CHAPTER

Integrated Organization-Wide Risk Management

3

TABLE OF CONTENTS

Chapter Overview and Key Learning Points **23**
Risk Management **23**
Risk Management and the RMF **24**
Components of Risk Management **25**
Framing the Risk 25
Risk Assessment 26
Risk Response 27
Monitoring Risk 27
Multi-tiered Risk Management **28**
Tier 1, Organizational Risk Management 28
Tier 2, Mission/Business Processes 30
Tier 3, Information System 31
Risk Executive (Function) **31**

INFORMATION IN THIS CHAPTER:

- How risk management integrates with the RMF
- The multi-tiered risk management process
- Introduction to the components of the risk management process
- Further development of the risk executive (function)

CHAPTER OVERVIEW AND KEY LEARNING POINTS

One of the biggest improvements introduced in the RMF is the way that risk is managed. The RMF stresses the use of a managed organization wide method of assessing and managing risk. This chapter will introduce the components of risk, multi-tiered risk management and a new position created for the RMF, the risk executive (agent).

RISK MANAGEMENT

To fully understand and successfully implement the risk management framework, one must have a complete understanding of how the organizational multi-tiered

risk management process is structured and used. This chapter discusses these concepts and how the RMF and organizational risk management techniques are interrelated. The chapter covers the three tiers of a typical multi-tiered organizational risk management process and describes the components of organizational risk management. It also introduces the risk executive (function) and explains this component's relationship to the RMF and risk management. Risk management is an extensive topic; this chapter only touches on the high points of the process. Several universities offer undergraduate degrees, postgraduate certificates, master's degrees, and even doctoral degrees in risk management. For-profit, non-profit, and not-for-profit organizations also have large investments of time, money, people and other resources in risk management that delve deeply into the theory and processes that encompass complete risk management. The intention of this chapter is not to make the reader an expert in risk management, but rather to introduce the basic components of risk management as defined by NIST and associate these with the RMF.

RISK MANAGEMENT AND THE RMF

Risk management and the risk management framework seem to be the same thing, but it is important to understand the distinction between the two. The risk management process is specifically detailed by NIST in three different volumes. NIST SP 800-30, *Guide for Conducting Risk Assessments*, provides an overview of how risk management fits into the system development life cycle (SDLC) and describes how to conduct risk assessments and how to mitigate risks. NIST SP 800-37 discusses the risk management framework that is the subject of this book; the guide is discussed in great detail in coming chapters. Finally, NIST SP 800-39, *Managing Information Security Risk*, defines the multi-tiered, organization-wide approach to risk management that is discussed in this chapter.

The older certification and accreditation (C&A) process had a number of shortcomings, including looking at risk only from the information systems perspective. This view focused on evaluating risks as they impacted a specific system, in a vacuum and does not address how the systems risks will impact larger business unit or the organization itself. In developing the RMF, members of the Joint Task Force Transformation Initiative, including members from NIST, determined that the best approach to risk management is to view risks at not only the system level, but also at the business unit level and the organizational level. This approach includes determining how the organizational risk picture may be impacted if a specific system is placed into the production environment. This evaluation takes place at three levels: the organizational level, or tier 1; the mission and business process level, or tier 2; and the system level, or tier 3, as illustrated in Figure 3-1. This holistic, multi-tiered, organizational view of risk assists senior leaders in determining how to effectively and efficiently manage risk in the most cost-effective manner across the entire organization.

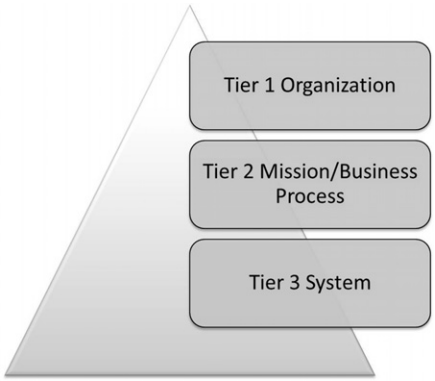

FIGURE 3-1

COMPONENTS OF RISK MANAGEMENT

Effective risk management is composed of four basic components: framing the risk, assessing the risk, responding to the risk, and monitoring the risk. Each component is interrelated and lines of communication go between them. The output from one component becomes the input to another component. Risk management is a process that must be ingrained across the entire organization, involving information system owners, developers, engineers, and administrators at the tactical level; mid-level planners and managers at the business unit level; and the organization's most senior leaders, who view risk at the strategic level as it impacts the entire organization. The leaders define the environment in which risk-based decisions are made and set the risk management process on a framework by developing a risk management strategy.

Framing the Risk

Leaders in the organizational tier establish the risk framework that the organization will use to define risk assumptions, risk constraints, risk tolerances, and risk priorities. Defining risk assumptions includes determining the likelihood that a vulnerability, threat, or occurrence could impact the organization and what the consequences or impact would be if it were to occur. Issues in the enterprise that restrict or slow risk assessments, risk response, or risk monitoring are categorized as risk constraints. Risk tolerances are those possible events or occurrences whose impacts on the organization are acceptable; often these risks are deemed acceptable because of the excessive cost of countering them. Finally, risk priorities are those events that must be protected against and systems that have a reduced risk tolerance. Many organizations prioritize system risk acceptance based on whether or not systems support critical business or mission functions, as these systems have the lowest risk tolerance and highest risk priority.

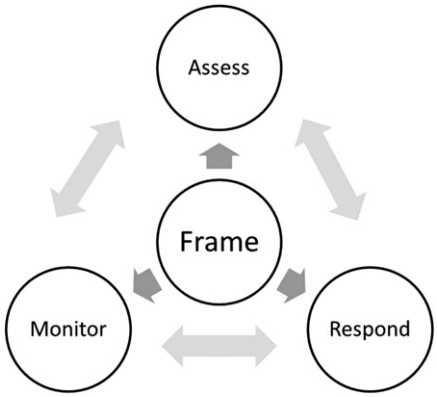

FIGURE 3-2

Figure 3-2 illustrates the interaction that each of the components of the risk management process has with each other. The risk framework helps to inform and drive each component of the risk management process assessment, monitoring, and response. By evaluating sources of threat information, either from open source information or through classified briefings (depending on the organization or environment), the risk management process is framed and acceptable values are developed for risk assumptions, risk constraints, risk tolerances, and risk priorities. The framing process also includes external risk relationships with other organizations that will accept the transfer of risk. For example, insurance carriers and stakeholders may be impacted by the organization's risk management process, as may suppliers, customers, served populations, mission/business partners, and service providers. These stakeholders can be either providers of risk management processes or consumers of the organization's protections from risk. Risk framing results in a critical output for the organization—the risk management strategy—which, like the risk assessment, is an input for the risk response component.

Risk Assessment

The risk assessment aims to draw a risk picture for the organization. This includes threats directed at the organization, the internal and external vulnerabilities the organization faces, and the harm that will come to the organization if a threat exploits a given vulnerability. The likelihood of the harm occurring is also evaluated and calculated in the risk assessment.

The organization's leaders determine various components in the risk assessment strategy, including the tools, techniques, and methodologies that will be used to develop the risk assessment; assumptions and constraints to the risk assessment; and the roles and responsibilities for various positions within the risk management process. The leadership also defines assumptions related to the risk picture, how risk and threat information is collected, the frequency of risk assessments at each tier, and

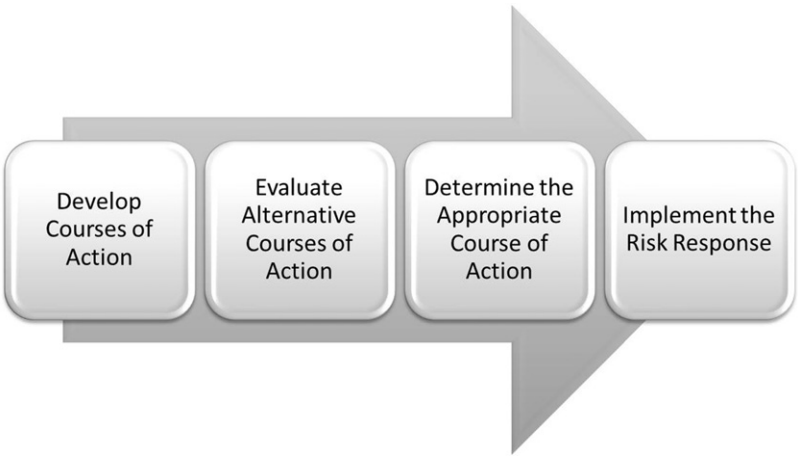

FIGURE 3-3

how risk assessments are conducted. Risk assessment results can drive changes to other components of the risk management process.

Risk Response

This component determines how the organization responds to a risk once it is identified. This identification normally is an input to the risk response from the risk assessment component in the form of the determination of risk, but can also come from the risk frame in the form of the risk management strategy described earlier. The risk response serves to provide an organization-wide, consistent response that addresses the risk frame. This includes developing courses of action, evaluating alternative courses of action, determining the appropriate course or courses of action, and implementing the risk response based on the selection. These steps are illustrated in Figure 3-3. The selection made has the potential to change the organization's risk procedure and, once made, the other components of the risk management process need to be evaluated for necessary changes.

Monitoring Risk

The final component of risk management determines how the organization monitors risk over time. This component validates that the risk program has implemented the planned risk response and that information security plans are derived from traceable mission/business functions. It also determines the effectiveness of ongoing risk response plans and determines and identifies changes in the environment that will impact the risk profile of the organization. The risk program can be modified as needed to respond to changes identified in the monitoring process. These changes initiate updates to the organization's risk assessment, risk response, and risk frame components.

MULTI-TIERED RISK MANAGEMENT

Tier 1, Organizational Risk Management

Organizational leadership is responsible for framing risks and developing the environment for which risk-based decisions will be made. These activities occur at tier 1 of the multi-tiered risk management process, commonly called the organizational tier. Tier 1 activities address risks at the organizational level and drive risk management at levels 2 and 3. These activities include defining the environment and developing an organizational risk management strategy. The leaders establish the risk foundation and define risk boundaries. Activities at the organizational tier also include updating the risk strategy to comply with legislation, directives, and policies as well as updating the risk frame to ensure that these requirements are properly addressed across the organization. The rapid requirement shifts that occur based on the changing threat and regulatory landscape require the organization's risk management process to remain flexible while providing direction to the organization; processes at lower tiers of the risk management process must also remain flexible.

A number of critical events occur at tier 1 that impact the organizational, business/mission, and system risk and security profiles. Common controls are selected by organizational leaders at this level; they also identify common control providers and determine the common control assessment schedule. Activities at this tier influence and guide the allocation of other security controls. Tier 1 activities also include determining the order of recovery should an incident occur and defining strategic goals. The risk executive (function) is a tier 1 function that supports risk management at all tiers.

Common controls are those controls that support more than one information system or process. They can be implemented at higher levels in the organization, typically at the business function or organizational levels, that support two or more information systems. These common controls can be managed by a common control provider and, once approved, can be offered to information system owners and other business functions in the organization, thereby reducing the cost and time spent developing these controls multiple times throughout the organization. Once the risk management principles, processes, and methodologies are developed at the organizational level, it is imperative that the leaders at this tier make the information available to the users, information system owners, and business leaders at lower levels in the organization. This allows the entire organization to develop risk management and risk decision-making processes using a common framework.

Developing an order of recovery should be part of the organization's overall risk management strategy and process. To develop this strategy, organizational leaders evaluate the organization's strategic mission and determine the criticality of each information system and process in the organization. The results are then prioritized, ensuring that those information systems having the highest impact to the stated mission are recovered first. Using this process, a listing of the systems is developed, with the most critical system at the top and descending by order of importance to the

organization's mission. If an event occurs that damages multiple systems in the organization, leaders at all levels can use this prioritized listing to determine where to devote critical resources and which systems will be recovered first. By defining strategic goals, the organization aligns its ongoing processes with not only these goals, but through them the mission of the organization. This provides a way to define risk that is synchronized with the organization's mission, ensuring that resources are placed for maximum benefit. Risks to the strategic goals, and therefore to the organization's mission, can be viewed with greater scrutiny.

Some activities that support the risk management framework and should take place at tier 1 are occasionally overlooked. These include fully defining roles and responsibilities; defining organizationally defined variables for security controls and enhancements; and defining terms such as custom terms, phrases, and acronyms used in the organization.

Key positions required by the risk management framework are defined in Chapter 7 and in NIST SP 800-37. It is important that tier 1 leaders support and promote these key positions. They must also identify individuals in the organization who will assume each role, add the role to the employee's job description or contractual requirements, and include in evaluations the individual's ability to perform that role. Positions that could be filled by an individual, a board, or a group, like the risk executive (function), should receive special scrutiny to ensure that each role's complete functionality is addressed.

NIST SP 800-53, *Recommended Security Controls for Federal Information Systems and Organizations*, currently defines over six hundred security controls and control enhancements that strengthen organizational and information systems security. Many of these controls were designed at a level that allows flexibility in implementation at the organizational level by providing organizationally defined variables. The organization must determine each variable's value before the risk management framework can be correctly implemented. For example, enhancement 1 of IA-5, Authenticator Management, is outlined below. The organization must define the variables named in the square brackets before the control enhancement can be properly implemented.

Control Enhancements:

1. The information system, for password-based authentication:
   - **a.** Enforces minimum password complexity of [Assignment: organization-defined requirements for case sensitivity, number of characters, mix of upper-case letters, lower-case letters, numbers, and special characters, including minimum requirements for each type];
   - **b.** Enforces at least a [Assignment: organization-defined number of changed characters] when new passwords are created;
   - **c.** Encrypts passwords in storage and in transmission;
   - **d.** Enforces password minimum and maximum lifetime restrictions of [Assignment: organization-defined numbers for lifetime minimum, lifetime maximum]; and
   - **e.** Prohibits password reuse for [Assignment: organization-defined number] generations.

In this example, the organization must define the minimum password complexity (part 1a), the number of characters changed when a new password is created (part 1b), the minimum and maximum password lifetime (part 1d), and rules on password reuse (part 1e). Defining these variables enables all information system developers across the organization to have a common set of requirements with which to build information systems. Defining these variables is also a requirement for the RMF itself and failure to do so will not only result in differences of requirement implementation across the enterprise, but will also cause information systems to fail the security control assessment for this enhancement.

Defining terms early in the risk management process helps reduce confusion when developing, documenting, and assessing the information system. Common terms often have different meanings to different people. NIST has developed a glossary of key information security terms, NIST IR 7298, which, at the time of this writing, is in draft form for revision 2. The Committee on National Security Systems (CNSS) produced a glossary titled *National Information Assurance (IA) Glossary*, CNSSI 4009, which is also under revision. Organizations can turn to these documents to begin building the organizational lexicon for common security and information systems terms. An organization can greatly assist system developers, technical writers, and assessors by defining its interpretations of these common terms. For example, how long is near-real time? What is the organization's definition of automatic versus automated?

Tier 2, Mission/Business Processes

Activities at tier 2 are associated with those activities that occur at the mission or business process level. This level in the organization has specific goals and tasks that ensure that the organization continues to function and key tasks are completed, thus ensuring that the organization remains viable. An example of a mission or business process level many readers are familiar with is the human resources (HR), or personnel, division of an organization. Activities typical at tier 2 include defining the mission or business need; prioritizing the mission or business processes; defining required information types; and incorporating and establishing technology solutions with required security components, which are integrated early in the process and incorporated into the enterprise architecture. Enterprise architecture decisions made at tier 2 determine the acceptable technology solutions that can be implemented at tier 3. Activities from tier 1 impact tier 2, activities at tier 2 impact tier 3, and tier 2 provides feedback to tier 1. This feedback could, and often does, result in changes to the organization's risk frame. Organizational leaders at tier 2 influence the allocation of certain security controls to specific components or information systems once they are implemented at tier 3, based on the organization's information protection needs. Leaders at this level may determine and define what technologies are acceptable for processing information that is derived from a specific business function. For this to be most successful, the selection of approved and prohibited technologies should be well-documented and distributed throughout the business unit and to information system owners, developers, and administrators who support the business function.

Tier 3, Information System

Tier 3 activities include categorizing the information system; allocating security controls; and managing the selection of allocated security controls, including continuous monitoring of these controls. The information system in this tier is central to the risk assessment process and is dependent on the correct and consistent allocation of security controls, including common controls, across each of the tiers in order to operate as efficiently and effectively as possible. These functions are normally completed by system owners, common control providers, system administrators, information system security engineers, and information systems security officers. Controls not allocated to tier 1 or tier 2 will be levied to the information system at tier 3. Operations at this tier provide feedback to tiers 1 and 2 and, like tier 2 activities, this feedback can drive changes to the organization's risk frame.

RISK EXECUTIVE (FUNCTION)

One of the most confusing positions introduced with the RMF is that of the risk executive (function). This is due to the uniqueness of the requirements of this function and the inability to map this function to a position that existed in the C&A process. While the risk executive (function) is normally located at tier 1, it provides risk management guidance to individuals at all tiers, including, but not limited to, senior leaders, executives, chief information security officers, authorizing officials, business process and information owners, enterprise architects, system security professionals, and system administrators. In this way, the risk executive (function) serves as the central point for information about the organization's risk management process and its current risk profile.

The risk executive (function) must look at risk from the organizational perspective across a number of unique domains, including information security, personnel security, physical security, and budget. Because of the complex and differing knowledge required, the function can be a group—normally, a board—or a person, or an office supported by an expert staff or group within the organization who has expert knowledge of the required domains. According to NIST SP 800-39, the risk executive (function) coordinates with senior leaders and executives to:

- Establish risk management roles and responsibilities;
- Develop and implement an organization-wide risk management strategy that guides and informs organizational risk decisions (including how risk is framed, assessed, responded to, and monitored over time);
- Manage threat and vulnerability information with regard to organizational information systems and the environments in which the systems operate;
- Establish organization-wide forums to consider all types and sources of risk (including aggregated risk);
- Determine organizational risk based on the aggregated risk from the operation and use of information systems and the respective environments of operation;

- Provide oversight for the risk management activities carried out by organizations to ensure consistent and effective risk-based decisions;
- Develop a greater understanding of risk with regard to the strategic view of organizations and their integrated operations;
- Establish effective vehicles and serve as a focal point for communicating and sharing risk related information among key stakeholders internally and externally to organizations;
- Specify the degree of autonomy for subordinate organizations permitted by parent organizations with regard to framing, assessing, responding to, and monitoring risk;
- Promote cooperation and collaboration among authorizing officials to include security authorization actions requiring shared responsibility (e.g., joint/leveraged authorizations);
- Ensure that security authorization decisions consider all factors necessary for mission and business success; and
- Ensure shared responsibility for supporting organizational missions and business functions using external providers receives the needed visibility and is elevated to appropriate decision making authorities.

Based on the extensive requirements of this function, it is hard to find a single individual with the required knowledge and skillset. Therefore, many organizations have established executive boards, steering committees, or executive leadership councils with the required support staff to fulfill the duties of this function. Members of these groups should have expert knowledge in one or more areas that include security and risk assessment experience in several domains of security such as information security, personnel security, or physical security. In addition to security professionals, many boards include budget, privacy, and document professionals as well as members of the organization's legal team. Most small organizations do not have the ability to develop a full board to serve as the risk executive (function), but the panel should be staffed with as many professionals as possible who have the required knowledge.