determine how gaps in security or privacy requirements between system and common controls affect the risk associated with the system.

Organizations also ensure that mandatory configuration settings are established and implemented on system elements in accordance with federal and organizational policies.

For additional guidance on risk assessments, view the NIST SP 800-30 Revision 1: Guide for Conducting Risk Assessments.

When organizations have no direct control over what controls are implemented in a system element, for example, in commercial off-the-shelf products, organizations consider the use of system elements that have been tested, evaluated, or validated by approved, independent, third-party assessment facilities.

For example, NIST Cryptographic Module Validation Program Testing Laboratories, and the National Information Assurance Partnership Common Criteria Testing Laboratories.

The tests, evaluations, and validations consider products in specific configurations and in isolation. Control implementation addresses how the product is integrated into the system while preserving security functionality and assurance.

Task I-1 Assurance Requirements

Organizations also address, where applicable, assurance requirements when implementing controls. *Assurance requirements* are directed at the activities that control developers and implementers carry out to ***increase the level of confidence*** that the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security and privacy requirements for the system. The assurance requirements address quality of the design, development, and implementation of the controls.

Task I-1 Common Controls

A Common control is a security or privacy control that is inherited by multiple information systems or programs.

For the common controls inherited by the system, systems security, and privacy engineers, with support from system security and privacy officers, coordinate with the common control provider to determine the most appropriate way to implement common controls.

System owners can refer to the authorization packages prepared by common control providers when making determinations regarding the adequacy of common controls inherited by their systems.

During implementation, it may be determined that common controls previously selected to be inherited by the system do not meet the specified security or privacy requirements for the system.

For common controls that do not meet the requirements for the system inheriting the controls, or when common controls have unacceptable deficiencies, the system owners identify compensating or supplementary controls to be implemented.

System owners can supplement the common controls with system-specific or hybrid controls to achieve the required protection for their systems or they can accept greater risk with the acknowledgement and approval of the organization.

Task I-1 Potential Inputs

The Potential Inputs for Task I-1 include:

- Approved security and privacy plans

- System design documents
- Organizational security and privacy policies and procedures
- Business impact or criticality analyses
- Enterprise architecture information
- Security architecture information
- Privacy architecture information
- List of security and privacy requirements allocated to the system
- System elements; and environment of operation
- System element information
- System component inventory
- Organization- and system-level risk assessment results

Task I-1 Expected Outputs

The expected outputs for Task I-1 is the Implemented Controls

Task I-1 Roles and Responsibilities

The primary responsibilities are carried out by the ***System Owner and the Common Control Provider.***

The System Owner is an organizational official responsible for the procurement, development, integration, modification, operation, maintenance, and disposal of a system. The system owner is responsible for addressing the operational interests of the user community and for ensuring compliance with security requirements.

The Common Control Provider is an individual, group, or organization that is responsible for the implementation of common controls. The Common Control Providers are responsible for ensuring the documentation of organization-defined common controls in security and privacy plans; and ensuring that required assessments of the common controls are conducted by qualified assessors with an appropriate level of independence.

The Supporting Roles include the Information Owner or Steward, the Security Architect, the Privacy Architect, the Systems Security Engineer, the Privacy Engineer, the System Security Officer, the System Privacy Officer, the Enterprise Architect, and the System Administrator.

Review Activity

Knowledge Check 2

Try answering this question.

Organizations implement the controls from which documents?

- a) Security and Privacy Plans
- b) Systems Elements
- c) System Design Document and System Description
- d) Tailored Controls for the System and Environment of Operations

Task I-2: Update Control Implementation Information

Despite the control implementation details in the security and privacy plans and the system design documents, it is not always feasible to implement controls as planned.

Therefore, as control implementations are carried out, the security and privacy plans are updated with as-implemented control implementation details.

Task I-2 Details

The updates include revised descriptions of implemented controls including changes to planned inputs, expected behavior, and expected outputs with sufficient detail to support control assessments.

Documenting the "as implemented" control information is essential to providing the capability to determine when there are changes to the controls, whether those changes are authorized, and the impact of the changes on the security and privacy posture of the system and the organization.

Task I-2 Potential Inputs

Potential Inputs include:

- Security and Privacy Plans
- Information from Control implementation Efforts

Task I-2 Expected Outputs

The Expected Outputs include:

- Security and Privacy Plans updated with implementation detail sufficient for use by assessors
- System configuration baseline

Task I-2 Roles and Responsibilities

The Primary Responsibilities are carried out by the ***System Owner*** and the ***Common Control Provider.***

The System Owner is an organizational official responsible for the procurement, development, integration, modification, operation, maintenance, and disposal of a system. In coordination with the system security and privacy officers, the system owner is responsible for the development and maintenance of the security and privacy plans and ensures that the system is operated in accordance with the selected and implemented controls.

The Common Control Provider is an individual, group, or organization that is responsible for the implementation, assessment, and monitoring of common controls, which are controls inherited by organizational systems.

Security and privacy plans, security and privacy assessment reports, and plans of action and milestones for common controls are made available to the system owners of systems inheriting common controls after the information is reviewed and approved by the authorizing officials accountable for those common controls.

The Supporting Roles for Task I-2 include:

- Information Owner or Steward
- Security Architect
- Privacy Architect
- System Security Engineer
- Privacy Engineer
- System Security Officer
- Enterprise Architect
- System Administrator

Review Activity

Knowledge Check 3

Try answering this question.

Why is documenting the “as-implemented” control information essential?

○ a) Documenting identifies when the changes occurred
○ b) Documenting identifies authorized changes
○ c) Documenting identifies the impact of changes on the system and the organization
○ d) Documenting ensures and verifies there is no conflict of interest

You have completed this lesson. You should now be able to define:

- Implement Step Tasks
- Potential Inputs and Expected Outputs
- Roles and Responsibilities associated with each Task.

Course Conclusion

Conclusion

Congratulations, you have completed the RMF Implement Step course.

You should now be able to

- Identify Policies and guidelines for the Implement Step in the RMF
- Identify the two tasks and associated inputs, outputs, roles and responsibilities in the Implement Step.

For more information on the RMF Implement Step, please visit the Course Resources link.

To receive credit for this course, you must take the course examination.

Appendix A: Answer Key

Lesson 1: Review Activity

Knowledge Check 1

Select all that apply.

Which document establishes controls for systems and organizations?

☒ a) NIST SP 800-53 Rev 5 - Security and Privacy Controls for Information Systems and Organizations
☐ b) FIPS 199 – Standards for Security Categorization of Federal Information and Information Systems
☐ c) NIST SP 800-60v2 Rev 1 Guide for Mapping types of Information and Information systems to Security Categories: Appendices
☐ d) OMB FEA – Federal Enterprise Architecture

Feedback: *NIST SP 800-53 Rev 5 Security and Privacy Controls for Information Systems and Organizations*

Lesson 2: Review Activity

Knowledge Check 2

Select the correct response.

Organizations implement the controls from which documents?

☒ a) Security and Privacy Plans
☐ b) Systems Elements
☐ c) System Design Document and System Description
☐ d) Tailored Controls for the System and Environment of Operations

Feedback: *Security and Privacy Plans*

Knowledge Check 3

Select all that apply.

Why is documenting the "as-implemented" control information essential?

☒ a) Documenting identifies when the changes occurred
☒ b) Documenting identifies authorized changes
☒ c) Documenting identifies the impact of changes on the system and the organization
☐ d) Documenting ensures and verifies there is no conflict of interest

Feedback:

Documenting identifies when the changes occurred.

Documenting identifies authorized changes.

Documenting identifies the impact of changes on the system and the organization.