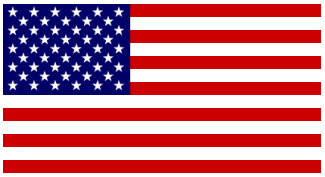


USAID
FROM THE AMERICAN PEOPLE

USAID Trade Project

Risk Management Framework for Information Technology Systems

USAID Trade Project
USAID/Pakistan
Office of Economic Growth & Agriculture
Contract Number: EEM-I-03-07-00005

August 2014

Table of Contents

List of Figures and Tables

Terms, Acronyms, and Initialisms

Terms, Acronyms, Abbreviations	Definition
FBR	Federal Board of Revenue
NIST	National Institute for Standards and Technology: The U.S federal technology agency that works with industry to develop and apply technology, measurements, and standards
POA&M	Plan of Actions and Milestones: A document with discovered system vulnerabilities, actions to be taken to address these weaknesses and the timelines for taking actions.
PRAL	Pakistan Revenue Automation Limited: A Private Limited Company, wholly owned by the Federal Board of Revenue, which provides tax and revenue collection solutions.
RMF	Risk Management Framework: A framework developed by the NIST to manage and mitigate risks and provide security controls for Information Systems.
RSD	Requirements Specification Documents: A document produced as part of the Software Development Lifecycles initiation and definition phases which describes what the system functions are and how they satisfy business requirements.
SAR	Security Assessment Report: A document produced as part of the RMF six phases which details the findings of the security controls assessment and is used by the official responsible for authorizing the system.
SDLC	Software Development Lifecycle: A methodical approach to initiating, developing, implementing, monitoring, and decommissioning information systems.
SP	Special Publication: A series of documents produced by the NIST that describe the Risk Management Framework and include details on how to become compliant with RMF.
WeBOC	Web Based One Customs: A software system developed by PRAL for use by the FBR and which provides automated Customs management.

Executive Summary

The Risk Management Framework (RMF) provides a structured approach to the development of secure Information Systems. It stresses building security controls into the system early on in the development lifecycle and introduces a set of defined roles and processes to guide the development, authorization, operation, and subsequent operations of secure Information Systems. Within the United States (US) Federal Government, it is mandated to be followed prior to approving an automated system's operational status, with some difference in phases and requirements for systems considered as National Security Systems.

The Federal Board of Revenue (FBR) through previous interactions with the USAID Trade Project, expressed interest in adopting or using elements of the RMF to improve the security of its Information Technology (IT) environment and, in particular, to address deficiencies that were identified in a previous assessment of the Web Based One Customs (WeBOC) system, the Customs automation system currently in use by the FBR. These deficiencies include the following:

- A risk management framework does not exist within FBR or Pakistan Revenue Automation Limited (PRAL), the solution provider for WeBOC
- Gaps in assessing, implementing, and maintaining appropriate security controls within the IT environment for WeBOC
- Absence of a requirements management process including requirements definition and formal approval of functional and non-functional requirements
- Communications management including requirements authorization, design authorization, testing procedures approval and change control procedures are lacking or absent

An initiative to introduce RMF compliance within FBR can address the gaps mentioned above while also introducing efficiencies to WeBOC's Software Development Lifecycle. The required steps include:

- Introducing a change management initiative focused on addressing risk and risk mitigation
- Establishing the Governance model for RMF
- Appointing senior officials within the FBR to sponsor and lead the RMF process
- Defining elements of the RMF to be adopted for use in introducing information systems
- Integrating the six phases of the RMF with the current WeBOC software development lifecycle
- Carrying out the tasks and duties as described within the six phases of the RMF
- Introducing, managing, and promoting a continuous improvement cycle

Introduction

Organizations depend on information systems to automate business processes and to hold, secure, and disseminate information within the enterprise. The functionalities provided by these systems and the roles assigned to manage them are complex and increasingly subject to internal and external threats that can have an adverse impact on the organization's operations.

These systems, unless managed in a secure manner, offer the opportunity for malicious activities that compromise the confidentiality, integrity and availability of information and, for Government-owned assets, can present threats at a national level.

Threats to information and information systems include environmental disruptions, human or machine errors, and purposeful attacks. Cyber-attacks on information systems today are often aggressive, disciplined, well-organized, well-funded, and, in a growing number of documented cases, very sophisticated. Given the significant and growing danger of these threats, it is imperative that leaders at all levels of an organization understand their responsibilities for achieving adequate information security and for managing information system-related security risks.

The RMF was developed by the National Institute for Standards and Technology (NIST) and is defined in the NIST Special Publication (SP) 800-37 Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems. This publication details the six-phase process that allows US federal IT systems to be designed, developed, maintained, and decommissioned in a secure, compliant, and cost-effective manner. The framework provides cost savings by promoting the reuse as well as reciprocity of information systems' approvals and inheritance of organizationally authorized and approved common controls.

Purpose

The RMF approach was adopted in this document based on the PRAL input into Terms of Reference (ToRs) for an advisor provided earlier to the Trade Project; this input noted a need for adopting an RMF approach to managing risks and requested an assessment of required security controls to strengthen the security of WeBOC. This document was developed to explain the rationale behind using a risk-based approach to implement information security controls within an organization and to introduce, at a high level, the RMF introduced by NIST and its Special Publications (SP) series.

Objectives

This document can be used by the reader to understand the RMF and organizational structures, particularly those within the IT function, that are necessary for organizations such as the FBR in considering the improvement of its risk management methodologies and enhancing its security environments. It can be used to provide a high-level overview of the RMF processes and to familiarize the reader with the six phases of the RMF and its relationship to the Software Development Lifecycle (SDLC). The document aims to:

- Provide the reader with an introduction to the RMF and its relevance to organizations implementing Information Systems
- List accountable and supporting roles that need to be staffed within organizations seeking to implement a RMF-compliant environment and the duties performed by each role
- Provide an overview of the six phases required to implement RMF and the tasks within each phase

Scope - Inclusions and Exclusions

The document scope includes selected components from NIST's RMF Framework; particularly the organizational roles that need to be assigned in order for an organization to move to a RMF compliant

environment, and authorities for these roles. It also includes the six RMF phases and tasks within each phase for implementing a RMF within the organization.

Although the document will include, at a high level, gaps relative to the Software Development Lifecycle for WeBOC obtained from a previous assessment of the system[1], it will exclude from its scope a more comprehensive current state assessment of FBR's Risk Management methodology as the Trade Project, despite repeated attempts, was not able to obtain such information from the FBR. Also excluded from the scope are any particular hardware and software vulnerabilities or existing security controls within the FBR, as the Trade Project was not able to obtain any architectural or other relevant documentation related to hardware or software from the FBR, even after repeated requests to support such an analysis.

Audience

Management, administrative, and technical staff can use the information in this document to understand the RMF and to develop Information Systems that incorporate RMF guidance. Management, in particular Information Technology Managers within the FBR, can use the information to ensure that systems are developed in compliance with the regulatory environment within the organization through a consistent approach. Administrative professionals associated with departmental functions and processes within these departments can use this information to formulate structured and overarching policies and programs for compliance with RMF principles and apply these as common controls, eliminating the need for individual security controls for information systems developed at the FBR. Finally, technical professionals required to develop and manage information systems that meet security requirements will also benefit from the recommendations of the RMF for building security into systems early on in the SDLC to eliminate potential costs and re-work later on.

Current State of Technology Risk Management Frameworks within the FBR

Information was obtained from a previous external party assessment of FBR's WeBOC system, developed by PRAL for managing Customs transactions. It is not a comprehensive selection of these findings and focuses only on those findings that are relevant to Risk Management and Security. Findings include:

- RSD(s) lack information objectives of the system, what is to be accomplished, how the system fits into the needs of the business, and finally, how the system performance will be measured
- There is no mechanism for "Requirements Management" in the RSD(s)
- FBR and/ or the FBR project team have not validated and approved the RSD(s)
- Regarding System Architecture and its scalability, issues have been identified; scaling out this architecture to three-tier and /or multiple tiers will require a significant effort. Furthermore. no initial planning has been conducted to design the network architecture of the WeBOC system.
- Kyoto ICT Guidelines, which outline a comprehensive ICT security strategy to ensure availability, integrity and confidentiality of the information and IT systems, and the information they handle, have not been followed
- Similarly with regards to security controls (Encryption), Monitoring, Logical Security, Audit Trail, Segregation of Duties, Security Awareness, User Management, and Physical Security, control weaknesses have been identified in WeBOC
- A formal risk assessment was not carried out by the FBR for its IT environment to assess the possible impact on the organization of a failure of a particular component (e.g., infrastructure, personnel, business applications, communication channels)
- PRAL Change Control Procedures are not being formally and consistently complied with for all changes as part of the System Development Life Cycle. Furthermore, upon review of PRAL' s change control procedures, the following major weaknesses were revealed:

[1] System Audit of One-Customs WeBOC Final Report submitted by SIDAT HYDER MORSHED ASSOCIATES

  - Most of the change requests are not being logged and properly documented. Verbal request for changes and general ad-hoc reports/queries are also being processed

With regards to Software related changes, the following has been observed:

  - Migration of software program from test to production environment is not adequately controlled
  - Documentation supporting the authorization, testing, and approval of program modification is not formally retained
  - Documentation and audit trail of changes to the application source code is not maintained

- Impact analysis of business process changes in the WeBOC system is not conducted in consultation with all stakeholders

The assessment conducted by the external party and submitted on December 24, 2011 may or may not be an accurate reflection of the current state of WeBOC; however, based on Trade Project interactions with PRAL in Karachi and Islamabad[2], it can be assumed that a structured approach to software development, risk management, or implementation of security controls continues to be absent at PRAL, as no information was provided to indicate the introduction and adoption of such applicable frameworks during these meetings or through other communications.

Risk Management Framework Compliant Architecture

The goal of Risk Management, in general, is to recognize, assess, and subsequently reduce and manage risks associated with projects being introduced to an environment or those that may impact ongoing operations within organizations. A number of such frameworks exist, such as those from PMI, COBIT, ITIL, and RMF. While all of these architectures share common elements for assessing and managing risks, RMF goes beyond these to describe, in detail, the security controls required for Information Systems development, operations, and maintenance. In terms of security controls, it provides different security controls for functions within an enterprise (HR, Finance, procurement and others) hence allowing a differentiation of these controls depending on the function where the Information System provides technology.

Architecturally, RMF can be broken down into the following three components:

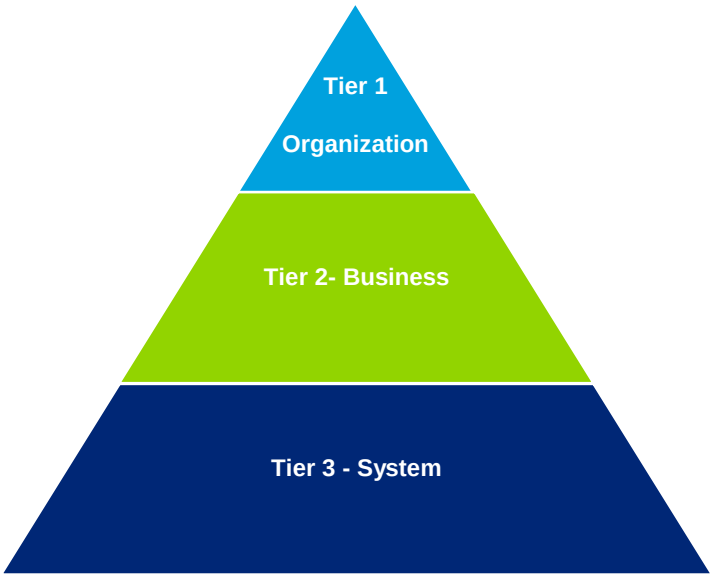
- Risk Management Framework Organizational Tiers
- Risk Management Framework Processes
- Risk Management Framework Roles

Risk Management Framework Organizational Tiers[3]

NIST suggests three organizational tiers for the purpose of defining roles and assuming responsibilities to implement the RMF. It is important to realize that the responsibilities and activities within each tier do not exist in isolation, as Risk Management is an integrated organizational approach with inputs and outputs flowing across these tiers and is an undertaking that involves the entire organization: from Senior Leadership defining the methodology and management overseeing the implementation to individuals responsible for developing the Information Systems and operating the IT environment.

[2] Meetings held in Karachi on August 28 and 29, 2013 with PRAL system and network professional and on 23rd of September 23rd 2013 with Mr. Humayun Zafar/FBR
[3] NIST SP-800

Figure 1 - RMF Organizational Tiers



Tier 1: Organizational Risk Management

Tier 1 addresses risk from an organizational perspective with the development of a comprehensive governance structure and organization-wide risk management strategy that includes:

- The techniques and methodologies the organization plans to employ in order to assess information system-related security risks and other types of concerns to the organization
- The methods and procedures the organization plans to use to evaluate the significance of the risks identified during the risk assessment
- The types and extent of risk mitigation measures the organization plans to employ to address identified risks
- The level of risk the organization plans to accept (i.e., risk tolerance)
- How the organization plans to monitor risk on an ongoing basis, given the inevitable changes to organizational information systems and their environments of operation
- The degree and type of oversight the organization plans to use to ensure that the risk management strategy is being effectively carried out

Tier 2: Business Process Risk Management

Tier 2 addresses risk from a mission and business process perspective and is guided by the risk decisions at Tier 1. Tier 2 activities are closely associated with enterprise architecture and include:

- Defining the core missions and business processes for the organization (including any derivative or related missions and business processes carried out by subordinate organizations)
- Prioritizing missions and business processes with respect to the goals and objectives of the organization
- Defining the types of information that the organization needs to successfully execute the stated missions and business processes and the information flows both internal and external to the organization
- Developing an organization-wide information protection strategy and incorporating high-level information security requirements into the core missions and business processes
- Specifying the degree of autonomy for subordinate organizations (i.e., organizations within the parent organization) that the parent organization permits for assessing, evaluating, mitigating, accepting, and monitoring risk

Tier 3: Information Systems Risk Management

Tier 3 addresses risk from an information system perspective and is guided by the risk decisions at Tiers 1 and 2. Risk decisions at Tiers 1 and 2 impact the ultimate selection and deployment of needed safeguards and countermeasures (i.e., security controls) at the information system level. Information security requirements are satisfied by the selection of appropriate management, operational, and technical security controls from NIST Special Publication 800-53.19. The security controls are subsequently allocated to the various components of the information system as system-specific, hybrid, or common controls in accordance with the information security architecture developed by the organization. Security controls are typically traceable to the security requirements established by the organization to ensure that the requirements are fully addressed during design, development, and implementation of the information system. Security controls can be provided by the organization or by an external provider. Relationships with external providers are established in a variety of ways, for example, through joint ventures, business partnerships, outsourcing arrangements (i.e., through contracts, interagency agreements, lines of business arrangements), licensing agreements, and/or supply chain arrangements.

The RMF operates primarily at Tier 3 in the risk management hierarchy but can also have interactions with Tiers 1 and 2 (e.g., providing feedback from ongoing authorization decisions to the risk executive [function], dissemination of updated threat and risk information to authorizing officials and information system owners). The RMF steps particular to Tier 3 include:

- **Categorize** the information system and the information processed, stored, and transmitted by that system based on an impact analysis.
- **Select** an initial set of baseline security controls for the information system based on the security categorization; tailoring and supplementing the security control baseline as needed based on an organizational assessment of risk and local conditions.
- **Implement** the security controls and describe how the controls are employed within the information system and its environment of operation.
- **Assess** the security controls using appropriate assessment procedures to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.
- **Authorize** information system operation based on a determination of the risk to organizational operations and assets, individuals, other organizations, and the Nation resulting from the operation of the information system and the decision that this risk is acceptable.
- **Monitor** the security controls in the information system on an ongoing basis including assessing control effectiveness, documenting changes to the system or its environment of operation, conducting security impact analyses of the associated changes, and reporting the security state of the system to designated organizational officials.

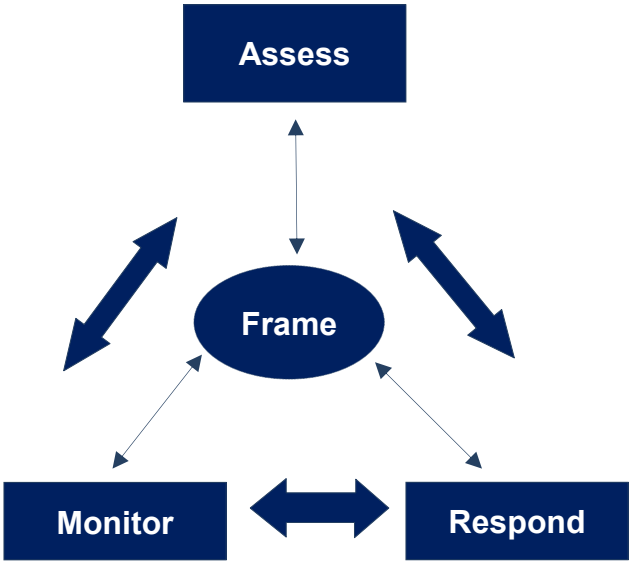
Risk Management Processes

NIST publishes a number of SPs to define the Risk Management processes and to provide guidance on security control assessment and implementation. Of particular importance are:

- NIST SP 800-30 (guide for conducting risk assessments) provides an overview of Risk Management and how it fits into the SDLC lifecycle and how to conduct risk assessments and manage risks
- NIST SP 800-37 (Guide for applying the RMF) defines and provides a guide for applying the six RMF Phases
- NIST SP 800-39 (Managing Information Security Risk) defines the multi-tiered, organization-wide approach to risk management that is discussed in this chapter
- NIST SP 800-53 (Security and Privacy Controls for Federal Information Systems) provides security control categories, designations, suggested selections and baselines

At the basic level, four processes are required for effective risk management within an organization, namely risk framing, risk assessment, risk responses, and risk monitoring. The processes interact with each other and outputs of each are used as inputs to the others in a continuous improvement and re-enforcement cycle.

Figure 2 - Risk Management Processes



Risk Framing

The responsibility to develop and manage this process belongs to Tier 1 leadership and groups within an organization. Risk policies impacting the entire organization are developed by the organization's leadership and cascaded to the functional and technical groups. Below are some of the areas that need to be considered while framing risks:

- Risk Categories: Categories both internal and external to the organization are developed and, when possible, grouped
- Risk Assumptions: The likelihood of risks
- Risk Constraints: The impediments to categorizing risks and development of risk responses
- Risk Thresholds: The acceptable tolerance levels to the organizations. Risk thresholds are used to allocate financial resources and plans to address risks that are above acceptable thresholds

Risk Assessment

All members within the organization are tasked with viewing external and internal risks for the purpose of developing risks that may impact the organization, should they occur. The outcomes of this exercise are risk registers which include risks and their associated quantitative and qualitative data. Based on the data, priorities are then assigned to risks.

Risk Responses

This process takes the outputs of Risk Assessment in order to develop actions for each categorized risk. Risk acceptance, avoidance, mitigation, and risk transfer (to another provider) are some of the strategies that can be taken towards addressing materialized risks. More than one course of action should be developed and evaluated towards agreement on a specific action.

- Acceptance
- Avoidance
- Mitigation
- Transfer

Risk Monitoring

Ongoing evaluation of the risk responses and their success are the key activities within this component. The entire risk profile of the organization should be subject to ongoing scrutiny and inspection to identify new threats that will require updates to the risk assessment and risk responses as part of a continuous improvement cycle.

SDLC and the RMF

NIST publication SP 800-64 details the required organizational structure, roles, and key processes recommended to incorporate security as part of the system development lifecycle. It's important to recognize, despite the use of Agile Frameworks, that the publication assumes and is focused on a traditional Waterfall approach for systems development, as this approach continues to be the main framework used by project managers and system developers implementing information systems.

Figure 3 below is a brief overview of the key activities for each of the five phases within the Waterfall approach. The six RMF phases which will be described later include tasks that are to be carried out during and as part of the SDLC phases to ensure that security is built into the system as part of the development approach.

Figure 3 - SDLC Lifecycle

Phase 1 Initiation	• Develop Business Case and Project Charter • Establish budget • Develop high-level system requirements • Develop Master Plan and Initiate Project
Phase 2 Development/Acquisition	• Evaluate Requirements • Develop functional, non-functional and system security plans • Decide on development or procurement of system
Phase 3 Implementation/Assessment	• Establish test environment • Evaluate functionalities and system security • Develop Security Assessment Report (SAR)
Phase 4 Operation/Maintenance	• Move system into production environment • Use system • Manage system configuration and changes
Phase 5 Disposal	• Manage and secure existing system data • Establish termination and data migration or archiving plans • Terminate system

RMF Implementation Required Roles

Thirteen roles are suggested as part of establishing and maintaining the RMF approach. Passages in this section detail these roles, as defined by the NIST[4]. These roles are:

Head of Agency (Chief Executive Officer)

The head of agency (or chief executive officer) is the highest-level senior official or executive within an organization with the overall responsibility to provide information security protections commensurate with the risk and magnitude of harm (i.e., impact) to organizational operations and assets, individuals, other organizations, and the nation resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained by or on behalf of the agency; and

[4] NIST SP 800-37

information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency. Agency heads are also responsible for ensuring that information security management processes are integrated with strategic and operational planning processes; senior officials within the organization provide information security for the information and information systems that support the operations and assets under their control; and the organization has trained personnel sufficient to assist in complying with the information security requirements in related legislation, policies, directives, instructions, standards, and guidelines. Through the development and implementation of strong policies, the head of agency establishes the organizational commitment to information security and the actions required to effectively manage risk and protect the core missions and business functions being carried out by the organization. The head of agency establishes appropriate accountability for information security and provides active support and oversight of monitoring and improvement for the information security program. Senior leadership commitment to information security establishes a level of due diligence within the organization that promotes a climate for mission and business success.

Risk Executive (Function)

The risk executive (function) is an individual or group within an organization which helps to ensure risk-related considerations for individual information systems, including authorization decisions, are viewed from an organization-wide perspective with regard to the overall strategic goals and objectives of the organization for carrying out its core missions and business functions.

The risk executive function ensures that the approach to managing information system-related security risks is consistent across the organization, reflects organizational risk tolerance, and is considered along with other types of risks in order to ensure mission/business success. The risk executive function coordinates with the senior leadership of an organization to:

- Provide a comprehensive, organization-wide, holistic approach for addressing risk—an approach that provides a greater understanding of the integrated operations of the organization
- Develop a risk management strategy for the organization providing a strategic view of information security-related risks with regard to the organization as a whole
- Facilitate the sharing of risk-related information among authorizing officials and other senior leaders within the organization
- Provide oversight for all risk management-related activities across the organization (e.g., security categorizations) to help ensure consistent and effective risk acceptance decisions
- Ensure that authorization decisions consider all factors necessary for mission and business success
- Provide an organization-wide forum to consider all sources of risk (including aggregated risk) to organizational operations and assets, individuals, and other organizations
- Promote cooperation and collaboration among authorizing officials to include authorization actions requiring shared responsibility
- Ensure that the shared responsibility for supporting organizational mission/business functions using external providers of information and services receives the needed visibility and is elevated to the appropriate decision-making authorities
- Identify the organizational risk posture based on the aggregated risk to information from the operation and use of the information systems for which the organization is responsible.

The risk executive function presumes neither a specific organizational structure nor formal responsibility assigned to any one individual or group within the organization. The head of the agency/organization may choose to retain the risk executive function or to delegate the function to another official or group (e.g., an executive leadership council).

Chief Information Officer
The chief information officer is an organizational official responsible for designating a senior information security officer and for developing and maintaining information security policies.

Information Owner/Steward
The information owner/steward is an organizational official with statutory, management, or operational authority for specified information and the responsibility for establishing the policies and procedures governing its generation, collection, processing, dissemination, and disposal. In information-sharing environments, the information owner/steward is responsible for establishing the rules for appropriate use and protection of the subject information (e.g., rules of behavior) and retains that responsibility even when the information is shared with or provided to other organizations. The owner/steward of the information processed, stored, or transmitted by an information system may or may not be the same as the system owner. A single information system may contain information from multiple information owners. Information owners/stewards provide input to information system owners regarding the security requirements and security controls for the systems where the information is processed, stored, or transmitted.

Senior Information Security Officer
The senior information security officer is an organizational official responsible for:

- Carrying out the chief information security officer responsibilities
- Serving as the primary liaison for the chief information officer to the organization's authorizing officials, information system owners, common control providers, and information system security officers
- Maintaining information security duties as a primary responsibility
- Managing an office with the mission and resources to assist the organization in achieving more secure information and information systems

The senior information security officer (or supporting staff members) may also serve as an authorizing entity for official designated representatives or security control assessors.

Authorizing Official
The authorizing official is a senior official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations and assets, individuals, other organizations, and the nation. Authorizing officials typically have budgetary oversight for an information system or are responsible for the mission and/or business operations supported by the system. Through the security authorization process, authorizing officials are accountable for the security risks associated with information system operations. Accordingly, authorizing officials are in management positions with a level of authority commensurate with understanding and accepting such information system-related security risks. Authorizing officials also approve security plans, memorandums of agreement or understanding, and plans of action and milestones and determine whether significant changes in the information systems or environments of operation require reauthorization. Authorizing officials can deny authorization to operate an information system, or halt operations if the system is operational and unacceptable risks exist. Authorizing officials coordinate their activities with the risk executive function, chief information officer, senior information security officer, common control providers, information system owners, information system security officers, security control assessors, and other interested parties during the security authorization process. With the increasing complexity of missions/business processes, partnership arrangements, and the use of external/shared services, it is possible that a particular information system may involve multiple authorizing officials. If so, agreements are established among the authorizing officials and documented in the security plan. Authorizing officials are responsible for ensuring that all activities and functions associated with security authorization that are delegated to the authorizing official designated representatives are carried out.

Authorizing Official Designated Representative

The authorizing official designated representative is an organizational official that acts on behalf of an authorizing official to coordinate and conduct the required day-to-day activities associated with the security authorization process. Authorizing official designated representatives can be empowered by authorizing officials to make certain decisions with regard to the planning and resourcing of the security authorization process, approval of the security plan, approval and monitoring the implementation of action plans and milestones, and the assessment and/or determination of risk. The designated representative may also be called upon to prepare the final authorization package, obtain the authorizing official's signature on the authorization decision document, and transmit the authorization package to appropriate organizational officials. The only activity that cannot be delegated to the designated representative by the authorizing official is the authorization decision and signing of the associated authorization decision document.

Common Control Provider

The common control provider is an individual, group, or organization responsible for the development, implementation, assessment, and monitoring of common controls (i.e., security controls inherited by information systems). Common control providers are responsible for:

- Documenting the organization-identified common controls in a security plan (or equivalent document prescribed by the organization)
- Ensuring that required assessments of common controls are carried out by qualified assessors with an appropriate level of independence, as defined by the organization
- Documenting assessment findings in a security assessment report
- Producing a plan of action and milestones for all controls having weaknesses or deficiencies

Security plans, security assessment reports, and plans of action and milestones for common controls (or a summary of such information) are made available to information system owners inheriting those controls after the information is reviewed and approved by the senior official or executive with oversight responsibility for those controls.

Information System Owner

The information system owner is an organizational official responsible for the procurement, development, integration, modification, operation, maintenance, and disposal of an information system. The information system owner is responsible for addressing the operational interests of the user community (i.e., users who require access to the information system to satisfy mission, business, or operational requirements) and for ensuring compliance with information security requirements. In coordination with the information system security officer, the information system owner is responsible for the development and maintenance of the security plan and ensures that the system is deployed and operated in accordance with the agreed-upon security controls. In coordination with the information owner/steward, the information system owner is also responsible for deciding who has access to the system (and with what types of privileges or access rights) and ensures that system users and support personnel receive the requisite security training (e.g., instruction in rules of behavior). Based on guidance from the authorizing official, the information system owner informs appropriate organizational officials of the need to conduct the security authorization, ensures that the necessary resources are available for the effort, and provides the required information system access, information, and documentation to the security assessor. The information system owner receives the security assessment results from the security control assessor. After taking appropriate steps to reduce or eliminate vulnerabilities, the information system owner assembles the authorization package and submits the package to the authorizing official or the authorizing official designated representative for adjudication.

Information System Security Officer

The information system security officer is an individual responsible for ensuring that the appropriate operational security posture is maintained for an information system and works in close collaboration with the information system owner. The information system security officer also serves as a principal advisor on all matters, technical and otherwise, involving the security of an information system. The information system security officer has the detailed knowledge and expertise required to manage the security aspects of an information system and, in many organizations, is assigned responsibility for the day-to-day security operations of a system. This responsibility may also include, but is not limited to, physical and environmental protection, personnel security, incident handling, and security training and awareness. The information system security officer may be called upon to assist in the development of security policies and procedures and to ensure compliance with those policies and procedures. In close coordination with the information system owner, the information system security officer often plays an active role in the monitoring of a system and its environment of operation to develop and update the security plan, manage and control changes to the system, and assess the security impact of those changes.

Information Security Architect

The information security architect is an individual, group, or organization responsible for ensuring that the information security requirements necessary to protect the organization's core missions and business processes are adequately addressed in all aspects of enterprise architecture including reference models, segment and solution architectures, and the resulting information systems supporting those missions and business processes. The information security architect serves as the liaison between the enterprise architect and the information system security engineer and also coordinates with information system owners, common control providers, and information system security officers on the allocation of security controls as system-specific, hybrid, or common controls. In addition, information security architects, in close coordination with information system security officers, advise authorizing officials, chief information officers, senior information security officers, and the risk executive (function), on a range of security-related issues including, for example, establishing information system boundaries, assessing the severity of weaknesses and deficiencies in the information system, plans of action and milestones, risk mitigation approaches, security alerts, and potential adverse effects of identified vulnerabilities.

Information System Security Engineer

The information system security engineer is an individual, group, or organization responsible for conducting information system security engineering activities. Information system security engineering is a process that captures and refines information security requirements and ensures that the requirements are effectively integrated into information technology component products and information systems through purposeful security architecting, design, development, and configuration. Information system security engineers are an integral part of the development team (e.g., integrated project team), designing and developing organizational information systems or upgrading legacy systems. Information system security engineers employ best practices when implementing security controls within an information system including software engineering methodologies, system/security engineering principles, secure design, secure architecture, and secure coding techniques. System security engineers coordinate their security-related activities with information security architects, senior information security officers, information system owners, common control providers, and information system security officers.

Security Control Assessor

The security control assessor is an individual, group, or organization responsible for conducting a comprehensive assessment of the management, operational, and technical security controls employed within or inherited by an information system to determine the overall effectiveness of the controls (i.e., the extent to which the controls are implemented correctly, operating as intended, and

producing the desired outcome with respect to meeting the security requirements for the system). Security control assessors also provide an assessment of the severity of weaknesses or deficiencies discovered in the information system and its environment of operation and recommend corrective actions to address identified vulnerabilities. In addition to the above responsibilities, security control assessors prepare the final security assessment report containing the results and findings from the assessment. Prior to initiating the security control assessment, an assessor conducts an assessment of the security plan to help ensure that the plan provides a set of security controls for the information system that meet the stated security requirements.

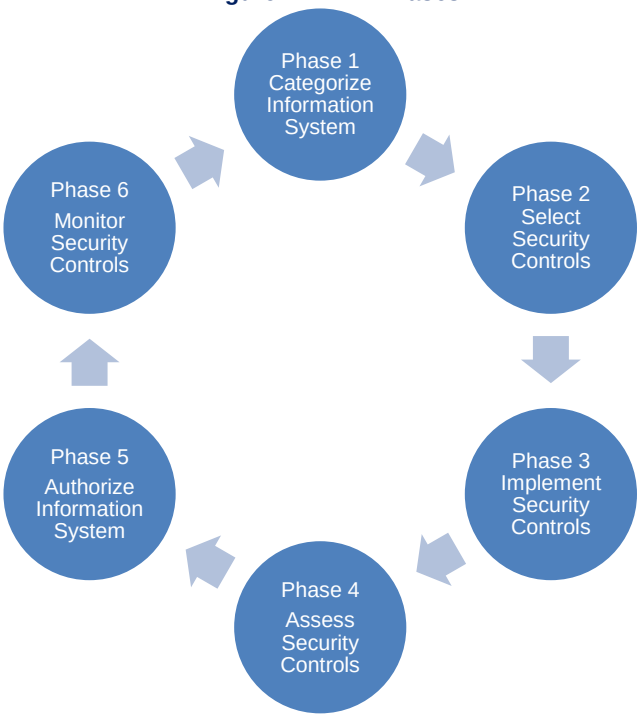
The required level of assessor independence is determined by the specific conditions of the security control assessment. For example, when the assessment is conducted in support of an authorization decision or ongoing authorization, the authorizing official makes an explicit determination of the degree of independence required in accordance with federal policies, directives, standards, and guidelines.

Assessor independence is an important factor in preserving the impartial and unbiased nature of the assessment process, determining the credibility of the security assessment results, and ensuring that the authorizing official receives the most objective information possible in order to make an informed, risk-based, authorization decision.

RMF Phases

The RMF consists of six phases which are implemented in a cyclic fashion and through a progressive elaboration approach to ensure that all SDLC phases are covered and to enable continuous improvement. Each of the RMF phases map to a particular phase within the SDLC lifecycle. It is important to maintain this relationship to satisfy security requirements at the outset and to reduce costly change controls and additional time and effort that may be required prior to authorizing the system. The phases and tasks within will be described in further detail below. **Appendix 1** contains a summary of these phases along with owners and supporting roles.

Figure 4 - RMF Phases



RMF Phase 1: Categorize the Information System

Phase 1 of the RMS defines the system and its categorization levels. It sets a solid foundation for the selection of security controls in subsequent phases, and is hence critical for the overall security and compliance of the system. It consists of the three tasks below:

RMF Phase 1, Task 1: Security Categorization

Security categorization starts with gathering, grouping and documenting all information system types that will be processed, transmitted and used by the system (within FBR, the scope would be WeBOC security) and then mapping each against the security categorizations of Confidentiality, Integrity, and Availability (CIA). Once mapped, the impacts are then determined using a low, medium, and high impact to the organization (**Table 1** below).

As the information types have not been provided by FBR for assessment, it is not possible to assess and suggest categorizations or their impacts. Further guidance on suitable types is available in NIST publication FIPS PUB 199 “Standards for Security Categorization of Federal Information and Information Systems” and can be used as reference.

The official definitions for the security objects as well as impact levels are quoted from FIPS Publication 199 as follows:

Confidentiality: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. A loss of confidentiality is the unauthorized disclosure of information.

Integrity: Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.

Availability: Ensuring timely and reliable access to and use of information.

Table 1 - Security Categorizations

Information Types	Security Objective	Potential Impact		
		Low	Medium	High
	Confidentiality			
	Integrity			
	Availability			

The exit point for phase 1, task 1 is an updated security plan with impacts for information systems for the objective groups (CIA).

RMF Phase 1, Task 2: Information Systems Description

The primary objective of this task is to provide identifiers for system components and establish boundaries. This is done in order to understand owners of the components, authorizations required in subsequent phases, and budget allocations. Below is a list of sections that should be incorporated in the systems security document.

- Descriptive name of the system and unique identifier
- Acronyms for system components
- Owner and contact information
- Authorization official and contact information
- Location of component
- Environment, which is usually under one of the three categories of standalone, enterprise, or custom

- Version number of system
- Processes supported
- SDLC/Acquisition cycle defines where in the development or procurement cycle the component exists

RMF Phase 1, Task 3: Information System Registration
The final step in phase 1 is to register the system with the Project or Portfolio Management office within the organization. This step is only necessary if the system is replacing an existing one and is performed to ensure that no duplicate systems exist and that no other parallel efforts and resources are committed to a similar system within the organization

RMF Phase 2: Select Security Controls

Key activities during phase 2 include determining security controls for the information types identified earlier and the development of a monitoring plan to ensure that these controls are functioning and followed.

It is of benefit prior to viewing the tasks associated with phase 2 to understand the structure of the security controls that are documented in the systems security plan. **Table 2** below illustrates these sections.

Table 2 - Security Controls Structure

Section Name	Explanation
Control Section	A two-part alphanumeric identifier that defines the control. An alphabetic identifier (of two characters) is used to define the family the control is under and is followed by a number that indicates the order of the control within that family. For example, AC-2 identifies a control under the Access Control family and is the second control within the group
Supplemental Guidance Section	Optional section. Further defines information related to the control including relationships to other controls and information related to its design and implementation
Control Enhancement Section	Optional section. Additional components that can be added to the control to enhance its security
Reference Section	Any laws, regulatory or compliance relationships and dependencies
Priority and Baseline Allocation	Priorities (1-3) are assigned for prioritizing the implementation of controls. A P1 control will be designed and implemented before a P2 or P3 control

RMS Phase 2, Task 1: Common Control Identification
The objectives of this task are to develop common security controls applicable to all information systems within the organization. It is performed at the organizational level and is recommended to be inherited as-is or used, with some modifications at the system level. The concept of inheritance is recommended as it reduces or eliminates duplication and ensures consistency. Controls should be identified and, whenever possible, grouped under a category. Example controls are authorization controls, remote access controls, account lock out, and others. A catalogue of controls can be found in NIST 800-53 and can be used as guidance.

RMS Phase 2, Task 2: Security Control Selection
This task takes the common controls identified earlier and selects controls relevant to the needs and environment within the organization as it is not expected or required that all controls be considered or implemented.

RMS Phase 2, Task 3: Developing a Monitoring Strategy
The objective of this task is to review the ongoing applicability of a control, its behavior when used, and potential areas for improvement (or dropping the control if no longer relevant). NIST has

developed a publication, entitled Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations, SP 800-137, that describes how to develop a continuous monitoring program for a system or organization, and should be referred to for the purpose of monitoring of control and continuous improvement.

RMS Phase 2, Task 4: Review and Approve the System Security Plan
The final step in phase 2 is for the Authorizing Official or designates to approve the System Security Plan with the inputs from Phase 2 tasks.

RMF Phase 3: Implementing Security Controls

This phase takes the identified security controls from Phase 2 and implements them in the system. It consists of the two tasks below:

RMS Phase 2, Task 1: Security Control Implementation
For systems being developed, this task often runs in parallel with the implementation phase of the SDLC lifecycle. The focus is on reviewing the security controls while implementing the system and three different assessment methods can be used, depending on the focus areas:

- **Examinations** are reviews of the organization and business unit policies, regulations and documentation to ensure that the system implementation and security controls are in-line with those requirements
- **Interviews** are held with system owners, developers and staff members to evaluate and provide feedback on security controls implemented and their adherence to requirements
- **Tests** are focused on the system, particularly on system outputs and their functionality from a security control perspective

NIST publication 800-53 provides assessments for each of the security controls recommended in the catalogue and should be referenced for future guidance.

RMS Phase 2, Task 2: Security Control Documentation
This task involves documenting the different types of security controls and specifying whether they are common or hybrid (common and custom) implementations. It also provides traceability to the requirements defined in Phase 1 (categorizing controls) and the inputs and outputs of the assessments in Phase 2, task 1.

RMF Phase 4: Assess Security Controls

Key activities within Phase 4 include development of an Assessment Strategy, assessment of the security controls and the production of a Security Assessment Report (SAR). Four tasks are carried out within this phase, as detailed below.

RMF Phase 4, Task 1: Develop Security Control Assessment Plan
In this step, the objectives for the assessment, a roadmap with actions, and required procedures are developed. The plan and subsequent actions will vary depending on whether the system is developed or acquired, what types of assessments are to be carried out (internal versus independent) as well as the scope of the assessment (full versus select audits). This task should be conducted in parallel to the system development and implementation cycles as it allows for the identification of threats, weaknesses, and remedies before the system is placed into production. Some of the inputs to the plan include:

- Assessment boundaries
- Automated and/or manual tools and processes to conduct the assessment
- Roles required to conduct the assessment
- Which controls are to be assessed (some controls that were assessed prior to authorization in earlier steps do not require a re-assessment)

- Detailed procedures to be followed by the assessor

The output of this task is an approved test plan that guides the assessors in conducting the security control assessments.

RMF Phase 4, Task 2: Conduct Security Control Assessments
During this phase, a test director, with a thorough understanding of the plan and its implementation, should be appointed. The test director will guide and work with the assessors to implement the assessment plan and is the point of contact and interface between the different teams involved in the system development and security control assessments. It is also important to note that no changes to the system are implemented prior to finalizing this assessment, hence system development and changes should seize at the baseline point prior to conducting assessments. The use of automated assessments should be maximized during this phase.

RMF Phase 4, Task 3: Develop Security Assessment Report (SAR)
This SAR is a document prepared as an output of task 2 above and is used to guide the authorizing official. At minimum, it should contain the following information:

- Information System Name
- Categorizations
- Time and location of assessments
- Assessor name
- Methods used
- Assessor comments
- Summary findings (including threats and weaknesses)
- Recommendations

RMF Phase 4, Task 4: Develop Remediation Actions
Using the SAR, the system owner develops a plan of action to address the threats and weaknesses in the system. Each security control with weaknesses is either redeveloped or reconfigured and the testing cycle should be conducted again to ensure that threats have been resolved or mitigated.

RMF Phase 5: Authorizing the Information System

During this phase, the Authorizing Official approves or rejects the system going into operation. It is where the Program Management Staff develop a Plan of Actions and Milestones (POA&M) to address any deficiencies identified in the earlier phase. There are four tasks within this phase, as noted below.

RMF Phase 5, Task 1: Develop the Plan of Actions and Milestones
This plan is developed by the system owner and, in addition to the System Security Plan and Security Assessment Report, is part of the authorization package to be reviewed by the Authorizing Official. Below are some of the inputs to the plan

- Identified weaknesses
- Resources required to remedy the weaknesses identified
- Required funding
- Timelines and milestones to resolve threats and weaknesses
- Changes to milestones
- Current status

It is important to maintain the integrity of this document in a way where no information is deleted, only new information is added to ensure a full audit trail for review is available, and all deficiencies have been resolved and tracked in the future.

RMF Phase 5, Task 2: Assembly of the Authorization Package

The authorization package consists minimally of the System Security Plan, Security Assessment Report, and the Plan of Action and Milestones. Task 2 within Phase 5 is assigned to the system owner to prepare the Authorization package, which is then submitted to the Authorizing Official for approval.

RMF Phase 5, Task 3: Determine Risks

This task is where the Authorizing Official reviews the Authorization Package to determine the security state of the system. A risk assessment strategy should be followed to assess the package and to further update risk assessment documentation based on the system being placed into production.

RMF Phase 5, Task 4: Accepting Risks

This task includes one of two authorization decisions which can only be made by the Authorizing Official, either authorizing the system with its known risks or not authorizing the system. Authorization can also mean that the system is allowed to operate in a test environment or reduced functionality until the threats identified in the Plan of Action and Milestones are remedied. The authorization should also include terms and conditions detailing whether the system is to be operational for a limited time or indefinitely along with a continuous monitoring system. The decision can also include a re-authorization of the system once the initial authorizing expires.

RMF Phase 6: Monitor Security Controls

Once the system is operational, the RMF focus moves to Operations and Maintenance (O&M) activities which include an ongoing assessment of security controls, remediation actions, documentation, status reporting, and decommissioning, among other tasks. This phase has the seven tasks detailed below.

RMF Phase 6, Task 1: Monitoring Information System and Environment Changes

Task one within this phase focuses on reviewing changes requested to the system and approving or rejecting these changes. It is essential that the system production environment is base-lined and documented as part of a configuration management system. A change management process should be developed to be followed when changes are raised and any changes should be assessed for potential impact to security controls prior to implementation. Roll-back plans should be available to implement should the systems' functionality be affected negatively post-implementation of changes.

RMF Phase 6, Task 2: Ongoing Security Controls Assessment

All security controls should be assessed at least once during the operation of the system to ensure their effectiveness, preferably by an independent assessor. The Security Assessment Report is updated based on any deficiencies recognized and can be used as input for subsequent re-authorization of the system, once its term expires.

RMF Phase 6, Task 3: Ongoing Remediation Actions

This task is based on the updated Security Assessment Report from Task 2 above. Actions include prioritizing deficiencies and assigning remediation actions to resources. All remedied security controls have to be re-assessed and the SAR updated to reflect results of testing.

RMF Phase 6, Task 4: Update the Security Documentation

This task includes updates to the System Security Plan, Security Assessment Report and Plan of Action and Milestones. As noted earlier, it is important that information is not removed from these documents while adding new updates, to ensure a full audit trail.

RMF Phase 6, Task 5: Security Status Reporting
Event-driven updates and time-driven updates should be provided to the Authorization Official or designates. Event-driven updates are the result of an action such as a system security breach or newly assessed information; time-driven updates are those provided on a regular basis as established by the Authorization Official.

RMF Phase 6, Task 6: Ongoing Risk Determination and Acceptance
This task is a review of the reported security status of the information system (including the effectiveness of security controls employed within and inherited by the system) on an ongoing basis in accordance with the monitoring strategy to determine whether the risk to the organization remains acceptable.

RMF Phase 6, Task 7: System Removal and Decommissioning
When a federal information system is removed from operation, a number of risk management-related actions are required. Organizations ensure that all security controls addressing information system removal and decommissioning (e.g., media sanitization, configuration management and control) are implemented. Organizational tracking and management systems (including inventory systems) are updated to indicate the specific information system components that are being removed from service. Security status reports reflect the new status of the information system. Users and application owners hosted on the decommissioned information system are notified as appropriate, and any security control inheritance relationships are reviewed and assessed for impact.

Conclusions and Recommendations

A previous assessment of WeBOC identified vulnerabilities and areas for improvement in a number of categories, some of which are pertinent to the security of information systems. These areas include requirements gathering and approvals, security controls, and communication management.

To manage threats emanating from these areas, FBR can follow the RMF approach and adopt the recommendations across all three tiers of the enterprise (Organization, Business, and Process).

1. Initiating a change management initiative focused on risk and risk mitigation as relevant to Information Systems within the FBR. This initiative should be led and introduced by senior officials within the FBR and promoted across all levels within the organization
2. Establishing the Governance model including the initiation of a Risk Executive function within the FBR and an approved charter to lead and guide the RMF implementation
3. Appointing senior roles within the FBR starting with a Security Systems Information Officer and Security Systems Architect
4. In partnership with WeBOC's implementer, PRAL, defining elements of the RMF to be adopted for use in initiating, designing, and putting into production future iterations of WeBOC and the system operating environment, including the required infrastructure security controls
5. Integrating the six phases of the RMF with the current WeBOC system development lifecycle
6. Carrying out the tasks and duties for each of the six RMF phases
7. Introducing, managing, and promoting a continuous improvement cycle within the FBR and its partners

Appendix 1: RMF Phases and Owners[5]

RMF Tasks	Primary Responsibility	Supporting Roles
RMF Step 1 – Categorize Information System		
Task 1-1 **Security Categorization** Categorize the information system and document the results of the security categorization in the security plan.	Information System Owner Information Owner/Steward	Risk Executive (Function) Authorizing Official or Designated Representative Chief Information Officer Senior Information Security Officer Information System Security Officer
TASK 1-2 **Information System Description** Describe the information system (including system boundary) and document the description in the security plan.	Information System Owner	Authorizing Official or Designated Representative Senior Information Security Officer Information Owner/Steward Information System Security Officer
TASK 1-3 **Information System Registration** Register the information system with appropriate organizational program/management offices.	Information System Owner	Information System Security Officer
RMF Task 2 – Select Security Controls		
TASK 2-1 **Common Control Identification** Identify the security controls that are provided by the organization as common controls for organizational information systems and document the controls in a security plan (or equivalent document).	Chief Information Officer or Senior Information Security Officer Information Security Architect Common Control Provider	Risk Executive (Function) Authorizing Official or Designated Representative Information System Owner Information System Security Engineer
TASK 2-2 **Security Control Selection** Select the security controls for the information system and document the controls in the security plan.	Information Security Architect Information System Owner	Authorizing Official or Designated Representative Information Owner/Steward Information System Security Officer Information System Security Engineer
TASK 2-3 **Monitoring Strategy** Develop a strategy for the continuous monitoring of security control effectiveness and any proposed/actual changes to the information system and its environment of operation.	Information System Owner or Common Control Provider	Risk Executive (Function) Authorizing Official or Designated Representative Chief Information Officer Senior Information Security Officer Information Owner/Steward Information System Security Officer
TASK 2-4 **Security Plan Approval** Review and approve the security plan.	Authorizing Official or Designated Representative	Risk Executive (Function) Chief Information Officer Senior Information Security Officer
RMS Step 3 – Implement Security Controls		
TASK 3-1 **Security Control Implementation** Implement the security controls specified in the security plan.	Information System Owner or Common Control Provider	Information Owner/Steward Information System Security Officer Information System Security Engineer
TASK 3-2 **Security Control Documentation** Document the security control implementation, as appropriate, in the	Information System Owner or Common Control Provider	Information Owner/Steward Information System Security Officer Information System Security Engineer

[5] NIST Special Publication 800-37

security plan, providing a functional description of the control implementation (including planned inputs, expected behavior, and expected outputs).		
RMF Step 4 – Assess Security Controls		
TASK 4-1 **Assessment Preparation** Develop, review, and approve a plan to assess the security controls.	Security Control Assessor	Authorizing Official or Designated Representative Chief Information Officer Senior Information Security Officer Information System Owner or Common Control Provider Information Owner/Steward Information System Security Officer
TASK 4-2 **Security Control Assessment** Assess the security controls in accordance with the assessment procedures defined in the security assessment plan.	Security Control Assessor	Information System Owner or Common Control Provider Information Owner/Steward Information System Security Officer
TASK 4-3 **Security Assessment Report** Prepare the security assessment report documenting the issues, findings, and recommendations from the security control assessment.	Security Control Assessor	Information System Owner or Common Control Provider Information System Security Officer
TASK 4-4 **Remediation Actions** Conduct initial remediation actions on security controls based on the findings and recommendations of the security assessment report and reassess remediated control(s), as appropriate.	Information System Owner or Common Control Provider Security Control Assessor	Authorizing Official or Designated Representative Chief Information Officer Senior Information Security Officer Information Owner/Steward Information System Security Officer Information System Security Engineer
RMF Step 5 – Authorize Information System		
TASK 5-1 **Plan of Action and Milestones** Prepare the plan of action and milestones based on the findings and recommendations of the security assessment report excluding any remediation actions taken.	Information System Owner or Common Control Provider	Information Owner/Steward Information System Security Officer
TASK 5-2 **Security Authorization Package** Assemble the security authorization package and submit the package to the authorizing official for adjudication.	Information System Owner or Common Control Provider	Information System Security Officer Security Control Assessor
TASK 5-3 **Risk Determination** Determine the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the nation.	Authorizing Official or Designated Representative	Risk Executive (Function) Senior Information Security Officer
TASK 5-4 **Risk Acceptance** Determine if the risk to organizational operations, organizational assets,	Authorizing Official	Risk Executive (Function) Authorizing Official Designated Representative Senior Information Security Officer

individuals, other organizations, or the nation is acceptable.		
RMF Step 6 – Monitor Security Controls		
TASK 6-1 **Information System and Environment Changes** Determine the security impact of proposed or actual changes to the information system and its environment of operation.	Information System Owner or Common Control Provider	Risk Executive (Function) Authorizing Official or Designated Representative Senior Information Security Officer Information Owner/Steward Information System Security Officer
TASK 6-2 **Ongoing Security Control Assessments** Assess a selected subset of the technical, management, and operational security controls employed within and inherited by the information system in accordance with the organization-defined monitoring strategy.	Security Control Assessor	Authorizing Official or Designated Representative Information System Owner or Common Control Provider Information Owner/Steward Information System Security Officer
TASK 6-3 **Ongoing Remediation Actions** Conduct remediation actions based on the results of ongoing monitoring activities, assessment of risk, and outstanding items in the plan of action and milestones.	Information System Owner or Common Control Provider	Authorizing Official or Designated Representative Information Owner/Steward Information System Security Officer Information System Security Engineer Security Control Assessor
TASK 6-4 **Key Updates** Update the security plan, security assessment report, and plan of action and milestones based on the results of the continuous monitoring process.	Information System Owner or Common Control Provider	Information Owner/Steward Information System Security Officer
TASK 6-5 **Security Status Reporting** Report the security status of the information system (including the effectiveness of security controls employed within and inherited by the system) to the authorizing official and other appropriate organizational officials on an ongoing basis in accordance with the monitoring strategy.	Information System Owner or Common Control Provider	Information System Security Officer
TASK 6-6 **Ongoing Risk Determination and Acceptance** Review the reported security status of the information system (including the effectiveness of security controls employed within and inherited by the system) on an ongoing basis in accordance with the monitoring strategy to determine whether the risk to organizational operations, organizational assets, individuals, other organizations, or the Nation remains acceptable.	Authorizing Official	Risk Executive (Function) Authorizing Official Designated Representative Senior Information Security Officer
TASK 6-7 **Information System Removal and Decommissioning**	Information System Owner	Risk Executive (Function) Authorizing Official Designated Representative

Implement an information system decommissioning strategy, when needed, which executes required actions when a system is removed from service.		Senior Information Security Officer Information Owner/Steward Information System Security Officer

Appendix 2: Relevant NIST Publications

Relevant NIST publications are listed below for reference:

http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf (NIST SP 800-30-guide for conducting risk assessments)

http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf (NIST SP 800-37 - Guide for applying the RMF)

http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf (NIST SP 800-39 **-** Managing Information Security Risk)

http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf (FIPS 200 - Minimum Security Requirements for Federal Information and Information Systems)

http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf (NIST 800-53 Rev 4 – Security and Privacy Controls for Federal Information Systems and Organizations)

http://csrc.nist.gov/publications/nistpubs/800-64-Rev2/SP800-64-Revision2.pdf (SP 800-64 - Security Considerations in the systems development lifecycle)

http://csrc.nist.gov/publications/nistpubs/800-137/SP800-137-Final.pdf (SP 800-137 - Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations)

A full list of NIST SP Publications can be found at the NIST SP 800 series homepage http://csrc.nist.gov/publications/PubsSPs.html