ELECTRICITY SECTOR CYBERSECURITY RISK MANAGEMENT PROCESS GUIDELINE

U.S. Department of Energy

SEPTEMBER 2011

24

Acknowledgments

This risk management process (RMP) guideline was developed by the Department of Energy (DOE), in collaboration with the National Institute of Standards and Technology (NIST) and the North American Electric Reliability Corporation (NERC). Members of industry (utilities and vendors) and utility-specific trade groups were included in authoring guidance that would be meaningful and reflect industry advice. The primary goal of this guideline is to describe an RMP that is tuned to the specific needs of Electricity Sector organizations. The NIST Special Publication (SP) 800-39, *Managing Information Security Risk*, provides the foundational methodology for this document. The NIST Interagency Report (NISTIR) 7628, *Guidelines for Smart Grid Cyber Security*, and NERC critical infrastructure cyber security standards provide a strong foundation for the development of cybersecurity guidelines that will further refine the definition and application of effective cybersecurity for all organizations in the Electricity Sector. The NERC Critical Infrastructure Protection (CIP) cybersecurity standards are outside the scope of this guideline.

The DOE wishes to acknowledge and thank the senior leaders from the DOE, NIST, NERC, and the members of the core development and subject matter expert teams who participated in the development of this guideline. The senior leaders, the core development and subject matter expert team members, and their organizational affiliations include:

Department of Energy
Patricia Hoffman
Assistant Secretary, Office of Electricity Delivery and Energy Reliability

National Institute of Standards and Technology
Cita M. Furlani
Director, Information Technology Laboratory

William C. Barker
Cyber Security Advisor, Information Technology Laboratory

Donna Dodson
Chief, Computer Security Division

George Arnold
National Coordinator for Smart Grid Interoperability

North American Electric Reliability Corporation
Mark Weatherford
Chief Security Officer

Risk Management Process Core Development Team

Tanya Brewer
National Institute of Standards and Technology

Bob Caldwell
Edgewater

Rocky Campione
Planet Technologies

Paul Crist
Lincoln Electric System

Rick Dakin
Coalfire Systems

Dave Dalva
Smart Grid Interoperability Panel Cyber Security Working Group

Cameron Doherty
Southern California Edison

Summer Esquerre
NextEra Energy, Inc.

Susan Farrand
Department of Energy

Win Gaulding
Northrop Grumman Corporation

Brian Harrell
North American Electric Reliability Corporation

William Hunteman
Department of Energy

Lisa Kaiser
Department of Homeland Security

Matthew Light
Department of Energy

John Lim
Consolidated Edison

Samara Moore
Department of Energy

David Norton
Federal Energy Regulatory Commission

Scott Saunders
Sacramento Municipality Utility District

Sean Sherman
Arctic Slope Regional Corporation

Marianne Swanson
National Institute of Standards and Technology

Bill Watson
Edgewater

Ken Watson
Information Technology Sector Coordinating Council

Victoria Yan
Booz Allen Hamilton

63
64
65 **Risk Management Process Subject Matter Expert Team**

James Brenton
Electric Reliability Council of Texas

James Gilsinn
National Institute of Standards and Technology

Neil Greenfield
American Electric Power

Felix Kwamena
Natural Resources Canada

Scott Mix
North American Electric Reliability Corporation

Brian Evans-Mongeon
Utility Services, Inc.

Reynaldo Deleon
Southern California Edison

66

67

CAUTIONARY NOTE

INTENDED SCOPE AND USE OF THIS PUBLICATION

The guidance provided in this publication is intended to address *only* the management of cybersecurity-related risk derived from or associated with the operation and use of information technology and industrial control systems and/or the environments in which they operate. The guidance is *not* intended to replace or subsume other risk-related activities, programs, processes, or approaches that Electricity Sector organizations have implemented or intend to implement addressing areas of risk management covered by other legislation, regulation, policies, programmatic initiatives, or mission and business requirements. Additionally, this guidance is not part of any regulatory framework. Rather, the cybersecurity risk management process guidance described herein is complementary to and should be used as part of a more comprehensive enterprise risk management program.

CONTENTS

List of Figures

List of Tables

1. Introduction

Electricity is widely recognized as a basic necessity for all citizens. It powers economies, consumer conveniences, national security capabilities and industrial production to deliver competitive advantages in global markets. Electric power systems are rapidly becoming the target of cyber terrorists, criminals, and industry insiders. Whether caused willingly or unknowingly, damage to these systems can have a direct effect on the economic and national security interests of all nations.[1]

Over the past few decades, the Electricity Sector has become increasingly dependent on digital technology to reduce costs, increase efficiency and maintain reliability during the generation, transmission and distribution of electric power. The information technology[2] (IT) and industrial control systems[3] (ICS) that utilize digital technology could be as vulnerable to malicious attacks and misuse as other technology infrastructures. The defense of this integrated power system requires constant vigilance and expertise. This is because ICS are now being integrated with traditional business IT that provide corporate services; data and information produced in the operation of ICS increasingly used to support business decision making processes. This has been witnessed with the introduction of Transmission Control Protocol/Internet Protocol (TCP/IP) networking technology in ICS devices, connection of operations systems to back-office and Internet-connected networks, and the development of home-level and distribution systems automation that crosses the line between traditional operations and "public" networks. Emerging technologies that drive the Smart Grid will add even more IT to energy management systems, ICS, and business systems. These innovations will provide utilities and Electricity Sector organizations with more control of devices and information throughout the grid. Organizations[4] in the Electricity Sector will depend on these integrated IT and ICS to successfully carry out their mission and business functions.

Historically, ICS were composed of proprietary technologies with limited connection to an organization's corporate networks or the Internet. In today's world, the efficiencies of Commercial Off-the-Shelf (COTS) hardware and software platforms, interconnected public and private networks, and remote support are moving organizations from an isolated environment into a global, interconnected environment. Thus, Electricity Sector organizations recognize these efficiencies represent new cybersecurity risks that were not present in their isolated environment. The evolution of ICS from proprietary to COTS platforms, has also introduced Electricity Sector organizations to new cybersecurity risks as illustrated by targeted malware against COTS platforms in the IT sector. Consequently, ICS deployed to support mission critical operations in the Electricity Sector can potentially be compromised and result in significant negative impact on operations.

[1] This is the Electricity Sector Critical Infrastructure defined by Homeland Security Presidential Directive (HSPD) – 7 Critical Infrastructure Protection Plans and the Canadian National Strategy for Critical Infrastructure.

[2] IT is a discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. In the context of this publication, the definition includes interconnected or dependent business systems and the environment in which they operate (i.e., people, processes, technologies, and facilities).

[3] An ICS is a set of hardware and software acting in concert that manages the behavior of other devices in the electrical grid.

[4] The term organization describes an Electricity Sector organization of any size, complexity, or positioning within an organizational structure (e.g., any independent company that is a stakeholder in the grid operation) that is charged with carrying out assigned mission and business processes and that uses IT and ICSs in support of those processes.

All IT and ICS have vulnerabilities that are subject to threat actors[5] who either intentionally or unintentionally (accidently) disrupt organizational operations, take revenge for perceived wrongdoings, or have means to perpetrate acts of terrorism. The increase in potential vulnerabilities, resulting from the use of COTS platforms, coupled with an increasing threat environment, results in increased risk to the Electricity Sector. The increasing number of vulnerabilities as well as the interconnectedness of systems could serve as a blueprint for attackers who wish to access controllers, safety systems, critical decision data, support systems, and physical and cybersecurity systems. This can cause damage to an Electricity Sector organization's assets or individuals, and can even compromise the reliable delivery of electricity.[6]

> The highly publicized Stuxnet threat is an example of how a complex threat can be crafted using elements of vulnerabilities within the Windows operating system to reach into an ICS management application, running on a COTS platform, and penetrate a managed element of the ICS (in this case, a programmable logic controller). Stuxnet can be considered a game changer because this type of threat blends social engineering with the use of the additional attack vector of USB drives, commonly used in plant maintenance practices, COTS vulnerabilities, and ICS application vulnerabilities to directly compromise a much targeted physical control device.

The establishment and continued refinement of enterprise risk management (ERM) programs, policies, and processes to prepare for, react to, and recover from adverse cybersecurity events must continue to be a high priority for the industry. Although the electricity delivery system has not yet experienced widespread debilitating cyber attacks, its reliance on the previous strategies of physical separation between the ICS environment and the business and administrative networks is no longer adequate to satisfy today's mission and business needs. This guideline provides a methodology that organizations can implement to manage the increased risks that these new technologies are introducing into the Electricity Sector.

The role of managing cybersecurity risk[7] from the operation and use of IT and ICS is critical to the success of organizations in achieving their strategic goals and objectives, including resiliency, reliability, and safety. This guideline is designed to build on an organization's existing cybersecurity policies and procedures, help organize and clarify risk management goals, and provide a consistent approach in which to make risk decisions. This guideline will provide vendors and supporting organizations a vision into the cybersecurity challenges of the Electricity Sector and aid in developing secure solutions.

The successful application of this guideline will result in the ability of an Electricity Sector organization to:

- Effectively and efficiently implement a risk management process (RMP) across the whole organization;
- Establish the organizational tolerance for risk and communicate throughout the organization including guidance on how risk tolerance impacts ongoing decision making;
- Prioritize and allocate resources for managing cybersecurity risk;[8]

[5] For additional information, see US-CERT Cyber Threat Source Descriptions.

[6] The North American Electric Reliability Corporation (NERC) Reliability Functional Model provides the framework for the development and applicability of NERC's Reliability Standards.

[7] Unless otherwise stated, references to risk in this publication refer to cybersecurity risk derived from the operation and use of organizational systems including the processes, procedures, and structures within organizations that influence or affect the design, development, implementation, and ongoing operation of IT and ICS. The aggregation of different types of risk across the organization is beyond the scope of this publication.

[8] Resources is defined as money, materials, staff, and other assets that can be utilized by an Electricity Sector organization in order to meet its mission and business objectives.

- Create an organizational climate in which cybersecurity risk is considered within the context of the mission and business objectives of the organization; and
- Improve the understanding of cybersecurity risk and how these risks potentially impact the mission and business success of the organization.

To successfully execute organizational mission and business functions in the Electricity Sector with IT and ICS processes, leadership must be committed to making risk management a fundamental mission and business requirement. Understanding and handling cybersecurity risk is a strategic capability and an enabler of efficient and sustained mission and business objectives across all Electricity Sector organizations. In the context of this document, the use of the term risk management will imply cybersecurity risk management unless specifically qualified as ERM.

2. Cybersecurity Risk Management Overview

Electricity Sector organizations deal with risk every day. As a result, these organizations must develop processes to evaluate the risk of any activity, then mitigate or accept the risk as a cost of operating and carrying out their mission. To this end, these organizations have developed enterprise risk management processes and strategies to define how they will address the inherent risk in accomplishing their missions.

Risk management is defined as the program and supporting processes used to manage cybersecurity risk to an organization's operations. [9] In order to effectively perform risk management, an organization must have a thorough understanding of their people, processes, and technology, as well as an understanding of how they enable the mission and communication throughout the organization. It is critical to not only understand the processes but also to enable the communications that facilitate information sharing. In this model, we utilize a three-tier approach to integrating the Risk Management Plan (RMP) within an organization. Risk management is a continuous process, and one that needs to be regularly evaluated to ensure the latest threats, vulnerabilities, and mitigation strategies are addressed.

The model presented in this document is meant to take this routine process and formalize it to ensure that risks are identified appropriately and responded to in a way that best carries out the mission of the organization. This is a shared responsibility at every level in the organization, from daily operations to the most senior executives in the organization.

2.1 Risk Management Model

The risk management model[10] presented in this document is a three-tiered structure that provides a comprehensive view for the Electricity Sector organization on how risk management activities are undertaken across an organization. This structure is simple enough that it can be applied to any Electricity Sector organization regardless of size or operations. The three tiers of the risk management model are:

- Tier 1: Organization;
- Tier 2: Mission and Business Process; and
- Tier 3: Information technology (IT) and industrial control systems (ICS).

A key component of the risk management model is the identification of mission and business processes and the communications between well-defined organizational boundaries. Decisions being made within one organizational mission or business unit could have an effect on the rest of the organization's units. The model is meant to be applied using a "top-down" approach, where the activities an Electricity Sector organization starts from a strategic focus in Tier 1 and shifts to a tactical focus in Tier 3. Figure 1 illustrates the tiered risk management model and once complete reflects an organization's cybersecurity risk management strategy[11] and its risk evaluation.[12]

[9] Adapted from CNSSI-4009.

[10] NIST Special Publication (SP) 800-39, *Managing Information Security Risk*, provides the definition and the foundational methodology used in this document.

[11] A risk management strategy includes any strategic-level decisions on how risks to an organization's operations, assets, individuals, and other organizations are managed by senior business/executives.

[12] Risk evaluation is a component of the risk assessment element in which observations are made regarding the significance and acceptability of risk to the organization.

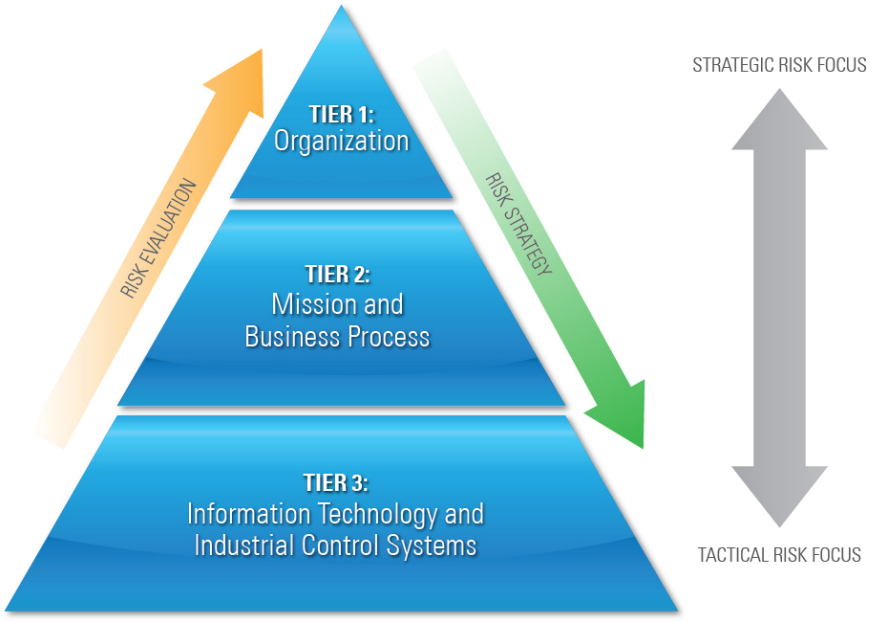

Figure 1: Risk Management Model

2.1.1 Tier 1: Organization

Tier 1 addresses risk from an organizational perspective by establishing and implementing governance structures that are consistent with the strategic goals and objectives of the Electricity Sector organization. Governance[13] structures provide oversight for the risk management activities conducted by an organization. The risk management decisions at Tier 1 provide direct inputs to the activities carried out at Tier 2 and Tier 3. The Tier 1 risk management activities may include:

- Establishing and implementing a risk governance structure;
- Prioritizing mission and business functions that drive investment decisions;
- Establishing the organization's risk tolerance;
- Defining techniques and methodologies for assessing cybersecurity risk;
- Defining risk constraints and requirements;
- Establishing the recovery order for critical mission and business processes; and
- Establishing the Electricity Sector organization's cybersecurity risk management strategy.[14]

2.1.2 Tier 2: Mission and Business Processes

Tier 2 addresses risk from a mission and business process perspective, based on the risk management strategy and other activities of Tier 1. This tier focuses on the mission and business processes of an Electricity Sector organization and both informs and is informed by the IT and ICS technical architecture. Tier 2 decisions are direct inputs to activities in Tier 3, while also providing feedback to Tier 1. The business involved in this tier is that of operational management; in some Electricity Sector organizations

[13] Additional information regarding the responsibilities of organizational officials can be found in Appendix F, Governance Models.

[14] The cybersecurity risk management strategy is a component within an organization's enterprise risk management strategy. The enterprise risk management strategy may consist of additional risk strategy components for program management risk, investment risk, budgetary risk, legal liability risk, safety risk, inventory risk, or supply chain risk, in addition to a cybersecurity risk management strategy.

this will be the same as the executive management, but the analysis of cybersecurity risk at this level is focused on the execution of mission and business processes. The risk management activities for Tier 2 may include:

- Identifying and defining mission and business processes and assets necessary to support the functions of an Electricity Sector organization defined in Tier 1;
- Prioritizing the mission and business processes with respect to the strategic goals and objectives of an Electricity Sector organization defined at Tier 1;
- Identifying cybersecurity processes needed to successfully execute the mission and business processes;
- Incorporating cybersecurity requirements[15] into the mission and business processes;
- Developing a disciplined and structured approach for managing IT and ICS assets that support the mission and business processes; and
- Providing a clear and concise roadmap to (1) allow traceability from the highest level strategic goals and objectives of the organization; (2) ensure that mission and business process-driven cybersecurity requirements and protections are defined, implemented, maintained and monitored; and (3) promote cost-effective, efficient, and resilient IT and ICS.

2.1.3 Tier 3: Information Technology and Industrial Control Systems

Tier 3 addresses risk from an IT and ICS perspective and is guided and informed by the activities from Tiers 1 and 2. Tier 3 activities lead to the selection, deployment, and monitoring of cybersecurity controls (safeguards and countermeasures) at the system level. The cybersecurity controls are subsequently allocated to the various components of the IT and ICS in accordance with the cybersecurity architecture[16] developed by the organization. Activities at this level will provide risk performance and policy compliance feedback to Tier 2 and then Tier 1. The Tier 3 risk management activities may include:

- Categorizing IT and ICS into levels by risk and value;
- Allocating cybersecurity controls to systems and the environments in which they operate;
- Managing the selection, implementation, assessment, and monitoring of cybersecurity controls; and
- Establishing a process to routinely reassess a system's cybersecurity posture based on new threat information, vulnerabilities, or system changes.

The inclusion of traditional methods to address risk and controls in a structured method is part of the risk management at Tier 3. This impacts the system lifecycle from development through disposal.

2.2 Risk Management Cycle

The risk management cycle is not static but a continuous process, constantly re-informed by the changing risk landscape as well as by organizational priorities and functional changes. The risk management cycle provides four elements that structure an organization's approach to risk management, as represented in

[15] Cybersecurity requirements can be obtained from a variety of sources (e.g., legislation, policies, regulations, standards, and organizational mission and business requirements).

[16] Cybersecurity architecture is a component of the enterprise architecture that describes the structure and behavior for an enterprise's cybersecurity processes, cybersecurity systems, personnel, and organizational units, showing their alignment with the enterprise's mission and strategic plans.

Figure 2:

- Frame;
- Assess;
- Respond; and
- Monitor.

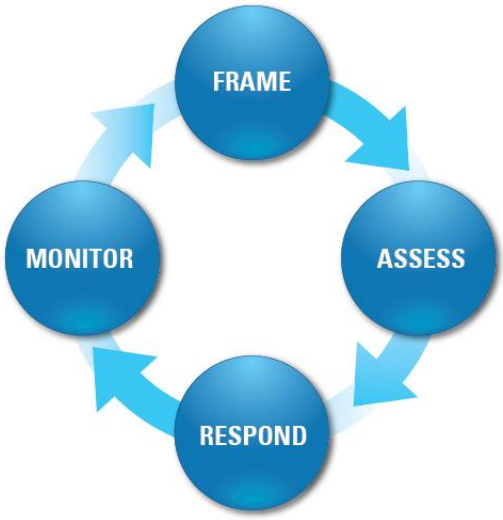

Figure 2: Risk Management Cycle

The risk management cycle is a comprehensive process that requires organizations to (i) frame risk (i.e., establish the context for risk-based decisions), (ii) assess risk, (iii) respond to risk once determined, and (iv) monitor risk on an ongoing basis, using effective organizational communications and a feedback loop for continuous improvement in the risk-related activities of organizations. Risk management is carried out as a holistic, organization-wide activity that addresses risk from the strategic level to the tactical level, ensuring that risk-based decision-making is integrated into every aspect of the organization. The following sections briefly describe each of the four risk management components.

The output of the risk management cycle is a risk management strategy that addresses how an Electricity Sector organization intends to frame, assess, respond to, and monitor risk. The risk management strategy makes explicit and transparent the risk perceptions that an organization in the Electricity Sector routinely uses in making investment and operational decisions.

The following sections provide brief descriptions of each of the four elements in the risk management cycle and the various activities that occur within each element.

2.2.1 Risk Framing

Risk framing must include third parties that are provided access to sensitive data and critical systems. For example, vendors may need access to systems to provide updates and support but the risks they introduce could impact subsequent risk analysis and mitigation strategies.

The risk-framing element describes the environment in which risk-based decisions are made. Establishing a realistic and credible risk frame requires that organizations in the Electricity Sector, identify:

- Assumptions about threats, vulnerabilities, consequences, impacts, and likelihood of occurrence;
- Constraints imposed by legislation, regulation, resource limitations, and other factors identified by the organization;
- Risk tolerance which identifies levels of risk, types of risk, and the degree of risk uncertainty that is acceptable;
- Priorities within mission and business functions, and trade-offs among different types of risk across those functions; and
- Trust relationships, such as physical interconnections, third-party billing organizations, reciprocity agreements, or device vendors.[17]

[17] For many Electricity Sector organizations, external risk relationships are not managed to the same degree as those directly impacting that organization. Each organization must take steps to be aware of the potential for risk from external relationships to ensure that it does not impose undue risks on others. Additional information regarding the responsibilities of organizational officials can be found in Appendix G, Trust Models.

Trust relationships and organizational culture influence the risk management elements and the risk management model. Changes in mission and business requirements may require a greater acceptance of risk and/or additional measures to establish and/or build trust. Such measures facilitate building trust and evolving organizational cultural values, beliefs, and norms over the longer term. Additional information on trust and organization culture can be found in Appendix G.

The ever broadening reliance upon globally sourced equipment exposes IT, ICS and networks to an enlarging risk of exploitation through counterfeit materials, malicious software, or untrustworthy products. A supplier of IT or ICS components is also an acquirer of sub-components that make up their products. To obtain a level of trust, each organization that performs the role of an acquirer conducts supply chain risk management activities and flows down those supply chain requirements to its sub-tiers.

2.2.2 Risk Assessment

The risk assessment element identifies, prioritizes, and estimates risk to an organization's operations, assets, individuals, and other interconnected Electricity Sector organizations. This is done through the risk context created in the risk-framing element. The purpose of the risk assessment element is for organizations to identify and evaluate:

- Threats (to operations, assets, or individuals);
- Vulnerabilities[18] (to operations, assets, or individuals);
- Impact (consequence or opportunity); and
- Likelihood (probability or frequency an event will occur).

To support the risk assessment element, organizations identify:

- Tools, techniques, and methodologies that are used to assess risk;
- Assumptions related to risk assessments;
- Constraints that may affect risk assessments;
- Roles and responsibilities[19] related to risk assessment;
- Risk assessment information to be collected, processed, and communicated; and
- Threat information to be obtained.

2.2.3 Risk Response

The risk response element addresses how an Electricity Sector organization responds to risk once that risk is assessed. The purpose of the risk response element is to provide a consistent, organization-wide response to risk in accordance with the risk framing and risk assessment elements to:

- Develop alternative courses of action for responding to risk;
- Evaluate the alternative courses of action;
- Determine appropriate courses of action consistent with the organization's risk tolerance level; and
- Implement the courses of action.

[18] Vulnerabilities are not confined to IT and ICSs but can also include vulnerabilities in governance structures, mission and business processes, enterprise and cybersecurity architectures, facilities, equipment, supply chain activities, and external service providers.

[19] Additional information regarding the responsibilities of organizational officials can be found in Appendix D, Roles and Responsibilities.

The output of the risk response element includes the risk management strategy and describes the types of risk responses that may be implemented (i.e., accepting, avoiding, mitigating, sharing, or transferring risk); the process to evaluate courses of action; the communication methods used across an organization and to external organizations (e.g., external service providers, supply chain partners) for those risk responses; and the tools, techniques, and methodologies used to develop courses of action for responding to risk.

It may be determined through a cost-benefit analysis that during the risk response element certain requirements are not feasible to implement, are cost prohibitive, or are not relevant to Electricity Sector operations. In this event, the risk monitoring cycle may require a reevaluation of the framing or assessment elements. It may also require compensating controls to manage the risk in an acceptable way to meet the spirit of the requirements.

2.2.4 Risk Monitoring

The risk monitoring element addresses how risks are monitored and communicated over time in an Electricity Sector organization. The purpose of the risk-monitoring element is to:

- Verify that risk response measures are implemented and that the cybersecurity requirements derived from the risk strategy are satisfied;
- Determine the ongoing effectiveness of risk response measures;
- Identify changes that may impact risk to an organization's IT and ICS and its environment;[20] and
- Describe the monitoring process to assess how change impacts the effectiveness of risk responses.

2.3 Risk Management Process

The RMP shown in Figure 3 is based on integrating the risk management cycle shown in Figure 2 at each business tier in the risk management model shown in Figure 1. The goals of this process are to improve risk-assessment, awareness, and security behavior at all levels of an organization. To facilitate these goals, further sections of this document will elaborate on the activities and artifacts recommended to focus leaders, managers, security, and IT and ICS personnel on the practices of a strong risk program. The artifacts will help to promote communications between

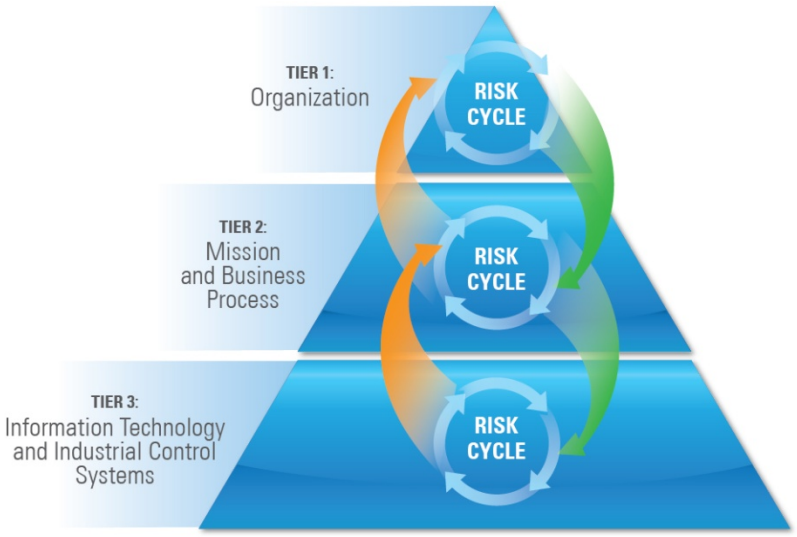

Table 1: Risk Management Process

[20] Environments of operation include, but are not limited to the threat space; vulnerabilities; mission and business functions; mission and business processes; enterprise and cybersecurity architectures; ITs; personnel; facilities; supply chain relationships; organizational governance and culture; procurement and acquisition processes; organizational policies and procedures; and organizational assumptions, constraints, risk tolerance, and priorities and trade-offs.

stakeholders, maintain focus on cybersecurity risk and security topics, and provide a basis for risk analysis and risk mitigation. The process is designed to (1) accommodate any size or type of organization, (2) support a mission and business focus "top- down" approach, and (3) support the objectives of integrating a security mindset and improving risk communications into the organization.

The RMP assumes little about the size or type of organization, but it does assume that the functions of leadership (Tier 1), business management (Tier 2), and systems management (Tier 3) are similar in all Electricity Sector organizations.

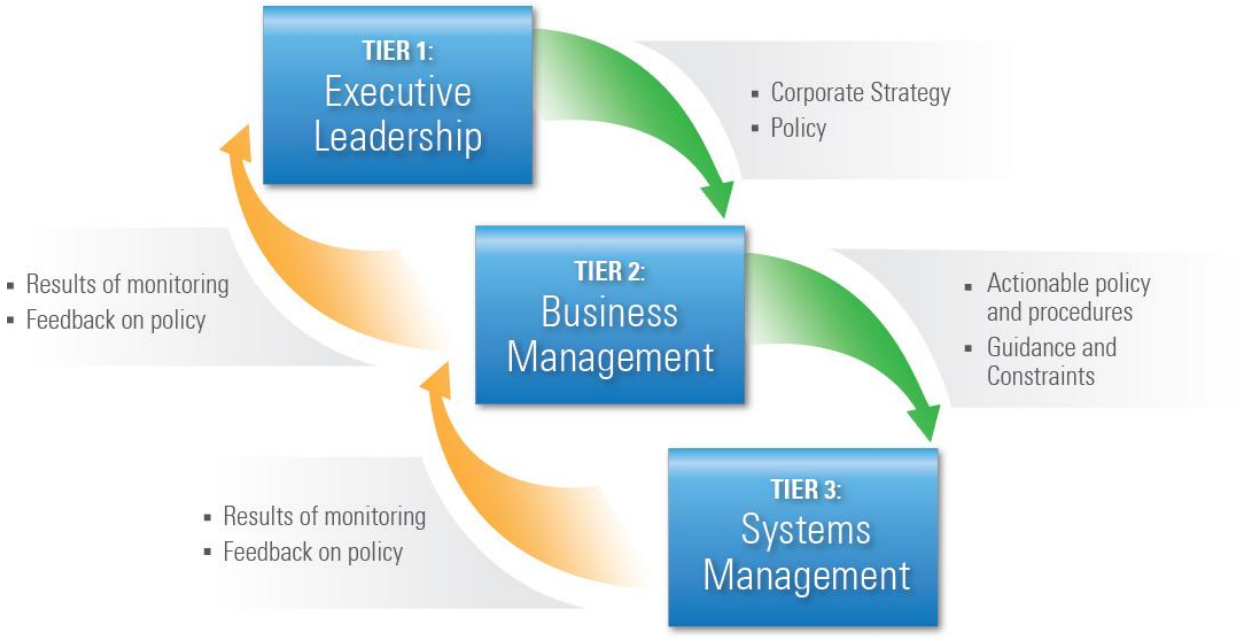

Figure 3: RMP Information Flowchart

As Figure 3 shows, each tier has within it an execution of the risk management cycle. The cycle elements (frame-assess-respond-monitor) each produce outputs that become inputs to the next element. The RMP represents how the output(s) from the risk assessment element in Tier 1 or Tier 2 become inputs to the risk framing element in Tier 2 or Tier 3.

As illustrated in Figure 4, the risk management cycle would be applied first at Tier 1 and complete the cycle, at least once, from risk framing to risk monitoring, before implementing the RMP at Tier 2 and then Tier 3. However, it is recognized that this does not correspond to the real world, and it is up to each Electricity Sector organization to determine which tier to first apply the risk management cycle, based on its governance structure, policies, costs, and resources. Regardless of where the organization has started, the outputs of this process will be valuable to the risk management of the organization and support the process goals.

Understanding that the flow of information in the RMP is bi-directional helps the organization understand that this process is flexible and informative. The results of elements at each tier support and enhance the risk program. Figure 4 shows the flow of information to and from each tier in greater detail than Figure 3.The main outputs from Tier 1 serving as inputs to Tier 2 are organizational strategies and policies. These strategies will address the overall goals and objectives of the organization's RMP; the organization's overall tolerance for risk; and how the organization intends to assess, respond to, and monitor risks. These artifacts also set the tone for security within the organization. Organizational policies

stem from these strategies and reflect decisions that affect the implementation of the RMP. These are generally nontechnical policies that relate to management structure, financial implications, and external regulation or compliance requirements.

Tier 2 provides feedback to Tier 1 in the form of consolidated results from monitoring the Tier 2 and Tier 3 activities and knowledge gained from applying organizational policies. As the organization develops mission and business process policies and procedures at Tier 2, it may find that there are organizational-level policies that may be possible but impractical to implement. This feedback from Tier 2 will allow the organizational managers at Tier 1 to determine whether the return on investment outweighs the expense of implementing the organizational policies. The main outputs from Tier 2, serving as inputs to Tier 3, will be programmatic and business policies, practices, and procedures. These will provide input for those personnel actually implementing the security program and countermeasures at Tier 3. The programmatic and business policies, practices, and procedures will also dictate how the performance of the systems will be measured. These metrics will have an impact on the specific controls, mitigation, and countermeasures chosen at Tier 3.

	TIER 1 The Organization	TIER 2 Mission & Business Processes	TIER 3 Information Technology & Industrial Control Systems
RISK FRAMING	Produce a description of the environment; e.g., generation assets, transmission operations, distribution end-points, etc.	Establish the cybersecurity architecture and type of risk assessment. Evaluate operational impacts for prioritization.	Identify the components, systems, hardware, and software of the information technology and industrial control systems.
RISK ASSESSMENT	Identify mission, resources, and functions in order to prioritize strategies and establish risk methodology.	Conduct the mission and business-specific risk management producing a risk-prioritized list of processes.	Provide the list of controls, controls implementation, and the cybersecurity plan.
RISK RESPONSE	Decide on the appropriate courses of action to accept, avoid, mitigate, share, or transfer risk.	Use risk-prioritized list of elements, assumptions, and constrains, to establish cybersecurity architecture	Produce a report based on the findings and recommendations of the cybersecurity assessment report. Produce tasks to correct any weaknesses or deficiencies in the cybersecurity controls.
RISK MONITORING	Evaluate in context with entire enterprise, multiple systems, and all relevant mitigation controls.	Measure the effectiveness of and level of conformance with the cybersecurity architecture.	Monitor change activities and ongoing assessment and remedial action activities.

Table 2: Risk Management Plan Overview

Tier 3 provides feedback to Tier 2 in the form of consolidated results from monitoring Tier 3 activities and specific information about effects of programmatic and business policies, practices, and procedures. As an organization takes the organizational policies from Tier 1 and transforms them into actionable policies, procedures and practices at Tier 2, input will be needed from Tier 3 on the ability to implement the desired policies, procedures, and practices with the existing set of countermeasures available. The

decision makers at Tier 2 need feedback from Tier 3 to understand the cybersecurity capabilities and the possible costs associated with those countermeasures.

The RMP helps define and promote a common understanding of risk tolerance and risk policy to be communicated. Because the process starts or includes the highest management levels of a business, it supports a top-down approach that incorporates business goals and objectives. It also benefits an organization by supporting risk program communications that allows for risk performance and policy compliance to be communicated and aggregated from the bottom-up (Tier 3 to Tier 2 to Tier 1).

2.4 Document Organization

The remainder of this document discusses how the risk management cycle applies to each of the tiers with additional supporting information provided in the appendixes. The chapters describe the inputs, activities, and outputs of each element within the risk management cycle, including those from other tiers. At the end of each chapter, a table summarizing the inputs, activities, and outputs is provided.

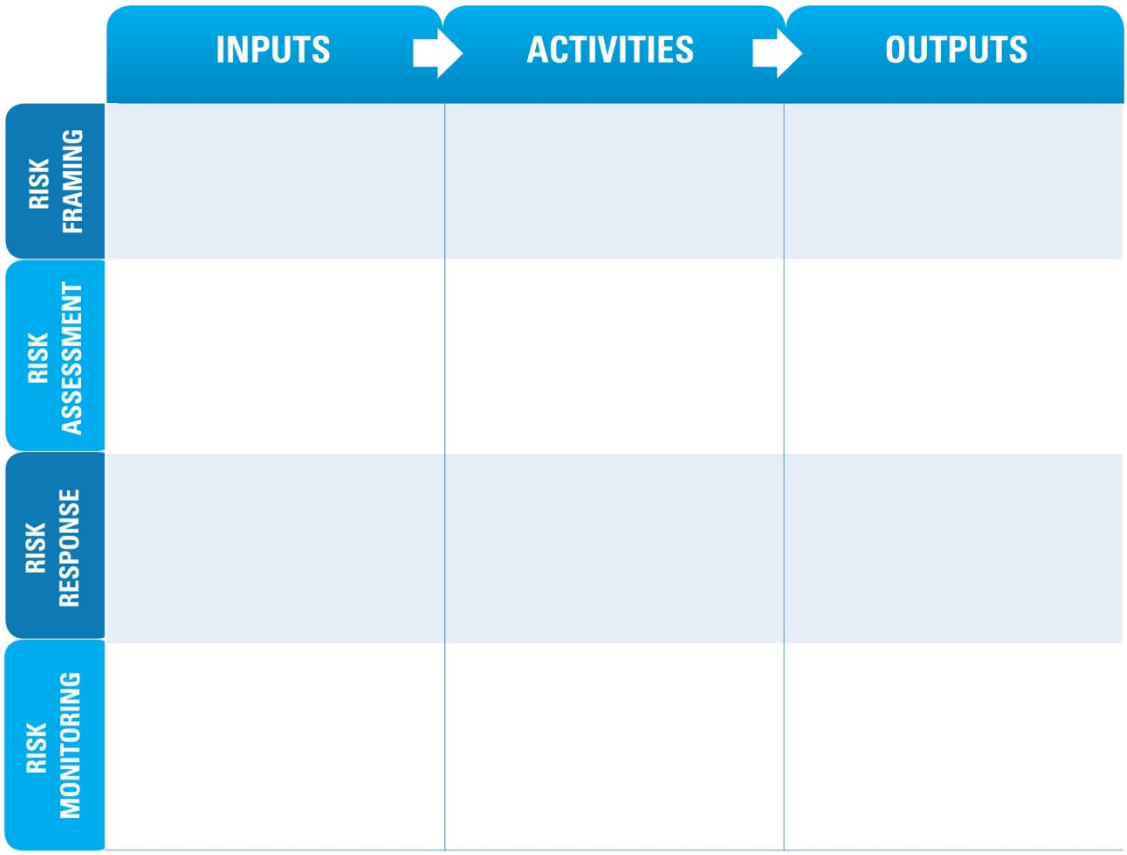

Table 3: Sample Inputs, Activities and Outputs

3. TIER 1: THE ELECTRICITY SECTOR ORGANIZATION

This chapter will address the RMP at the Organization Tier (Tier 1) of the risk management model. As described in Chapter 2, each tier of the model performs a similar process to define and refine risk information, develop a risk management strategy, and enhance the cybersecurity posture of an Electricity Sector organization.

Regardless of the size or type of an organization in the Electricity Sector, senior executives are responsible for how cybersecurity risk impacts the organization's mission and business functions. As part of governance, each organization establishes a risk executive function that develops an organization-wide strategy to address risks and set direction from the top, establishing accountability. The risk executive is a functional role established within organizations to provide a more comprehensive, organization-wide approach to risk management. This could exist as a collection of executive managers, board of directors, or committee of a co-operative organization. The function serves as the common risk management resource for senior leaders or executives, mission and business owners, chief information officers (CIOs), chief information security officers, information system owners, enterprise architects, cybersecurity architects, and any other stakeholders having a vested interest in the mission and business success of organizations. Managers at all three tiers then apply this risk management strategy to their mission and business processes and the IT and ICS that support them.

The RMP requires consultation between the senior executive leadership and organizational stakeholders to address each of the elements in the risk management cycle:

- Frame;
- Assess;
- Respond; and
- Monitor.

These elements are defined in such a way that all Electricity Sector organizations can follow the guidance, but the specific method they use is not dictated. The process is designed to be flexible to each organization's size or sophistication.

Electricity Sector organizations have significant flexibility in determining the inputs, how the risk management activities are performed (e.g., sequence, degree of rigor, formality, and thoroughness of application), and how the results or outputs of each activity are captured and shared across the organization and between organizations. Ultimately, the objective of applying the RMP is to develop a better understanding of cybersecurity risk in the context of the broader actions and decisions of organizations and, in particular, with respect to an organization's operations, assets, individuals, and relationships with other organizations.

Electricity Sector organizations have a variety of risk management methodologies, models, and systems that they may already use for addressing areas such as safety and financial risk. The RMP discussed in this document is not meant to supersede these but to add aspects of cybersecurity. If an organization already has an established RMP, then much of the information contained in this document may already be known and may be used in conjunction with that process. This RMP is not meant to replace an organization's existing process if it exists but to add to it, making it stronger and more secure.

The RMP at Tier 1 produces a cybersecurity risk management strategy that includes a risk assessment methodology, a risk monitoring strategy, and a cybersecurity governance program. The cybersecurity risk management strategy will enable business unit managers, mission and business process owners, and IT

and ICS managers to allocate resources in a prioritized manner and provide feedback to senior management on the effectiveness of the risk management program. The development and institution of a governance program will provide focus and structure to the executive leadership responsible for providing oversight and systematic review of the RMP.

3.1 RISK FRAMING AT TIER 1

Risk framing establishes the context and provides a common perspective on how an Electricity Sector organization manages risk. This will vary across Electricity Sector organizations on the basis of their type and size. For instance, a small rural cooperative may have a fairly well-defined but limited scope of business that includes a few hundred distribution end points, a couple of generation assets, small field operations, and administration functions. This is dramatically different from a larger investor-owned utility that includes thousands of distribution customers, interstate transmission assets, investments in large-scale generation facilities, and wholesale marketing activities. Risk framing for both of these organizations will reflect the "realities" of each organization, from the unique functions they perform to the specific assets they manage.

NOTE.—For each element (frame, assess, respond, and monitor) at all tiers, said element is defined by its inputs, its activities performed against the inputs and the outputs from the activities. At the end of Chapter 3, Chapter 4, and Chapter 5, there is a summary sheet detailing the tier's inputs, activities, and outputs for each element.

Once the environment is adequately framed, an organization's senior leadership will be able to appropriately assess, respond to, and monitor risk. The risk framing element makes explicit the specific risk assumptions, risk constraints, risk tolerances, and priorities and trade-offs used within organizations for making investment and operational decisions.

3.1.1 Inputs

Source inputs to the Tier 1 risk framing element may include:

- Mission and vision statements;
- Legislation (international, Federal, regional, State, local, and tribal);
- Organizational policies;
- Regulatory requirements (e.g., North American Electric Reliability Corporation [NERC] registration and functional model);
- Contractual relationships (e.g., third- party agreements, service-level agreements, memoranda of understanding, and memoranda of agreement);
- Financial limitations;
- Trust relationships, both internal and external to the organization;[21]
- Organizational culture, both internal and external to the organization;
- Governance structures;

Risk framing at Tier 1 should be limited to strategic information that defines cybersecurity risk throughout the organization. Some specific examples of Electricity Sector organizations could include:

- A large interstate transmission business that is covered by NERC and must comply with NERC CIP Standards;
- A small rural cooperative that has contracts with its neighboring distribution utilities to share substation and field operations management;
- A generation facility that contracts with wholesale marketing organizations for demand-response data feeds; or
- A regional municipal utility that employs wireless and broadband technologies for meter reading.

[21] Additional information regarding trust relationships and trust models can be found in Appendix G, Trust Models.

- Processes that indicate the extent of or limits on decision making authority;
- Outputs from the Tier 1 risk monitoring elements;[22] and
- Feedback from the Tier 2 risk management cycle.

3.1.2 Activities

3.1.2.1 Risk Assumption

Risk assumption activities identify how risk is assessed, responded to, and monitored. As part of the framing element, Electricity Sector organizations identify, describe and provide examples of threat sources, vulnerabilities, impacts, and likelihood determinations for risk assumption activities. This will promote a common terminology and frame of reference throughout the organization for comparing and addressing risks across the disparate mission and business areas. Additionally, at Tier 1 an organization may leverage threat scenarios, identified by industry associations and task forces, to enhance its approach to a complete risk analysis.

Threat Sources

Threat sources can introduce undesirable events with adverse impacts on organizational operations, assets, individuals, and other organizations in the Electricity Sector. Threat sources may include:

- People (malicious violation of policies by current/former employees and third-party personnel);
- Processes (missing or deficient procedures);
- Technology (component failure through design, implementation, and/or maintenance);
- External disasters (natural or man-made); and
- Systemic, recurring cybersecurity incidents.

For all threats determined through the analysis of threat sources, Electricity Sector organizations develop a concise description of the:

- Types of tactics, techniques, and procedures employed by adversaries;[23]
- Threat sources addressed by the safeguards and countermeasures;
- Threat sources not being addressed by safeguards and countermeasures;
- Assumptions about threat source targeting, intentions, and capabilities;
- Level of detail with which the events are described, by identifying a set of representative threat events;
- Conditions for when to consider threat events in risk assessments; and
- Credible and useful sources of threat information (e.g., Electricity Sector Information Sharing and Analysis Center [ES-ISAC], United States Computer Emergency Readiness Team [US-CERT], and NERC).

By identifying and establishing threat sources at Tier 1, Electricity Sector organizations provide a basis for aggregating and consolidating the results of risk assessments at Tier 2 into an overall assessment of risk throughout the organization.

[22] These outputs will not exist if this is the first time an organization is implementing the risk management lifecycle at Tier 1. These outputs will only exist once an organization has completed the risk management lifecycle at Tier 1 and Tier 2.

[23] Adversaries can be characterized in terms of threat levels (based on capabilities, intentions, and targeting) or with additional detail.

Vulnerabilities

Vulnerabilities are vectors that a threat source may exploit to cause adverse impacts to IT and ICS in Electricity Sector organizations. At Tier 1, vulnerabilities can be associated with deficiencies or weaknesses in organizational governance structures or processes. They can also be associated with the susceptibility of organizations to adverse impacts from external sources (e.g., technology owned or managed by third parties). The Electricity Sector organization at Tier 1 may:

- Provide guidance regarding how to consider dependencies on external organizations as vulnerabilities;
- Identify the degree of specificity with which vulnerabilities are described (e.g., identification of weak or deficient cybersecurity controls);
- Provide examples corresponding to threats;
- Determine how vulnerability information is shared across organizations, using governance structures and processes;
- Identify sources of vulnerability information found to be credible and useful; and
- Make explicit any assumptions about the degree of organizational, IT, and ICS vulnerability to specific threat sources (by name or type).

Impact

Electricity Sector organizations provide guidance on how to assess impacts to operations (i.e., mission disruption, financial loss, image, and reputation), assets, individuals, and other organizations from a cybersecurity event. Organizations can experience the impacts of cybersecurity events along with their consequences at Tier 1 (e.g., failing to comply with legal or regulatory requirements, damaging reputation or relationships, or undermining long-term viability as it relates to the consequences of cybersecurity breaches). At Tier 1, an organization's senior executive leadership determines which impact types and their consequences related to cybersecurity are to be considered at Tier 2.

A cybersecurity event can have multiple consequences and different types of impact, at different levels, and in different time frames. For instance, a cybersecurity compromise of communications equipment used for transmission line management could lead to cascading failures across portions of the grid. The resulting downstream outages could result in loss of customers, legal and regulatory actions, or impact on reputation brand and corporate value.

Likelihood

Electricity Sector organizations can employ a variety of approaches for determining the likelihood of cybersecurity threat events. One organization may prefer quantitative[24] risk assessments, while another organization may prefer qualitative[25] risk assessments, particularly when the risk assessment involves a high degree of uncertainty. Likelihood determinations can be based on either threat assumptions or actual threat data (e.g., historical data on cyber attacks or specific information on adversary capabilities, intentions, and targeting).

When specific and credible threat data is available (e.g., types of cyber attacks, cyber attack trends, and frequencies of attacks), Electricity Sector organizations use the empirical data and statistical analyses to determine more specific probabilities of threat events occurring. Organizations then select a method

[24] Quantitative risk is the use of measurable, objective data to determine asset value, probability of loss, and associated risks.

[25] Qualitative risk is the measure of risk or asset value based on rank or separation into categories such as low, moderate, high on a scale from 1 to 10.

consistent with its organizational culture and risk tolerance. Organizations can also make explicit assumptions concerning the likelihood that a threat event will result in adverse effects, as follows:

- Worst case (i.e., attack will be successful unless strong, objective reasons to presume otherwise);
- Best case (i.e., attack will not be successful unless specific, credible information to the contrary); or
- Something in between best and worst cases (i.e., the most probable case).

3.1.2.2 Risk Constraint

Electricity Sector organizations identify constraints based on risk framing activities. Some organizations may be compelled to meet strict regulatory requirements (e.g., NERC Critical Infrastructure Protection [CIP] Standards) that limit risk response options, while other organizations may be constrained by resource availability, contractual obligation, culture, or timing. Additionally, many IT and ICS assets in Electricity Sector organizations must serve a long, useful life without disruption. A lack of flexibility in changing legacy systems may drive the need to integrate more stringent cybersecurity controls into the systems upon initial deployment. Constraints on the RMP in the Electricity Sector may include:

- Direct financial limitations (e.g., limiting the total resources available for investments in risk assessments or in safeguards or countermeasures);
- Indirect financial limitations (e.g., eliminating activities that, while involving relatively small investments in risk response, entail curtailing or discarding investments in legacy IT and ICS);
- Legal, regulatory, and/or contractual requirements;
- Organizational policies (e.g., restrictions on outsourcing and/or on requirements for information to be gathered as part of risk monitoring);
- Organizational culture, which can impose indirect constraints on governance changes (e.g., precluding a shift from decentralized to hybrid governance structures);
- Cybersecurity controls considered by an organization to be implemented organization wide; and
- Cultural constraints that limit the visibility into and between IT and ICS.

3.1.2.3 Risk Tolerance

In the Electricity Sector, organizations identify and communicate the level of risk tolerance acceptable to meeting their mission and business objectives. At Tier 1, organizations will define their risk tolerance on the basis of the activities in the risk framing element in conjunction with organizational mission and business functions. There is no correct level of organizational risk tolerance. Rather, the degree of risk tolerance is (i) generally indicative of organizational culture, (ii) potentially different for different types of losses/compromises, and (iii) subject to the risk tolerance of senior executives. The ramifications of risk decisions that are based on risk tolerance are significant, resulting in less risk-tolerant organizations potentially failing to achieve needed mission and business capabilities in order to avoid what appears to be unacceptable risk, while more risk-tolerant organizations may focus on near-term mission and business efficiencies at the expense of setting themselves up for future failure.

It is important that organizations exercise due diligence in determining risk tolerance—recognizing how fundamental this decision is to the effectiveness of the risk management program. There are a variety of techniques for identifying cybersecurity risk tolerance. This variety is likely to be different, based on the uniqueness of the Electricity Sector organization and the perceived risk scenarios. Additionally, organizations may define risk tolerance for other types of organizational and operational risks (e.g., financial, safety, compliance, or reputation) that will have an impact on cybersecurity risk.

3.1.2.4 Priorities and Trade-Offs

At Tier 1, organizations make trade-offs and establish priorities for responding to risks. Electricity Sector organizations tend to have multiple priorities that can conflict. These conflicts may introduce other risks

as a result. Approaches employed by Electricity Sector organizations for managing risks reflect organizational culture, risk tolerance, risk-related assumptions and constraints. These approaches are integrated into strategic plans, policies, and roadmaps for organizations that may indicate preferences for different forms of risk response.

3.1.3 Outputs

Outputs from the Tier 1 risk framing element produce a set of organizational policies, governance structure, and guidance for the following:

- **Scope of the organizational RMP (e.g., organizations covered, mission and business functions** affected, how risk management activities are applied at Tier 1);
- Cybersecurity risk assessment guidance, including the description of threat, sources of threat information, example threat events (in particular, adversary tactics, techniques, and procedures), when to consider and how to evaluate threats, sources of vulnerability information, risk assessment methodologies to be used, and risk assumptions;
- Cybersecurity risk response guidance, including risk tolerances, risk response concepts to be employed, opportunity costs, trade-offs, consequences of responses, hierarchy of authorities, and priorities;
- Cybersecurity risk monitoring guidance, including analysis of monitored risk factors to determine changes in risk, monitoring frequency, methods, and reporting;
- Cybersecurity risk constraints on executing risk management activities; and
- Organizational priorities and trade-offs relating to cybersecurity risk.

The outputs of the risk framing element serve as inputs to the risk assessment element of the RMP.

3.2 Risk Assessment at Tier 1

At the Tier 1 organization level, the risk assessment element identifies the mission, functions, and individuals in order to:

- Prioritize investment strategies for business units or functions based on trade-offs;
- Establish a standard risk assessment methodology or provide guidance for consistent implementation of risk assessment across the enterprise; and
- Set tolerances for risk response.

Risk assessments conducted at Tier 1 are used to refine and enhance threat, vulnerability, likelihood, and impact information in assessments conducted in Tier 2. Organization-wide risk assessments in the Electricity Sector provide some initial prioritization of risks for the organization's leadership to consider when moving to the risk response element.

A common problem with risk assessment is treating it as a singular activity rather than as an ongoing process. Keeping risk assessments up to date provides many potential benefits such as timely and relevant information that enable senior executive leadership to perform continuous risk management.

A Tier 1 organization could be seen as the "investment holding company" of a number of related businesses involved in the generation, transmission, and distribution of electricity. The business goal is for maximum communication, consistency, and enhanced value. To achieve this, an organization sets standards for risk assessment by reviewing assessments already performed in the organization's operations environment and sets the standards for all of the related businesses to follow.

Organizations may determine that conducting comprehensive risk assessments does not provide sufficient value or is too overwhelming. In such situations, Electricity Sector organizations may consider conducting incremental and/or differential risk assessments. An incremental risk assessment considers only new information (e.g., the effects of using a new piece of technology on mission and business risk), whereas a differential risk assessment considers how changes affect the overall risk determination. Incremental or differential risk assessments are useful if organizations require a more targeted review of risk, seek an expanded understanding of risk, or desire an expanded understanding of the risk in relation to its mission and business functions.

3.2.1 Inputs

Inputs to the Tier 1 risk assessment element may include:

- Organizationally consistent risk assessment methodologies;[26]
- The breadth and depth of analysis employed during risk assessments;
- The level of granularity required for assessing threats and vulnerabilities;
- Whether and/or how to assess external service providers;
- Whether and/or how to aggregate risk assessment results from different organizational entities or mission and business functions organization wide; and
- Outputs from the risk framing element in Tier 1.

Organizational expectations regarding Tier 1 risk assessment methodologies, techniques, and/or procedures are shaped heavily by governance structures, risk tolerance, risk constraints, priorities, trade-offs, culture, familiarity, and trust. Prior to conducting risk assessments, Electricity Sector organizations determine the appropriate depth and breadth for the assessments.

Risk assessments can be conducted even when some of the inputs from the risk framing step have not been received or preconditions established. However, in those situations, the quality of the risk assessment results will be affected and may be incomplete.

3.2.2 Activities

3.2.2.1 Threat and Vulnerability Identification

A Tier 1 risk assessment focuses on the identification of threats to and vulnerabilities of an Electricity Sector organization. Threat analysis requires an examination of threat sources, data, and events to estimate capabilities, intentions, and targeting information from many sources. Threat and threat source information generated at Tier 1 can be used to inform or refine the risk-related activities in Tier 2 and Tier 3. Vulnerabilities related to organizational governance and external dependencies are most effectively identified at Tier 1. For instance, a moderate-sized utility will want to review threats to the IT and ICS employed by the utility. It might start with a catalog and classification exercise to identify and prioritize the most critical to least critical technology, based on mission and data importance. The list then helps inform which threats and vulnerabilities are applicable to which technology.

In many Electricity Sector organizations, risk scenarios are developed where subsequent decision tree-styled risk determination is more easily implemented. The Electricity Sector and supporting government organizations develop threat scenarios that are helpful in identifying and analyzing threats and vulnerabilities. As previously stated, these risk scenarios are constantly changing and will require routine review of threat assumptions that are used in organizational risk determination.

[26] Examples of risk assessment methodologies include: NIST SP800-30, OCTAVE/SQUARE, RAM-E, ISO-27005, ISO-31000, Probabilistic risk assessment (PRA), Failure Mode Effects and Analysis (FMEA).

3.2.2.2 Risk Determination

At Tier 1, organizations in the Electricity Sector determine the risk to their operations, assets, individuals, and other organizations if identified threats were to exploit identified vulnerabilities. Organizations determine risk by considering the likelihood that threats could exploit vulnerabilities and the resulting adverse impacts if such exploitations occur. An organization uses threat and vulnerability information, together with likelihood and impact information to determine risk, either qualitatively or quantitatively. To determine the likelihood of threats exploiting vulnerabilities, Electricity Sector organizations can employ a variety of approaches, such as:

- Threat source assumptions (e.g., historical data on cyber attacks, earthquakes, etc.);
- Threat modeling, such as comparison or perspective methods;[27]
- Actual threat information (e.g., specific information on threat source capabilities, intentions, and targeting);
- Empirical data and statistical analyses used to determine more specific probabilities of threats occurring; and
- Vulnerabilities identified at the individual weakness or deficiency level or at the root-cause level.

Risk Determination and Uncertainty

In instances involving potential high impact, any likelihood that a threat could exploit a known vulnerability would require a high-priority response to reduce the potential for unacceptable damage. Thus, risk determinations at Tier 1 require analysis of threat, vulnerability, likelihood, and impact-related information. Organizations will need to understand:

- Mission and business threats and vulnerabilities, where safeguards and/or countermeasures do not exist;
- How risk assessment inputs directly affect the type of outputs or risk determinations;
- That the reliability and accuracy of risk determinations are dependent on the currency, accuracy, completeness, and integrity of information collected to support the risk assessment process;
- The components of risk assessment results that affect reliability and accuracy of risk determinations; and
- The anticipated time frames associated with particular risks.

The Tier 1 guidance for determining risk uncertainty indicates how combinations of likelihood and impact are combined to determine the risk level or risk score rating. During the risk framing element, organizations may have provided guidance on how to analyze risk and how to determine risk when a high degree of uncertainty exists. Uncertainty is particularly a concern when the risk assessment considers advanced persistent threats (APTs) for which analysis of interacting vulnerabilities may be needed, the common body of knowledge is sparse, and past behavior may not be predictive.

Even with the establishment of explicit criteria, risk assessments are influenced by organizational culture and the personal experiences and accumulated knowledge of the individuals conducting the assessments. As a result, assessors of risk can reach different conclusions from the same information. It is the responsibility of the organization's senior risk executive function to harmonize a consistent risk determination across the organization, while driving the Electricity Sector organization to adopt justified risk response programs. The defined and applied processes of an organization provide the means to identify inconsistent practices and include processes to identify and resolve such inconsistencies.

[27] See *Performing Security Analyses of Information Systems*, pages 119-125, by Charles L. Smith, Sr., for additional information.

3.2.3 Outputs

The output of the risk assessment element is a determination of risk to an organization's operations, individuals, and other organizations. Risk determination is the primary input for selecting appropriate risk responses in subsequent tiers and elements. The information collected in assessment activities may be documented so that it can be re-assessed on a regular basis.

3.3 RISK RESPONSE AT TIER 1

Risk response at Tier 1 evaluates, decides upon, and implements appropriate courses of action to accept, avoid, mitigate, share, or transfer risk to an organization's operations, assets, individuals, and other organizations. Identifying and analyzing alternative courses of action at Tier 1 will impact risk determination at subsequent tiers. Decisions to employ risk response measures throughout an organization are typically made at Tier 1, although the decisions are informed by risk-related information from the lower tiers.

A municipality that is responsible for electricity delivery recognizes the risk of earthquake or natural disaster to the generation and transmission functions conducted by contracted organizations. The municipality finds its options to mitigate this risk to be highly limited and costly and therefore decides to take limited measures to address this supply-chain risk. This would be an example of partial acceptance of risk by an Electricity Sector organization at Tier 1.

Conversely, the same municipality may have recently replaced all consumer meters with new digital meters. The risk is considered relatively low after the risk assessment is performed; however, consumer fears about privacy leads the municipality to invest in expensive data protection measures as a means to promote trust and alleviate any perceived risk. In this case, the acceptance of risk at Tier 1 will affect the operations and risk constraints at Tier 2 and Tier 3.

3.3.1 Inputs

Inputs to the Tier 1 risk response element may include:

- Threat sources and threat events;
- Vulnerabilities that are subject to exploitation;
- Estimates of potential impact and consequences if threats exploit vulnerabilities;
- Estimates of likelihood that threats exploit vulnerabilities;
- Determinations of risk to an organization's operations, individuals, and other organizations;
- Risk response guidance from the organization's risk management strategy;
- Directions and guidance on appropriate responses to risk; and
- Outputs from the Tier 1 risk assessment element.

3.3.2 Activities

3.3.2.1 Risk Response Identification

At Tier 1, identification of risk response in an Electricity Sector organization will require identifying alternative courses of action to respond to risk determined during the risk assessment. A course of action is a time-phased or situation-dependent combination of risk response measures. Organizations can respond to risk in a variety of ways.[28]

An example of a risk response is how many electric utility operations rely on new IT for telemetry of line and device information. The risk of failure of these devices could affect both the cybersecurity and the safety of assets. Therefore, backup communications channels are needed

These include:

[28] Additional information regarding how an organization responds to risk can be found in Appendix H, Risk Response Strategies.

- Risk acceptance;
- Risk avoidance;
- Risk mitigation;
- Risk sharing;
- Risk transference; or
- Combinations of the above.

Risk Acceptance

Risk acceptance is the appropriate risk response when the identified risk is within the risk tolerance of an Electricity Sector organization. In some instances, organizations may accept risk deemed to be low or moderate, depending on particular situations or conditions. Conversely, organizations designated by regulatory authorities will have a lower risk tolerance and may be restricted from accepting risk for specific business functions.[29] Electricity Sector organizations may make determinations regarding the general level of acceptable risk and the types of acceptable risk, while considering organizational priorities and trade-offs between:

- Near-term mission and business needs and the potential for long-term mission and business impacts;
- Organizational interests and the potential impacts on individuals and other organizations; and
- Regulatory requirements.

Risk Avoidance

Risk avoidance involves taking specific actions to eliminate the activities or technologies that are the basis for the risk. Organizations revise or reposition activities or technologies to its mission and business processes to avoid the potential for unacceptable risk.

Risk Mitigation

Risk mitigation, also known as risk reduction, is the appropriate risk response for that portion of risk that cannot be accepted, avoided, shared, or transferred. The alternatives to mitigate risk depend on:

- The scope of risk response decisions assigned or delegated to the senior risk official, as defined by the organization's governance structure; and
- The organization's risk management strategy and associated risk response strategies.

The means used by organizations in the Electricity Sector to mitigate risk can involve a combination of risk response measures across all tiers.

Risk Sharing or Risk Transference

Risk sharing or risk transference is the appropriate risk response when an Electricity Sector organization desires and has the resources to shift risk liability and responsibility to other organizations. Risk transference shifts the entire risk responsibility or liability from one organization to another organization. Risk sharing shifts a portion of risk responsibility or liability to another organization. It is important to note that risk transference reduces neither the likelihood of harmful events occurring nor the impact to an organization's operations, assets, individuals, or other organizations. Risk sharing does not always reduce the impact of regulatory compliance enforcement or financial liability, unless the agreement(s) between the risk sharing organizations acknowledge transfer of both responsibility and liability. Risk sharing often

[29] For example, per NERC Reliability Standards, organizations in the Electricity Sector with components deemed part of the critical infrastructure may not accept any risk for said components.

occurs when organizations determine that addressing risk requires expertise or resources that are better provided by other organizations.

3.3.2.2 Evaluation of Alternatives

In the risk response element, Electricity Sector organizations evaluate alternative courses of action for responding to risk. The evaluation of alternative courses of action can include:

- How effectiveness is measured and monitored in achieving the desired risk response; and
- What is the feasibility of implementation throughout the expected period of time, during which, the course of action is followed.

During the evaluation of alternative courses of action, trade-offs can be made explicit between near-term gains in mission and business effectiveness or efficiency and long-term risk of mission and business harm. Trade-offs due to the compromise of IT and ICS are providing this near-term benefit. A risk prioritization evaluation is conducted for each course of action to provide the information necessary for:

- Selecting between the courses of action; and
- Evaluating the courses of action in terms of response effectiveness, costs, mission and business impact, and any other factors deemed relevant to an Electricity Sector organization.

Part of a risk prioritization evaluation considers the issue of competing resources. From an Electricity Sector organization's perspective, this means organizations consider whether the cost for implementing a given course of action has the potential to adversely impact other missions or business functions, and if so, to what extent. This is necessary because organizations have finite resources to employ and many competing mission and business functions. Therefore, organizations assess the overall value of alternative courses of action, with regard to the mission and business functions and the potential risk to all parts of the organization. Organizations may determine that irrespective of the mission and business function and the validity of the risk to the mission and business function, that there are more important mission and business functions that face more significant risks and hence have a better claim on the limited resources.

3.3.2.3 Risk Response Decision and Implementation

At Tier 1, an Electricity Sector organization decides on the appropriate course of action for responding to risk. These decisions on appropriate courses of action include some form of prioritization. Some risks may be of greater concern than other risks. In such a case, more resources may be directed at addressing higher priority risks than lower priority risks. This does not mean that the lower priority risks would not be addressed. Rather, it could mean that fewer resources might be directed at the lower priority risks or that they would be addressed at a later time. A key part of the risk decision process is the recognition that regardless of the decision, there still remains a degree of residual risk[30] that must be addressed. Organizations determine acceptable degrees of residual risk on the basis of their risk tolerance and the specific risk tolerances of particular decision makers. Impacting the decision process are some of the more intangible risk-related concepts (e.g., risk tolerance, trust, and culture). The specific beliefs and approaches that organizations embrace with respect to these risk-related concepts affect the course of action selected by decision makers. Once a course of action is selected, it is incorporated into the risk management strategy that is communicated throughout the organization and implemented.

3.3.3 Outputs

The output from the Tier 1 risk response element is a risk response plan that guides the implementation of the selected courses of action with consideration for:

[30] Residual risk is the risk that remains after a risk response has been applied.

- Individuals or organizational elements responsible for the selected risk response measures and specifications of effectiveness criteria (i.e., articulation of key indicators and thresholds);
- Dependencies of each selected risk response measure on other risk response measures;
- Dependencies of selected risk response measures on other factors (e.g., the implementation of other planned IT measures);
- Timelines for implementation of risk response measures;
- Plans for monitoring the effectiveness of risk response measures;
- Triggers for risk monitoring;
- Results of response activities added to the risk management strategy; and
- Interim risk response measures selected for implementation, if appropriate.

3.4 RISK MONITORING AT TIER 1

The risk monitoring element provides organizations in the Electricity Sector with the means to determine the ongoing effectiveness of risk response measures and to identify risk-impacting changes to the organization's IT and ICS and their environments of operation. Analyzing the risk monitoring results provides an organization the capability to maintain awareness of the risk being incurred, highlight the need to revisit the RMP, and initiate process improvement activities, as needed.[31] Organizations employ risk monitoring tools, techniques, and procedures to increase risk awareness, helping senior leadership develop a better understanding of the ongoing risk to organizational operations, individuals, and other organizations. Risk monitoring is fundamental to strategic cybersecurity management, as it improves awareness of threats and provides the foundation to correlate controls in a way that moves beyond the defense of a single technology.

The senior leadership in an Electricity Sector organization determines and verifies the metrics for evaluating mission and business processes and procedures to ensure that the activities involving cybersecurity risk are being performed in an effective manner. Risk monitoring provides Electricity Sector organizations with the means to:

- Verify risk response implementation;[32]
- Determine the effectiveness of risk response measures; and
- Identify risk-impacting changes to IT and ICS and their environment of operation.

At Tier 1, strategic criteria for continuous monitoring of cybersecurity are defined by the organization's risk tolerance, how the organization plans to monitor risk given the inevitable changes to organizational IT and ICS and their environments of operation, and the degree and type of oversight the organization plans to use to ensure that the risk management strategy is being effectively carried out. Metrics defined and monitored by officials at this level are designed to deliver information necessary to make risk management decisions in support of the organization's governance structure.

Review and analysis of monitoring results gives organizations in the Electricity Sector the capability to maintain an awareness of the risk being incurred, highlight the need to revisit other steps in the RMP, and initiate process improvement activities as needed. Each organization may employ risk monitoring tools, techniques, and procedures to increase risk awareness. This awareness provides senior executive

[31] Draft NIST SP 800-137, *Information Security Continuous Monitoring for Federal Information Systems and Organizations*, provides guidance on monitoring organizational information systems and environments of operation.

[32] Implementation verification ensures that organizations have implemented required risk response measures and that cybersecurity requirements derived from, and traceable to, organizational mission and business functions, directives, regulations, policies, and standards and guidelines are satisfied.

leadership a better understanding of the ongoing risk to the organization against its ability to perform its mission.

At Tier 1, monitoring activities might include ongoing threat assessments and how changes in the threat environment may affect Tier 2 and Tier 3 activities. This includes the organization's enterprise and cybersecurity architectures, as well as its IT and ICS. Organization-level monitoring is another key part of the governance structure and establishes accountability for deploying and maintaining controls selected for the risk management strategy. The metrics used to monitor program effectiveness and the frequencies of reporting are determined by the level of risk being managed in each business process within the organization.

3.4.1 Inputs

Inputs to the Tier 1 risk monitoring element include strategies for and implementations of Tier 1 courses of action for risk responses. Inputs to Tier 1 risk monitoring may also include:

- Information regarding industry best practices, tools, and frequency;
- Risk management strategy, including risk assessment methodology;
- Cybersecurity governance structure;
- Performance information; and
- Comprehensive lists of identified risks.

3.4.2 Activities

3.4.2.1 Risk Monitoring Strategy

In the Electricity Sector, organizations develop a risk monitoring strategy that includes the purpose, type, and frequency of monitoring activities. Organizations implement risk monitoring programs to:

- Verify that required risk response measures are implemented and that cybersecurity requirements are derived from and traceable to the organization's mission and business functions;
- Determine the ongoing effectiveness of risk response measures after implementation;
- Identify changes to the organization's IT and ICS and the environments in which they operate;
- Monitor changes in the feasibility of the ongoing implementation of risk response measures;
- Determine how the purpose of risk monitoring programs directly impact the means used by the organization to conduct monitoring activities and where monitoring occurs;
- Determine the type of monitoring to be employed, including approaches that rely on automation, procedural, or manual activities; and
- Determine how often monitoring activities are conducted, balancing value gained from frequent monitoring with potential for operational disruptions.

Monitoring and performance of risk response measures can best be ensured through:

- Configuration management and change control;
- Reports on risk response performance;
- Assessment of implemented controls; and
- Analysis of cybersecurity impacts.

Monitoring Implementation

Implementation monitoring is employed to ensure that business process owners are implementing needed risk response measures. Failure to implement the risk response measures selected by Electricity Sector

organizations can result in the organization continuing to be subject to identified risks and can introduce the potential for failing to comply with Federal mandates (e.g., legislation, regulations, standards) or organizational mandates (e.g., policies, procedures, mission and business requirements). Typically, the organization's senior risk executive will obtain feedback and reports as part of a governance structure from business process owners or function owners to determine whether implementation of the risk response strategy has been achieved.

Monitoring Effectiveness

Effectiveness monitoring is employed by organizations to determine if implemented risk response strategies have been successful in mitigating identified risks to the risk tolerance level. Although determining effectiveness is significantly more complex than implementation monitoring, failure to achieve desired levels of effectiveness are indications that risk response measures have been implemented incorrectly or are not operating as intended. Additionally, risk response measures implemented correctly and operating as intended do not guarantee an effective reduction of risk. This is primarily due to:

- The complexity of operating environments that may generate unintended consequences;
- Subsequent changes in levels of risk or associated risk;
- Inappropriate or incomplete criteria established as an output of the risk response element; and
- Changes in IT and ICS and their environment of operation after implementation of risk response measures.

Failure to achieve effective risk response may require an Electricity Sector organization to completely reassess its risk and to either select a new risk response course of action or direct that new controls be deployed to guide implementation.

Monitoring Changes

In addition to implementation monitoring and effectiveness monitoring, Electricity Sector organizations monitor changes to IT and ICS and the environments in which they operate. Monitoring changes is not linked directly to previous risk response measures, but it is nonetheless important to detect changes that may affect the risk to an organization's operation, individuals, and other organizations. Generally, such monitoring detects changes in conditions that may undermine risk assumptions, articulated in the risk framing element.

Automated Versus Manual Monitoring

In Tier 1, monitoring typically involves reporting, analysis, and policy or strategy change recommendations. The governance structure within an Electricity Sector organization assigns key metrics to track and evaluate on a routine basis. Each organization may employ a semi-automated risk management application or dashboard to track and monitor key metrics. While the risks and controls may be technical, Tier 1 focuses on organization-level responsibilities that meet the expectations, mission, and other defined key business metrics of the organization's senior executives and shareholders.

Frequency of Monitoring

The frequency of risk monitoring (whether automated or manual) is driven by the mission and business functions of the organization as well as the cost and ability to use the monitoring results to facilitate greater situational awareness. An increased level of awareness in the cybersecurity state of IT and ICS helps Electricity Sector organizations develop a better understanding and management of risk. Risk monitoring frequency is also driven by other factors, such as:

- The anticipated frequency of changes in IT and ICS and their operating environments;

- The potential impact of risk if not properly addressed through appropriate response measures; and
- The degree to which the threat space is changing.

The frequency of monitoring can also be affected by the type of monitoring conducted (i.e., automated versus manual approaches). Depending on the frequency of monitoring required, continuous monitoring[33] is most efficient and cost-effective when automated monitoring is employed. Continuous monitoring can provide significant benefits, especially in situations in which monitoring limits the opportunities of adversaries to gain access within an organization.

3.4.2.2 Risk Monitoring

In the risk monitoring element in Tier 1, organizations monitor IT and ICS and their environment on an organization-defined basis to verify compliance, determine the effectiveness of risk response measures, and identify any changes. Once Electricity Sector organizations complete the development of their monitoring strategies and risk response methods, the strategies are implemented throughout the organization. Because the size and complexity of monitoring programs can be large, monitoring may be phased in or performed at different frequencies, based on the risk level or complexity of the risk response mechanism. The particular aspects of monitoring that are performed are dictated largely by the assumptions, constraints, risk tolerance, and priorities and trade-offs established during the risk framing element.

> A medium-sized Electricity Sector utility determines that it has a good handle on its risk assessment and mitigation strategy. It wants to start a continuous monitoring program with automation tools to progress toward a systematic and higher level of cybersecurity for their organization. They begin with an inventory of all cybersecurity monitoring functions already in place by:
>
> - Taking existing tools and collecting samples of the data and reporting it;
> - Considering tools to help automate identification and status of all IT and ICS assets;
> - Assessing and categorizing technology by asset type, system boundary, and risk level or importance; and
> - Considering cybersecurity and compliance tool features that best match the needs for staff experience.
>
> Organizations then focus on the regulatory reporting and requirements they have to meet. In the above example, the organization must already report specific compliance adherence with NERC CIP Standards. This reporting offers a chance to re-evaluate the tools and methods employed to achieve compliance with the CIP Standards.

Coordination of monitoring activities facilitates the sharing of risk-related information to provide early warning or trending for allocating risk response measures in a timely and efficient manner. If monitoring is not coordinated, then its benefit may be reduced and could, therefore, undermine the overall effort to identify and address risk. As feasible, Electricity Sector organizations implement various monitoring activities in a manner that maximizes the overall goal of monitoring, looking beyond limited goals of a particular monitoring activity. Risk monitoring results are used when performing incremental risk assessments to maintain awareness of the risk being incurred, to highlight changes in risk, and to indicate the need to revisit the RMP, as appropriate.

Finally, Electricity Sector organizations decide:

- Which risk response measures will be automated for continuous monitoring;

[33] Continuous monitoring is the process and technology used to detect risk issues associated with an Electricity Sector organization's operational environment.

- Which tools to provide for reporting and for alerting officials when a control is not working;
- What alerting is necessary in each tier of the organization;
- Frequency of risk monitoring reports; and
- Any additional information that is associated with the risk analysis of any measure.

The result is appropriate alerting and reporting for all tiers to maintain better monitoring and assurance of risk management.

3.4.3 Outputs

The output from the Tier 1 risk monitoring element is the information generated by:

- Verifying that required risk response measures are implemented and cybersecurity requirements are derived from and traceable to an organization's mission and business functions;
- Determining the ongoing effectiveness of risk response measures;
- Identifying changes to IT and ICS and its environments of operation; and
- Developing a risk monitoring strategy and incorporating it into the risk management strategy.

As part of the RMP, outputs from the risk monitoring element can be useful feedback to the risk framing element within each tier.

3.5 SUMMARY AT TIER 1

The risk management cycle for Tier 1 has been described in this chapter as part of the risk executive function which serves as the common risk management resource for senior leadership without prescribing a specific governance model. This could exist as a collection of executive managers, board of directors, or a committee of a cooperative organization. However, the result remains that the Tier 1 function provides direction that management (at Tier 2 and Tier 3) use to guide the operations of the organization. Providing cybersecurity governance in most organizations includes a process to define expectations, provide policy and guidance, verify performance, and set constraints for organizational behavior. The RMP model assumes that governance functions for organizations already exist at Tier 1 and can be enhanced to address cybersecurity risk issues.

The cybersecurity risk management strategy is the high-level document that changes over time to direct the organization on how to analyze and prioritize cybersecurity risk, the risk tolerance of the organization, the priorities of the organization, and the goals of addressing cybersecurity risks. This information includes how to assess risk trade-offs and how to better understand cybersecurity risk factors to the organization.

The following table provides an overview of the inputs, activities, and outputs from the risk framing, assessment, response, and monitoring elements in Tier 1 of the RMP. This table focuses on the typical inputs and outputs, but the list is not exhaustive. Organizations will use the activities to develop artifacts that provide for the healthy examination of cybersecurity risk to their organization and develop a process to refine guidance and policy.

	INPUTS	ACTIVITIES	OUTPUTS

RISK FRAMING	• Mission and vision statement
	• Legislation
	• Organizational policies
	• Regulatory requirements
	• Contractual relationships
	• Financial limitations
	• Trust relationships
	• Organizational culture
	• Governance structures
	• Decision-making authority
	• Ouput from Tier 1 risk monitoring element
	• Feedback from Tier 2 risk management cycle
		• Define risk assumption
		  ▫ Threat sources
		  ▫ Vulnerabilities
		  ▫ Impact
		  ▫ Likelihood
		• Identify risk constraint
		• Determine risk tolerance
		• Identify priorities and trade-offs
		• Develop risk management strategy
			• Risk Management Strategy

RISK ASSESSMENT	• Risk assessment methodology • Risk assessment breadth and depth • How to assess external service providers • How to aggregate risk • Outputs from Tier 1 risk framing element	• Identify threat and vulnerability identification • Determine risk	• Determination of risk for the organization's operations, individuals, and other organizations

RISK RESPONSE	• Threat sources and threat events
	• Vulnerabilities
	• Estimates of potential impact and consequences
	• Estimates of likelihood that threats exploit vulnerabilities
	• Determinations of risk to the organization
	• Risk response guidance from the organization's risk management strategy
	• Directions and guidance on appropriate responses to risk
	• Outputs from the Tier 1 risk assessment element
		• Risk response identification
		  ▫ Risk acceptance
		  ▫ Risk avoidance
		  ▫ Risk mitigation
		  ▫ Risk sharing
		  ▫ Risk transference
		  ▫ Combination
		• Evaluate alternatives
		• Divide and implement risk response
			• Risk response plan
			  ▫ Designation of responsible Individuals or organizational elements
			  ▫ Dependencies of each selected risk response measure on other risk response measures
			  ▫ Dependencies of selected risk response measures on other factors
			  ▫ Timelines for implementation of risk response measures
			  ▫ Plans for monitoring the effectiveness of risk response measures
			  ▫ Triggers for risk monitoring
			  ▫ Results of response activities to the risk management strategy
			  ▫ Interim risk response measures selected for implementation

RISK MONITORING	• Information regarding industry best practices, tools and frequency
	• Risk management strategy including risk assessment methodology
	• Cybersecurity governance structure
	• Performance information
	• Comprehensive lists of identified risks
		• Develop risk monitoring strategy
		  ▫ Monitoring implementation
		  ▫ Monitoring effectiveness
		  ▫ Monitoring changes
		  ▫ Automated vs. manual monitoring
		  ▫ Frequency of monitoring
		• Monitor risk
			• Verify required risk response measures are implemented and cybersecurity requirements are derived from and traceable to an organization's mission and business functions
			• Determine the ongoing effectiveness of risk response measures
			• Identify changes to IT and ICS and its environments of operation
			• Develop a risk monitoring strategy and insert it into the risk management strategy

Table 4: Tier 1 RMP Overview

4. TIER 2: THE MISSION AND BUSINESS PROCESSES

At Tier 2, mission and business process owners consider cybersecurity risks from an operations perspective and explicitly take into account the adverse impact a process may have on the mission objectives of the organization's operations. This can be viewed as lines of business in which the business processes in an Electricity Sector organization are often grouped by generation, transmission, distribution, markets, and field operations. The identification of mission and business processes defines the criticality and sensitivity of the information as well as the flows internal and external to the organization.

Cybersecurity architecture is an integral part of an organization's enterprise architecture. It represents that portion of the enterprise architecture that specifically addresses IT and ICS resilience and provides architectural information for the implementation of cybersecurity capabilities. The primary purpose of the cybersecurity program is to develop the policies and procedures and to ensure that mission and business process cybersecurity requirements are consistently applied within an organization.

Tier 2 of the RMP addresses each of the elements in the risk management cycle:

- Frame;
- Assess;
- Respond; and
- Monitor.

The primary output from Tier 2 of the RMP is the cybersecurity program and architecture that will be used in Tier 3.

4.1 RISK FRAMING AT TIER 2

The risk framing element at Tier 2 identifies and documents the cybersecurity environment. Risk framing will establish a framework to guide the development of a cybersecurity program across the organization's mission and business processes. An essential input to this risk framing element at Tier 2 is the risk management strategy established in Tier 1. The organization and its business units identify the mission and business processes supporting the mission objectives and determine the risk assessment methodologies to be used. Within Tier 2, the business units identify and map cybersecurity threats, vulnerabilities, consequences, and impacts to each of the mission and business processes identified.

Methodologies are established to evaluate the impacts associated with the loss of confidentiality, integrity, and availability of operational information, data, and IT and ICS resources. These methodologies are integrated into a standard risk measurement methodology so risk assessments for the individual processes are harmonized and their resulting risks can be prioritized as inputs to the cybersecurity program to determine administrative and technical controls, mitigations, and countermeasures. The organization then assesses and determines the appropriate resources and funding needed to develop and implement the cybersecurity program.

4.1.1 Inputs

Inputs to the risk framing element for Tier 2 may include:

- Cybersecurity program and architecture (if already established);
- Mission objectives from the Tier 1 risk framing element;
- Risk management strategy from Tier 1;
- Governance structure from Tier 1;

- High-level security requirements identified at Tier 1;
- Constraints identified at Tier 1;
- Risk tolerance formulated at Tier 1; and
- Feedback from the risk monitoring element at Tier 2 and Tier 3.

4.1.2 Activities

Activities for the risk framing element will include identifying the mission and business processes linked to the objectives identified in Tier 1, selecting a risk assessment methodology to be used in Tier 2, taking inventory of the applications that support the mission objectives, and designating the application owner, classification, and disaster recovery (recovery time objectives and recovery point objectives [RTO/RPO]).

4.1.2.1 Identification of Mission and Business Processes and Applications

In Tier 2, organizations inventory and document their mission and business processes as well as the applications[34] that support the mission objectives identified in Tier 1. The mission and business processes derived from an analysis of the mission objectives may be shared across other business processes. These processes can be characterized as horizontal or vertical. Horizontal processes are those associated with cross-functional business processes, like payroll, regulatory services, or IT services. Vertical processes are more specific to a business function, such as field or customer operations, transmission operations, or distribution engineering. A highly integrated organization, for example, may include a large number of vertical processes related to generation, transmission, distribution, energy marketing and trading, and customer relationship management. A specialized organization performing a limited set of reliability functions, such as reliability coordination and/or load and generation balancing authority, may have fewer such vertical processes. The relationship between these processes and applications, whether they are insourced or outsourced, is an important input for the risk assessment element later in this section.

The determination of how granular an organization needs to be in the definition of its business processes is a function of how the organization determines the highest level at which the process supports a specific objective and performs a finite and coherent set of activities. These processes are reviewed to identify their cybersecurity objectives (e.g., confidentiality, integrity, availability). From the cybersecurity risk management perspective, the commonality of cybersecurity objectives derived from the security requirements is an important input in the determination of common requirements across mission and business processes. Electricity Sector organizations that perform Bulk Electric System functions may find useful guidance for identifying processes in the functions defined in the NERC Functional Model.[35]

4.1.2.2 Establish Risk Tolerance and Risk Methodology

Once the mission and business processes have been identified, each process is analyzed to establish process-specific cybersecurity risk assumptions and constraints. The impacts to the organization for the loss of confidentiality, integrity, and availability are established for each identified IT and ICS process. Electricity Sector organizations may consider how regulatory and contractual constraints may influence the impact to the identified processes. Some examples of such constraints are:

- Occupational Safety and Health Administration (OSHA) regulations;
- Health Insurance Portability and Accountability Act (HIPAA) for those organizations that process such information for internal health and medical-related processes;

[34] Application refers to a technology enabled solution that supports the mission and business process. The application is only defined at a level sufficient to identify the criticality to the mission and business process.

[35] For additional information, see NERC Functional Model.

- NERC reliability standards (CIP and others) for those organizations that are registered as NERC functional entities;
- Nuclear Regulatory Commission (NRC) cybersecurity regulations;
- Payment Card Industry Data Security Standards (PCI-DSS) for organizations processing credit card payments from customers;
- Sarbanes-Oxley Act (SOX) requirements for qualified publicly listed companies;
- Federal Information Security Management Act (FISMA) requirements for U.S. Federal Electricity Sector organizations; and
- Corporate contracts and/or agreements (including outsourcing and third parties).

In conjunction with the impact assessment, process-specific risk tolerance needs to be established. Organizations consider the risk tolerance policies from the Tier 1 analysis and apply this guidance to each mission and business process. Risk tolerance may vary based on the impact to the mission or business process. Feedback from the risk assessment phase from Tier 2 and Tier 3, especially the impact, may provide essential input to this aspect of the framing process as part of the iterative process for determining risk tolerance. Additional inputs to process-specific risk tolerance, including sources of information for cybersecurity threats and vulnerability assumptions (such as vendors, the ES-ISAC, Financial Services Information Sharing and Analysis Center [FS-ISAC], IT Information Sharing and Analysis Center [IT-ISAC], NERC Alert, ICS Cyber Emergency Response Team [ICS-CERT], and the US-CERT) may also be considered.

The risk assessment methodology provides a standard way to measure impact across the organization (often expressed as financial impacts in dollar amounts or in a variable scale of high, medium, and low). However, the risk assessment methodology may define impact in different ways for groups of processes using qualitative analysis techniques. Generally, risk is a function of the threat, vulnerability, likelihood, and consequence/impact:

$$\textbf{Risk} = f\textbf{(threat, vulnerability, likelihood, consequence/impact)}$$

An option for determining risk level may be to focus on consequence/impact. At the mission and business level, it is only important for the organization to understand the inherent level of risk in the process and to further define the methodology to determine risks in Tier 3.

The mission and business processes and the establishment of standard methodologies for determining the impacts associated with the loss of confidentiality, integrity, and availability of the process information, data elements, and IT and ICS for both business administrative services and operation of Electricity Sector resources are essential in providing input to the risk assessment element.

4.1.2.3 Identify Cybersecurity Program and Architecture

For organizations that currently maintain cybersecurity programs and architecture, it is during the risk assessment and risk response elements that an inventory of existing policies, architecture, and guidance are identified for validation. For organizations without a cybersecurity program and/or architecture, implementing the complete risk cycle in Tier 2 will develop these for your organization.

4.1.2.4 Enterprise Architecture

Enterprise architecture is a management practice employed by an Electricity Sector organization to maximize the effectiveness of IT and ICS resources in supporting achievement of mission and business success. Enterprise architecture establishes a clear and unambiguous connection from investments, including cybersecurity investments, to measurable performance improvements whether for an entire organization or portion of an organization. Enterprise architecture provides:

- A disciplined and structured approach for managing IT and ICS resources;
- Greater clarity and understanding of the infrastructure;
- Design and development of the associated IT and ICS for maximizing resilience;
- An opportunity to standardize, consolidate, and optimize resources;
- A common language for discussing risk management issues related to mission and business processes and performance goals;
- Efficient, cost-effective, consistent, and interoperable cybersecurity capabilities to help organizations better protect mission and business functions; and
- Concepts of segmentation, redundancy, and elimination of single points of failure.

4.1.3 Outputs

Outputs from the Tier 2 risk framing activities may include:

- Identification of the mission and business processes that support the organization's risk management strategy from Tier 1;
- Documented lists of the impacts associated with the loss of confidentiality, integrity, and availability of the process information, including data elements, and IT and ICS resources for both business administrative services and operations of Electricity Sector resources;
- Documented risk assessment methodologies to be applied across all mission and business processes;
- Process-specific risk tolerances; and
- An inventory of applications, classifications, and owners that support mission and business processes identified during the Tier 2 framing element.

4.2 Risk Assessment at Tier 2

In the risk assessment element at Tier 2, mission and business processes and associated application risks are identified using the selected risk assessment methodologies defined in the risk framing element in Tier 2. These risks are mapped to each of the mission and business processes and to the applications that support those processes. The assessment element includes the development of a prioritized list of processes based on the consequence/impact to the organization.

4.2.1 Inputs

Inputs to the Tier 2 risk assessment element may include:

- The risk management strategy from Tier 1;
- Reports from the threat and vulnerability sources[36] identified in Tier 1 and at the process-specific risk framing element in Tier 2;
- Selected risk assessment methodologies from the framing element in Tier 2;
- Inputs from previous Tier 2 risk assessments and feedback from Tier 3 monitoring element;
- Inventory of mission and business processes and applications from the framing element of Tier 2 that support the organization's mission objectives developed in Tier 1; and
- A documented list of the impacts associated with the loss of confidentiality, integrity, and availability of mission and business process information, data elements, and IT and ICS.

[36] When reviewing the process-specific cybersecurity threat and vulnerability reports, organizations must make a determination on whether threat reports have provided enough information to determine a probability of threat.

4.2.2 Activities

4.2.2.1 Prioritize Mission and Business Processes based on Consequence/Impact

In the assessment element of Tier 2, an organization first determines the consequence/impact for each mission and business process and application. In prioritizing mission and business processes, the organization may consider the consequence/impact to the reliability of the Electricity Sector.

4.2.2.2 Risk Determination

In determining risk at Tier 2, the organization focuses on organizational operations and vulnerabilities associated with architectural design and mission and business processes. In some cases, these processes may have greater impact on the ability of the organization to successfully carry out its mission and business functions due to the potential impact across multiple IT and ICS and mission environments. Organizations review process-specific cybersecurity threat and vulnerability reports to decide whether these reports have provided enough information to determine a probability of a threat.

In addition, an organization will prioritize each mission and business process to make risk response and monitoring decisions. Using the risks determined for the processes, the organization prioritizes the mission and business processes according to the determined risks and uses this priority list in the design of the cybersecurity program and the cybersecurity architecture within the enterprise architecture.

4.2.3 Outputs

Outputs from the Tier 2 risk assessment element may include:

- A mission and business process list prioritized by impact and;
- Specific threat and vulnerability information generated at Tier 2 that is used for the creation of the cybersecurity program and architecture.

4.3 Risk Response at Tier 2

In the Tier 2 risk response element, Electricity Sector organizations use the list of mission and business processes prioritized by impact from the risk assessment element. In most cases, input from the risk assessment element also influences the design of the IT and ICS architecture itself, due to considerations for meeting the requirements of the cybersecurity program.

4.3.1 Inputs

Inputs to the Tier 2 risk response element may include:

- The risk management strategy from Tier 1;
- A Tier 2 mission and business process list, prioritized by impact;
- The Tier 1 business processes risk tolerance;
- The risk constraints from Tier 1 and Tier 2;
- The cybersecurity and enterprise architectures; and
- Threat and vulnerability information, identified in the Tier 2 risk assessment activities.

4.3.2 Activities

4.3.2.1 Risk Response

Tier 2 risk response activities help organizations identify, evaluate, approve, and implement appropriate risk responses to accept, avoid, mitigate, share, or transfer the impact risks of their operations, resources, and other organizations that may result from the operation and use of IT and ICS. As such, organizations

develop risk mitigation strategies based on strategic goals and objectives, mission and business requirements, and organizational priorities.[37]

4.3.2.2 Defining the Cybersecurity Program and Architecture

During the response element of Tier 2, organizations develop and/or refine their cybersecurity program and architecture. Electricity Sector organizations consider how they can inject cybersecurity architecture-planning activities into the definition of the enterprise architecture. The dangers of defining the cybersecurity architecture into its own silo, separate from the enterprise architecture definition process, can be cost prohibitive and introduce additional risks to the Electricity Sector organization. Organizations may find it appropriate to define different cybersecurity architectural principles and ensure that connections or inheritance of cybersecurity controls between IT and ICS are clearly recognized.

A cybersecurity program may include:

- High-level policies and standards that define the objectives of the organization's cybersecurity program;
- Roles and responsibilities for the activities in the cybersecurity program;
- Establishment of minimum operating standards with common cybersecurity controls[38] that provide defense-in-depth and defense-in-breadth;
- Requirements and design principles for implementing controls, with consideration for various process-specific requirements;
- Procedures for implementing controls and enforcing policies;
- Transfer of high-operational impact risks to other mission and business processes; and
- Requirements and design principles for monitoring and measuring the effectiveness of the cybersecurity programs.

The cybersecurity architecture for organizations in the Electricity Sector may include the below items.

Guiding principles for network perimeter controls, access controls, and monitoring

Organizations need to establish, identify, and maintain only authorized communication as part of the cybersecurity architecture. This includes defining discreet ingress and egress filtering and documenting data flows. Sufficient system logs need to be maintained and preferably correlated to identify anomalous communication. There also need to be sufficient access controls that provide for guaranteed authentication, authorization, and accounting of people, systems, and processes.

Segmentation strategies for the various network and process types

Segmentation strategies for the various network types defined by cybersecurity requirements may include strategies for Internet connections, public carrier networks, virtual private networks (VPNs), corporate Intranet networks, and high-value networks, such as ICS networks. These provide guidance for the use of such controls as network firewalls (such as principles guiding the use of types of firewalls for public network perimeters or those for perimeters to networks hosting high-value resources or secured enclaves adjacent to business networks). Segmentation strategies for processes (e.g., production, development, and test) that are determined by the risk assessment to be high-risk mission and business processes may include increased intrusion detection monitoring for those processes

[37] Additional information regarding how an organization responds to risk can be found in Appendix G, Risk Response Strategies.

[38] A common cybersecurity control is one that is utilized and/or inherited throughout an organization.

Special requirements for generation plants and transmission and distribution field assets
Many field assets have requirements for providing operational and nonoperational[39] data to engineering or business users for planning and long-term analysis purposes. Organizations may provide "fleet model" standardized architectures to do this in a secure and controlled manner.

Data center and server farm environments
Electricity Sector organizations may provide standardized network architectures for providing secure services from networks with a high concentration of systems providing common services such as Web application services, database services, or file services. The architecture will clearly stipulate those elements necessary to provide an adequate level of network access control and monitoring for such networks.

Remote access requirements for business and operations networks
The ability to remotely access systems for the purpose of maintenance and support is an important function. Electricity Sector organizations may provide a standardized architecture that would provide the level of cybersecurity commensurate with their risk profiles. Organizations should consider the threat environment for the processes or class of processes and provide architectural options for remote access to the different cybersecurity requirements, as guidance to selecting actual controls at Tier 3.

Guiding principles for end point protection
Electricity Sector organizations may consider an adequate level of standardization to optimize the management of end points, taking into consideration the various differing cybersecurity requirements or priorities. These may include antivirus and malware protection, system integrity, system-level access controls, and cybersecurity event monitoring.

Standardized requirements for supply chain sourcing processes
Organizations in the Electricity Sector need to consider the standard cybersecurity requirements included in various types of supply chain sourcing processes and a standardized process for both technical and commercial evaluation for cybersecurity requirements, including frameworks for vendor qualification, technical evaluation, commercial evaluation, and selection processes.

Standardized requirements for change management, testing, and production certification processes
Electricity Sector organizations provide standardized architectural elements necessary to develop a framework for the change control, configuration management, testing, and certification processes to assure that cybersecurity effectiveness is maintained. These may include standardized software tools and methodologies for managing system changes, and testing across the organization.

Human resource practices relevant to cybersecurity
Organizations need to establish repeatable on-boarding and off-boarding processes to evaluate the suitability of the workforce. The on-boarding process needs to include a personnel risk assessment that performs at least a 7-year criminal history verification, identity verification (e.g., Social Security Number and driver's license), credit check, personal and professional reference check, and verification and validation of education and professional credentials. The personnel risk assessment may be updated based on risk classification determined by the organization. The organization needs to establish an off boarding program as well to ensure that all system and physical access is removed promptly. For cases in which an employee is terminated, organizations may consider establishing repeatable procedures to forensically maintain workforce systems for investigations.

[39] Operational data is data used to operate the system, such as line flows and breaker positions. Nonoperational data is data about the operations of the systems, such as configuration information, asset management information, or after-the-fact analysis data.

Standardized processes for cybersecurity incident response
Organizations need to establish repeatable processes that include training their workforce on how to identify, report, and respond to suspected cybersecurity incidents. The processes need to account for creating the categories of events and incidents (e.g., denial of service, malicious code/software, and inappropriate use), the identification of the computer incident response team, and their roles and responsibilities. The purpose of the incident response plan is to have processes that determine whether an incident has occurred, whether the incident was contained and/or eradicated, and whether the system recovered from the incident. There may be defined processes for the forensic analysis and storage of incident evidence.

Standardized processes for operational and business recovery
Organizations need to develop repeatable processes that are based on the classification and RTO/RPOs to ensure that applications are available to the organization. The degree to which business recovery is supported by the organization may be different for each mission or business process application.

4.3.3 Outputs

Output for the Tier 2 risk response element includes:

- Cybersecurity program, including policies, standards, and procedures; and
- Cybersecurity architecture.

4.4 Risk Monitoring at Tier 2

In the risk monitoring element, Electricity Sector organizations monitor and measure the effectiveness and level of conformance of their cybersecurity program and architecture. This process helps identify risk-impacting changes to IT and ICS and their environments of operation.

4.4.1 Inputs

Input to the Tier 2 risk monitoring element may include:

- The risk management strategy from Tier 1;
- The cybersecurity program and architecture;
- The results of previous audits, assessments, and cybersecurity reporting from Tier 2 and Tier 3;
- Threat and vulnerability industry alerts and warnings; and
- The outputs from the Tier 2 risk response element.

4.4.2 Activities

To monitor the effectiveness of and measure the level of conformance to the cybersecurity program and architecture, the Electricity Sector organizations may:[40]

Establish metrics to measure the level of conformance to the cybersecurity architecture
A good measure of the appropriateness of the cybersecurity architecture is the level at which the actual implementation of cybersecurity controls conform to that architecture. By periodically assessing the number of deviations from the standard architecture and the rationales for these deviations, organizations can fine tune the architecture in an iterative process.

[40] Draft NIST SP 800-137, *Information Security Continuous Monitoring for Federal Information Systems and Organizations,* provides guidance on monitoring organizational information systems and environments of operation.

Measure the effectiveness of the cybersecurity architecture

Measuring the effectiveness of the cybersecurity architecture ensures that the defined architecture is implemented and still providing a valid framework for the selection of controls for Tier 3. This is usually conducted in conjunction with an assessment of the implemented controls through testing and analysis. The results of this assessment can then be used as input for the risk response element to help develop new or modified architectural elements for the cybersecurity architecture. For example, performance requirements may dictate a change from a proxy-based network access control architecture to an inspection-based network access control architecture. In turn, inspection-based access control may have limitations on behavioral analysis or the use of heuristics in malware prevention.

Periodically reassess the cybersecurity architecture

Electricity Sector organizations need to define the frequency of comprehensive, organization-wide monitoring of the cybersecurity architecture implementation to maintain its effectiveness and conformance. Each organization allows for enough time between monitoring intervals for a comprehensive review and implementation of mitigations and changes to the architecture to be completed.

Monitor changes to the environment

Electricity Sector organizations need to establish processes to review changes to the threat and vulnerability landscape for input to the risk response element. The evolution of threats from simple threats based on basic scripts to sophisticated, multithreat advanced malware is an example of how changes to the threat environment can result in change needed to the cybersecurity architecture in order to respond to the threat. Deviations from enterprise architectures are evaluated by the governance body.

4.4.3 Outputs

Outputs from the Tier 2 risk monitoring activities may include:

- Risk monitoring reports from the conformance and effectiveness reviews and the appropriate resulting mitigations and changes; and
- A risk monitoring strategy embedded in the cybersecurity program that includes metrics, frequency, and scope of the monitoring processes.

The output from the Tier 2 risk monitoring element will be the input to the risk framing element in Tier 3 and the feedback to Tier 2 and Tier 1.

4.5 SUMMARY AT TIER 2

At Tier 2, mission and business process owners refine the risk management strategy and identify and prioritize the processes that are critical to the organization's operations. It is at this tier that the cybersecurity program and architecture are refined as inputs to the activities at Tier 3 and as feedback to activities in Tier 1.

The following table provides an overview of the inputs, activities, and outputs from the risk framing, assessment, response, and monitoring elements in Tier 2 of the RMP.

	INPUTS	ACTIVITIES	OUTPUTS
RISK FRAMING	• Cybersecurity program and architecture (if already established) • Mission objectives from the Tier 1 risk framing element • Risk management strategy from Tier 1 • Governance structure from Tier 1 • The high-level security requirements identified at Tier 1 • Constraints identified at Tier 1 • Risk tolerance formulated at Tier 1 • Feedback from the risk monitoring element at Tier 2 and Tier 3	• Identify mission and business processes and applications • Establish risk tolerance and risk methodology • Identify cybersecurity program and architecture • Develop or refine enterprise architecture	• Identification of the mission and business processes that support the organization's risk management strategy from Tier 1 • Documented lists of the impacts • Documented risk assessment methodologies to be applied across all mission and business processes • Process-specific risk tolerances • An inventory of applications, classifications, and owners that support mission and business processes identified at Tier 2 framing element
RISK ASSESSMENT	• Identification of the mission and business processes that support the organization's risk management strategy from Tier 1 • Documented lists of the impacts; • Documented risk assessment methodologies to be applied across all mission and business processes; • Process-specific risk tolerances; and • An inventory of applications, classifications, and owners that support mission and business processes identified at Tier 2 framing element.	• Prioritize mission and business processes based on consequence/ impact • Determine risk	• A mission and business process list prioritized by impact • Specific threat and vulnerability information generated at Tier 2 that is used for the creation of the cybersecurity program and architecture
RISK RESPONSE	• Risk management strategy from Tier 1 • Tier 2 mission and business process list prioritized by impact • Tier 1 business processes risk tolerance • Risk constraints from Tier 1 and Tier 2 • Cybersecurity and enterprise architectures • Threat and vulnerability information identified in the Tier 2 risk assessment activities	• Determine and implement risk response ▫ Defining the cybersecurity program and architecture ▫ Guiding principles ▫ Segmentation strategies ▫ Special requirements ▫ Data center and server farm environments ▫ Remote access requirements ▫ Standardized requirements ▫ Human resource practices ▫ Standardized processes	• Cybersecurity program including policies, standards, and procedures • Cybersecurity architecture
RISK MONITORING	• Risk management strategy from Tier 1 • Cybersecurity program and architecture • Results of previous audits, assessments • Cybersecurity reporting from Tier 2 and Tier 3 • Threat and vulnerability industry alerts and warnings • Outputs from the Tier 2 risk response element	• Establish metrics to measure the level of conformance to the cybersecurity architecture • Measure the effectiveness of the cybersecurity architecture • Periodically reassess the cybersecurity architecture • Monitor changes to the environment	• Risk monitoring reports from the conformance and effectiveness reviews and appropriate resulting mitigations and changes • A risk monitoring strategy embedded in the cybersecurity program that includes metrics, frequency and scope of the monitoring processes

Table 5: Tier 2 RMP Overview

5. TIER 3: INFORMATION TECHNOLOGY AND INDUSTRIAL CONTROL SYSTEMS

Tier 3 of the risk management model represents the IT and ICS resources. To address risk at Tier 3, the same four elements—framing, assessing, responding, and monitoring—are applied. The major activities at Tier 3 utilize the outputs from the Tier 2 cybersecurity program and architecture and the Tier 1 risk management strategy. Using these inputs, the organization inventories the resources, develops cybersecurity plans, evaluates the cybersecurity posture, selects appropriate controls, and evaluates the impact and effectiveness of those controls at the system level. The following sections provide a detailed description of the inputs, activities, and outputs for each of the elements.

> ICSs are generally time critical, with specific determinism requirements for communication jitter and latency. IT systems generally have much less stringent requirements. Delays in database interactions or Web page access are not unexpected by IT users. The bandwidth available for IT systems is typically more important to pass files or datasets. Delays or variability in the communications for ICS can have unintended consequences for the control system components and may lead to communication disruptions and a loss of availability. The determinism of individual network packets is more important than bandwidth, since ICS communications usually involve small bits of information passed on a regular basis. Adding cybersecurity controls, such as encryption or packet-level authentication, may reduce the level of performance that an ICS can deliver.

5.1 RISK FRAMING AT TIER 3

5.1.1 Inputs

The inputs to the risk framing element at Tier 3 for IT and ICS may include:

- Risk management strategy from Tier 1;
- Threat and vulnerability information from Tier 2;
- Prioritized list of processes and applications by impact/consequence from Tier 2;
- Catalogue of cybersecurity controls;
- Cybersecurity program and architecture;
- Enterprise architecture;
- Results from monitoring element of Tier 3; and
- Inventory of current systems and resources from Tier 3.

5.1.2 Activities

5.1.2.1 Information Technology and Industrial Control Systems Inventory

The IT and ICS inventory process begins by identifying the systems, resources, and relationships between the IT and ICS; the mission and business processes; and the applications they support. The organization that owns, manages, and/or controls the resources is derived from the relationship between the mission and business process, the application owner, and any contractual arrangements with internal or external organizations. This establishes authority and accountability for cybersecurity of the systems and resources.

5.1.2.2 Define or Refine the Cybersecurity Plans[41]

For each IT and ICS the organization gathers contextual information about the system, including the inventory, owners, network diagrams, data flows, and interfaces to other systems. The cybersecurity plan addresses the technical configuration and cybersecurity posture of the system. In the development of the cybersecurity plan, organizations identify the common cybersecurity controls applicable to the IT and ICS.

The results of the cybersecurity plan process influence both the selection and refinement of appropriate cybersecurity controls for the IT and ICS as well as the minimum assurance requirements. The cybersecurity plan process reviews organization responsibilities for each system in order to establish clear ownership to assess and respond to risk in subsequent activities. The level of detail provided in the cybersecurity plan is determined by the organization, and information may be added to the description as it becomes available.

The cybersecurity plan for the IT and ICS may include:

- Full descriptive name, including associated acronym;
- Owner and risk official (including contact information);
- Parent or governing organization that manages, owns, and/or controls it;
- Location and environment of operations (narrative and diagram views);
- Version or release number of the IT and ICS applications and hardware;
- Purpose, functions, and capabilities of (mission and business processes supported) and sensitivity of each function;
- IT and ICS integration into the enterprise architecture and cybersecurity architecture;
- Threat and vulnerability information;
- Cybersecurity controls;
- Common cybersecurity controls;
- Types and sensitivity of information processed, stored, and transmitted;
- Boundary for risk management and cybersecurity authorization purposes;
- Applicable laws, policies, regulations, or standards affecting the cybersecurity;
- Architectural description, including network topology;
- Hardware and firmware devices;
- System and applications software;
- Hardware, software, and system interfaces (internal and external);
- Subsystems (static and dynamic);
- Information flows and paths (including inputs and outputs);
- Network connection rules for external communications;
- Encryption techniques used for information processing, transmission, and storage;
- Authentication, authorization, and accounting processes that include shared accounts, administrative account, and user account management;
- Organizational affiliations, access rights, and privileges;
- Disaster recovery or business continuity requirements for RTO/RPO;
- Incident response points of contact;
- Cybersecurity assessment procedures; and
- Other information as required by the organization.

[41] Cybersecurity plan development outlines are provided by organizations such as NRECA and NIST SP 800-18.

This information will be used during the assessment element to evaluate the system's alignment with the cybersecurity program and architecture.

5.1.3 Outputs

The outputs from the Tier 3 risk framing element may include a baseline cybersecurity plan that contains an inventory of the IT and ICS, with identification of boundaries, and a list of threats and vulnerabilities.

5.2 Risk Assessment at Tier 3

5.2.1 Inputs

The inputs to the risk assessment element at Tier 3 are:

- Cybersecurity plan; and
- Assessment methodologies from Tier 2.

5.2.2 Activities

5.2.2.1 Perform Cybersecurity and Risk Assessment

This activity assesses the existing cybersecurity risk by using the assessment procedures defined in the cybersecurity plan.[42] The cybersecurity assessment considers new threats and vulnerabilities to guide the adjustment of existing controls and the selection of new controls. It does this by determining the extent with which the controls are implemented correctly, operating as intended, and producing the desired outcome, with respect to meeting the cybersecurity requirements for the IT and ICS. Organizations determine the level of assessor independence. Following the cybersecurity assessment, the organization determines the consequence/impact of the threats and vulnerabilities, and prioritizes the results. The reliability and accuracy of risk determinations are dependent on the currency, accuracy, completeness, and integrity of information collected.

5.2.2.2 Cybersecurity Risk Assessment Report

Organizations need to prepare a cybersecurity risk assessment report, documenting the issues, findings, and recommendations for correcting weakness from the cybersecurity control assessments. This assessment report must include the necessary information to determine the effectiveness of the cybersecurity controls employed within or inherited by the IT and ICS. Cybersecurity control assessment results are then documented with a level of detail appropriate for the assessment in accordance with the reporting format prescribed by the policies of the organization.

5.2.3 Outputs

The output from the Tier 3 risk assessment element is a cybersecurity risk assessment report with appropriate findings and recommendations.

5.3 Risk Response at Tier 3

5.3.1 Inputs

The inputs to the risk response element at Tier 3 are:

[42] The assessment may include penetration testing, vulnerability assessments, code reviews, software code reviews, and other appropriate tests.

- Cybersecurity plan; and
- Cybersecurity risk assessment report.

5.3.2 Activities

5.3.2.1 Risk Response Actions

As a result of the cybersecurity and risk assessment, an organization must determine the appropriate risk response action:[43]

- Risk acceptance;
- Risk avoidance;
- Risk mitigation;
- Risk sharing;
- Risk transference; or
- Combinations of the above.

5.3.2.2 Select and Refine Cybersecurity Controls

Cybersecurity controls will be selected and refined based on the cybersecurity categorization of the IT and ICS. This is incorporated into the cybersecurity plan. The cybersecurity control selection process includes:

- Listing cybersecurity controls to be implemented;
- Tailoring the baseline cybersecurity controls for the system;
- Supplementing the tailored baseline cybersecurity controls, if necessary, with additional controls and/or control enhancements to address unique needs based on the risk assessment; and
- Describing the intended application of each control.

5.3.2.3 Cybersecurity Plan Acceptance

Upon completion of the cybersecurity plan, the senior executive function reviews the plan and accepts the response actions identified in the plan. This process documents the organizational acceptance of risk.

5.3.2.4 Risk Mitigation Plan

The organization implements cybersecurity controls based on the findings and recommendations of the cybersecurity risk assessment report. The cybersecurity plan is updated based on the findings of the assessment and any remediation actions taken. The implementation of new controls or the modification of existing controls requires a reassessment to verify alignment with the cybersecurity plan. Once the response element is complete, the cybersecurity plan will contain an accurate list and description of the cybersecurity controls implemented, including compensating controls,[44] and a list of residual vulnerabilities. The organization may also develop a risk mitigation plan reflecting the organization's priorities for addressing the remaining weaknesses and deficiencies in the IT and ICS and its environment of operation. A mitigation plan identifies:

- The tasks to be accomplished, with a recommendation for completion either before or after IT and ICS implementation;
- Compensating controls and measures;
- The resources required to accomplish the tasks;

[43] Additional information regarding how an organization responds to risk can be found in Appendix G, Risk Response Strategies.

[44] A compensating control is a cybersecurity control employed in lieu of a recommended control that provides equivalent or comparable control.

- Any milestones in meeting the tasks; and
- The scheduled completion dates for the milestones.

5.3.3 Outputs

The outputs from the Tier 3 risk response element are:

- Risk acceptance decision;
- Refined cybersecurity plan; and
- Risk mitigation plan.

5.4 RISK MONITOR AT TIER 3

Ongoing monitoring of cybersecurity controls is essential for an effective cybersecurity plan. Electricity Sector organizations need to develop a strategy for the continuous monitoring of cybersecurity control, to include review of any proposed or actual changes to the IT and ICS. The implementation of a robust, continuous monitoring program allows an organization to understand the cybersecurity state over time and in a highly dynamic environment with changing threats, vulnerabilities, and technologies. An effective monitoring program includes:

- Configuration management and change control processes;
- Cybersecurity impact analyses on proposed or actual changes to the IT and ICS;
- Assessment of selected cybersecurity controls employed; and
- Cybersecurity status reporting.

5.4.1 Inputs

The inputs to the risk monitoring element at Tier 3 are:

- Cybersecurity program and architecture;
- Refined cybersecurity plan;
- Risk mitigation plan;
- Threat and vulnerability information; and
- Monitoring methodology from Tier 2.

5.4.2 Activities

5.4.2.1 Configuration Management and Change Control

Changes to resources and cybersecurity controls are managed through configuration management and change control processes. A disciplined and structured approach to managing, controlling, and documenting changes to IT and ICS and their environment of operation is an essential element of an effective cybersecurity control monitoring program. It is important to record any relevant information about specific changes to hardware, software, or firmware, such as version or release numbers, descriptions of new or modified features/capabilities, and cybersecurity implementation guidance.

5.4.2.2 Ongoing Cybersecurity Control Assessment

For this activity, organizations need to assess a selected subset of the technical, management, and operational cybersecurity controls employed within and inherited by the IT and ICS, in accordance with the Tier 1 monitoring strategy defined by the organization. The selection of cybersecurity controls to be monitored and the frequency of monitoring is based on the monitoring strategy developed by the IT and ICS owner(s) and approved by the risk executive. Automation and tools are likely to be used to verify whether a control is working as described and whether it remains an effective mitigation to specific risks.

5.4.2.3 Monitoring New Threats and Vulnerabilities

As part of the ongoing monitoring element, an organization needs to evaluate new threats and vulnerabilities identified during the framing element in Tiers 1 and 2 by reviewing and responding to additional vendor or industry warnings or alerts. To maintain an up-to-date awareness of threats and vulnerabilities, the organization must establish and maintain a schedule for checking applicable information sources.

5.4.2.4 Monitoring the Cybersecurity Mitigation Plan

During the monitoring element, an organization needs to continuously evaluate the mitigation plan to correct weaknesses or deficiencies identified during the cybersecurity control assessment. Organizations may use this as a means to report their system level cybersecurity status to management. Cybersecurity controls that are modified, enhanced, or added during the monitoring process are reassessed to ensure that appropriate corrective actions are taken to eliminate weaknesses or deficiencies or to mitigate identified risks.

5.4.2.5 Cybersecurity Status Reporting

Electricity Sector organizations need to report their IT and ICS cybersecurity status to the appropriate governance on an ongoing basis and in accordance with their monitoring strategy. This reporting includes the effectiveness of cybersecurity controls employed within or inherited by the IT and ICS. Organizations may need to review the reported cybersecurity status of the IT and ICS on an ongoing basis and in accordance with the monitoring strategy to determine whether the risk to operations and resources remains acceptable. This reporting can be event driven, time driven or both. The cybersecurity status report provides:

- Leadership with information regarding the cybersecurity state and the effectiveness of deployed cybersecurity controls;
- A description of the ongoing monitoring activities;
- The IT and ICS owners information on how vulnerabilities are being addressed;
- Ongoing communication with senior executives; and
- A summary of changes to cybersecurity plans and cybersecurity assessment reports.

5.4.2.6 Removal and Decommissioning

Electricity Sector organizations implement a decommissioning strategy when resources are removed from service. When a resource is removed from operation, a number of risk-management–related actions are required. Electricity Sector organizations ensure that:

- Cybersecurity controls addressing a system removal and decommissioning (e.g., media sanitization, configuration management, and control) are implemented;
- Tracking and management systems (including inventory systems) are updated to indicate the specific components being removed from service.

5.4.3 Outputs

The outputs from Tier 3 risk monitoring element may include:

- Status of the mitigation plan and remediation actions;
- Refined cybersecurity plan;
- Refined cybersecurity program and architecture; and
- Refined monitoring strategy for Tier 2 and Tier 1.

5.5 Summary at Tier 3

Tier 3 represents the application of the RMP to the IT and ICS resources. In Tier 3, organizations act on the outputs from the Tier 2 cybersecurity program and architecture and the Tier 1 risk management strategy. Applicable cybersecurity controls are selected and applied to resources, based on cybersecurity and risk assessments. Also, mitigation plans are used to monitor the progress of how and when identified residual risks are addressed during the cybersecurity and risk assessments. The outputs of Tier 3 provide feedback to the Tier 2 and Tier 1 framing elements.

The following table provides an overview of the inputs, activities, and outputs from the risk framing, assessment, response, and monitoring elements in Tier 3 of the RMP.

	INPUTS	ACTIVITIES	OUTPUTS
RISK FRAMING	• Risk management strategy from Tier 1 • Threat and vulnerability information from Tier 2 • Prioritized list of processes and applications by impact/consequence from Tier 2 • Catalogue of cybersecurity controls • Cybersecurity program and architecture • Enterprise architecture • Results from monitoring element of Tier 3 • Inventory of current systems and resources from Tier 3	• Conduct IT and ICS inventory • Define or refine the cybersecurity plans	• Baseline cybersecurity plan that include the inventory IT and ICS and identification of boundaries, and the list of threats and vulnerabilities.
RISK ASSESSMENT	• Cybersecurity plan • Assessment methodologies from Tier 2	• Perform cybersecurity and risk assessment • Develop cybersecurity risk assessment report	• Cybersecurity risk assessment report with appropriate findings and recommendations
RISK RESPONSE	• Cybersecurity plan • Cybersecurity risk assessment report.	• Determine and implement risk response actions ▫ Risk acceptance ▫ Risk avoidance ▫ Risk mitigation ▫ Risk sharing ▫ Risk transference ▫ Combinations of the above • Select and refine cybersecurity controls • Accept cybersecurity plan acceptance • Prepare risk mitigation plan	• Risk acceptance decision • Refined cybersecurity plan • Risk mitigation plan
RISK MONITORING	• Cybersecurity program and architecture • Refined cybersecurity plan • Risk mitigation plan • Threat and vulnerability information • Monitoring methodology from Tier 2	• Implement configuration management and change control • Assess ongoing cybersecurity control • Monitoring new threats and vulnerabilities • Monitoring the cybersecurity mitigation plan • Cybersecurity status reporting • Removal and decommissioning	• Status of the mitigation plan and remediation actions • Refined cybersecurity plan • Refined cybersecurity program and architecture • Refined monitoring strategy for Tier 2 and Tier 1

Table 6: Tier 3 Risk Management Process Overview

APPENDIX A

REFERENCES

LEGISLATION, POLICIES, DIRECTIVES, STANDARDS, GUIDELINES, AND CANADIAN GUIDANCE

1. American Recovery and Reinvestment Act (P.L. 111-5), February 2009.
2. Canada's Cyber Security Strategy.
3. *Canada-United States Action Plan for Critical Infrastructure* (Canada-U.S. Action Plan).
4. Canadian: Action Plan for Critical Infrastructure (2009).
5. Canadian: National Strategy for Critical Infrastructure (2009).
6. Committee on National Security Systems (CNSS) Instruction 4009, *National Information Assurance (IA) Glossary*, April 2010.
7. Committee on National Security Systems (CNSS) Instruction 1253, *Security Categorization and Control Selection for National Security Systems*, October 2009.
8. E-Government Act [includes FISMA] (P.L. 107-347), December 2002.
9. Energy Independence and Security Act of 2007 (P.L. 110-140, Title XIII–Smart Grid), December 2007.
10. Federal Information Security Management Act (P.L. 107-347, Title III), December 2002.
11. International Electrotechnical Commission 62443, *Security for Industrial Automation and Control Systems Series*.
12. International Organization for Standardization/International Electrotechnical Commission 15408:2005, *Common Criteria for Information Technology Security Evaluation*.
13. International Organization for Standardization/International Electrotechnical Commission 73:2009, *Risk Management – Vocabulary*.
14. International Organization for Standardization/International Electrotechnical Commission 31000:2009, *Risk Management – Principles and Guidelines.*
15. International Organization for Standardization/International Electrotechnical Commission 27000:2009, *Information Technology – Security Techniques – Information Security Management Systems – Overview and Vocabulary*.
16. International Organization for Standardization/International Electrotechnical Commission 27005:2011, *Information technology — Security techniques — Information security risk management*.
17. National Institute of Standards and Technology Federal Information Processing Standards Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004.
18. National Institute of Standards and Technology Federal Information Processing Standards Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006.
19. National Institute of Standards and Technology Interagency Report 7628, *Guidelines for Smart Grid Cyber Security*, August 2010.
20. National Institute of Standards and Technology Interagency Report 7298, Revision 1, *Glossary of Key Information Security Terms*, February 2011.
21. National Institute of Standards and Technology Special Publication 800-18, Revision 1, *Guide for Developing Security Plans for Federal Information Systems*, February 2006.

22. National Institute of Standards and Technology Special Publication 800-60, Revision 1, *Guide for Mapping Types of Information and Information Systems to Security Categories*, August 2008.

23. National Institute of Standards and Technology Special Publication 800-70, Revision 1, *National Checklist Program for IT Products--Guidelines for Checklist Users and Developers*, September 2009.

24. National Institute of Standards and Technology Special Publication 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009.

25. National Institute of Standards and Technology Special Publication 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, February 2010.

26. National Institute of Standards and Technology Special Publication 800-53A, Revision 1, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations: Building Effective Security Assessment Plans*, June 2010.

27. National Institute of Standards and Technology Special Publication 800-137, Initial Public Draft, *Information Security Continuous Monitoring for Federal Information Systems and Organizations*, December 2010.

28. National Institute of Standards and Technology Special Publication 1108, Release 1, *NIST Framework and Roadmap for Smart Grid Interoperability Standards*, January 2010.

29. National Institute of Standards and Technology Special Publication 800-30, Revision 1, *Guide for Conducting Risk Assessments*, (Projected Publication Spring 2011).

30. National Institute of Standards and Technology Special Publication 800-39, Revision 1, *Managing Information Security Risk: Organization, Mission, and Information System View*, March 2011.

31. National Institute of Standards and Technology Special Publication 800-82, *Guide to Industrial Control Systems (ICS) Security*, June 2011.

32. North American Electric Reliability Corporation, Critical Infrastructure Protection.

33. Office of Management and Budget, Circular A-130, Appendix III, Transmittal Memorandum #4, *Management of Federal Information Resources*, November 2000.

34. U.S. Department of Homeland Security (DHS), *DHS Risk Lexicon*, September 2010.

APPENDIX B

GLOSSARY

COMMON TERMS AND DEFINITIONS

This appendix provides definitions for security terminology used in this publication. The terms in this glossary are consistent with the commonly accepted standards, such as Software Engineering Institute (SEI), International Organization for Standardization (ISO), National Institute of Standards and Technology (NIST), and Committee on National Security Systems (CNSS).

Assurance	Grounds for confidence that the set of intended security controls in an IT and ICS are effective in their application.
Authentication	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an IT and ICS.
Availability	Ensuring timely and reliable access to and use of information.
Common Cybersecurity Control	A common cybersecurity control is a cybersecurity control that is utilized and/or inherited throughout an organization.
Compensating Control	A compensating control is a cybersecurity control employed in lieu of a recommended control that provides equivalent or comparable control.
Confidentiality	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
Cyber Attack	An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure, or for destroying the integrity of the data or stealing controlled information.
Cybersecurity	The ability to protect or defend the use of cyberspace from cyber attacks.
Cybersecurity Architecture	An embedded, integral part of the enterprise architecture that describes the structure and behavior for an enterprise's security processes, cybersecurity systems, personnel and subordinate organizations, showing their alignment with the organization's mission and strategic plans.
Cybersecurity Control Assessment	The testing and/or evaluation of the management, operational, and technical security controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the cybersecurity requirements for an IT and ICS or organization.

Cybersecurity Controls	The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an IT and ICS to protect the confidentiality, integrity, and availability of the system and its information.
Cybersecurity Plan	Formal document that provides an overview of the cybersecurity requirements for an IT and ICS and describes the cybersecurity controls in place or planned for meeting those requirements.
Cybersecurity Policy	A set of criteria for the provision of security services.
Cybersecurity Requirements	Requirements levied on an IT and ICS that are derived from applicable legislation, Executive Orders, directives, policies, standards, instructions, regulations, procedures, or organizational mission and business case needs to ensure the confidentiality, integrity, and availability of the information being processed, stored, or transmitted.
Cybersecurity Risk	The risk to organizational operations (including mission, functions, image, reputation), resources, and other organizations due to the potential for unauthorized access, use, disclosure, disruption, modification, or destruction of information and/or IT and ICS.
Cyberspace	A global domain within the information environment consisting of the interdependent network of IT and ICS infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.
Defense-in-Breadth	A planned, systematic set of multidisciplinary activities that seek to identify, manage, and reduce risk of exploitable vulnerabilities at every stage of the system, network, or subcomponent life cycle (system, network, or product design and development; manufacturing; packaging; assembly; system integration; distribution; operations; maintenance; and retirement).
Defense-in-Depth	Cybersecurity strategy integrating people, technology, and operations capabilities to establish variable barriers across multiple layers and missions of the organization.
Enterprise Architecture	The design and description of an enterprise's entire set of IT and ICS: how they are configured, how they are integrated, how they interface to the external environment at the enterprise's boundary, how they are operated to support the enterprise mission, and how they contribute to the enterprise's overall security posture.
Environment of Operation	The physical surroundings in which an IT and ICS processes, stores, and transmits information.

Industrial Control Systems	Used to control industrial processes such as manufacturing, product handling, production, and distribution.
Information Technology	A discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. In the context of this publication, the definition includes interconnected or dependent business systems and the environment in which they operate.
Integrity	Guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity.
Management Controls	The security controls for an IT and ICS that focus on the management of risk and security.
Operational Controls	The security controls for an IT and ICS that are primarily implemented and executed by people (as opposed to systems).
Organization	An Electricity Sector organization of any size, complexity, or positioning within an organizational structure that is charged with carrying out assigned mission and business processes and that uses IT and ICS in support of those processes.
Resources	Money, materials, staff, and other assets that can be utilized by an Electricity Sector organization in order meet it mission and business objectives.
Risk	A measure of the extent to which an organization is threatened by a potential circumstance or event, and typically a function of (i) the adverse impacts that would arise if the circumstance or event occurs and (ii) the likelihood of occurrence.
Risk Assessment	The process of identifying risks to organizational operations (including mission, functions, image, reputation), resources, other organizations, and the Nation, resulting from the operation of an IT and ICS. Part of risk management, incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place.
Risk Evaluation	A component of the risk assessment element in which observations are made regarding the significance and acceptability of risk to the organization.
Risk Management	The program and supporting processes to manage cybersecurity risk to organizational operations (including mission, functions, image, reputation), resources, other organizations, and the Nation, and includes: (i) establishing the context for risk-related

	activities; (ii) assessing risk; (iii) responding to risk once determined; and (iv) monitoring risk over time.
Risk Management Strategy	Any strategic-level decisions on how risk to an organization's operations, resources, and other organizations are managed by senior executives.
Risk Mitigation	Prioritizing, evaluating, and implementing the appropriate risk-reducing controls recommended from the RMP.
Risk Monitoring	Maintaining ongoing awareness of an organization's risk environment, risk management program, and associated activities to support risk decisions.
Risk Response	Accepting, avoiding, mitigating, sharing, or transferring risk to organizational operations, resources, and other organizations.
Security Objective	Confidentiality, integrity, or availability.
Technical Controls	Cybersecurity controls for an IT and ICS that are primarily implemented and executed by the IT and ICS through mechanisms contained in the hardware, software, or firmware components of the system.
Threat	Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), resources, and other organizations, through an IT and ICS via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.
Threat Assessment	Process of evaluating the severity of threat to an IT and ICS or organization and describing the nature of the threat.
Threat Source	The intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally exploit a vulnerability.
Vulnerability	Weakness in IT and ICS, system cybersecurity procedures, internal controls, or implementation that could be exploited by a threat source.
Vulnerability Assessment	Systematic examination of an IT and ICS or product to determine the adequacy of cybersecurity measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed cybersecurity measures, and confirm the adequacy of such measures after implementation.

APPENDIX C

ACRONYMS

COMMON ABBREVIATIONS

APT	Advanced Persistent Threat
CIO	Chief Information Officer
CIP	Critical Infrastructure Protection
CNSS	Committee on National Security Systems
COTS	Commercial Off-The-Shelf
DHS	Department of Homeland Security
DOE	Department of Energy
ERM	Enterprise Risk Management
ES-ISAC	Electricity Sector Information Sharing and Analysis Center
FERC	Federal Energy Regulatory Commission
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FMEA	Failure Mode And Effects Analysis
FS-ISAC	Financial Services Information Sharing and Analysis Center
HIPAA	Health Insurance Portability and Accountability Act
HSPD	Homeland Security Presidential Directive
IA	Information Assurance
ICS	Industrial Control System
ICS-CERT	Industrial Control Systems Cyber Emergency Response Team
IEC	International Electrotechnical Commission
IP	Internet Protocol
IT	Information Technology
IT-ISAC	Information Technology Information Sharing and Analysis Center
ISO	International Organization for Standardization
MOA	Memoranda of Agreement
MOU	Memoranda of Understanding
NERC	North American Electric Reliability Corporation
NIST	National Institute of Standards and Technology
NRC	Nuclear Regulatory Commission
NRECA	National Rural Electric Cooperative Association
OCTAVE	Operationally Critical Threat, Asset, and Vulnerability Evaluation

OSHA	Occupational Safety and Health Administration
PCI-DSS	Payment Card Industry Data Security Standard
PKI	Public Key Infrastructure
PRA	Probabilistic Risk Assessment
RAM-E	Risk Assessment Methodology for Energy Infrastructures
RMP	Risk Management Process
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SEI	Software Engineering Institute
SOX	Sarbanes–Oxley Act
SP	Special Publication
SQUARE	Security Quality Requirements Engineering
TCP	Transmission Control Protocol
U.S.	United States
US-CERT	United States Computer Emergency Readiness Team
VPN	Virtual Private Network

2156

APPENDIX D

ROLES AND RESPONSIBILITIES

KEY PARTICIPANTS IN THE RMP

The following sections describe the roles and responsibilities of key participants involved in an organization's RMP.[45] Recognizing that organizations have widely varying missions and organizational structures, there may be differences in naming conventions for risk management-related roles and how specific responsibilities are allocated among organizational personnel (e.g., multiple individuals filling a single role or one individual filling multiple roles).[46] However, the basic functions remain the same. The application of the RMP across the three risk management tiers described in this publication is flexible, allowing organizations to effectively accomplish the intent of the specific tasks within their respective organizational structures to best manage risk.

RISK EXECUTIVE

The *risk executive* is a functional role (individual or group) established within organizations to provide a more comprehensive, organization-wide approach to risk management. The risk executive serves as the common risk management resource and 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;
- Ensure that acceptance of the cybersecurity plan considers all factors necessary for mission and business success; and
- Ensure shared responsibility for supporting organizational missions and business functions through the use of external providers, receives an appropriate level of visibility and deliberation..

CHIEF INFORMATION OFFICER

The *chief information officer (CIO)* is an organizational official responsible for (i) designating a chief information security officer; (ii) developing and maintaining cybersecurity policies, procedures, and

[45] Organizations may define other roles (e.g., facilities manager, human resources manager, systems administrator) to support the risk management process.

[46] Caution is exercised when one individual fills multiples roles in the risk management process to ensure that the individual retains an appropriate level of independence and remains free from conflicts of interest.

control techniques to address all applicable requirements; (iii) overseeing personnel with significant responsibilities for cybersecurity and ensuring that the personnel are adequately trained; (iv) assisting senior organizational officials concerning their security responsibilities; and (v) coordinating with other senior officials.

INFORMATION OWNER

The *information owner* is an organizational official with statutory, management, or operational authority for specified information and with the responsibility for establishing the policies and procedures governing the generation, collection, processing, dissemination, and disposal of specified information. In information-sharing environments, the information owner is responsible for establishing the rules for appropriate use and protection of the subject information (e.g., rules of behavior) and retains that responsibility when the information is shared with or provided to other organizations. The owner of the information processed, stored, or transmitted by an IT and ICS may or may not be the same as the IT and ICS owner. Information owners provide input to IT and ICS owners regarding the cybersecurity requirements and controls for the systems where the information is processed, stored, or transmitted.

CHIEF INFORMATION SECURITY OFFICER

The *chief information security officer* is an organizational official responsible for serving as the primary liaison for the CIO to the IT and ICS owners, common control providers, and information system security officers. The chief information security officer (i) possesses professional qualifications, including training and experience, required to administer the cybersecurity program functions; (ii) maintains cybersecurity duties as a primary responsibility; and (iii) heads an office with the mission and resources to assist the organization in achieving more secure information and IT and ICS. The chief information security officer or supporting staff members may also serve as authorizing official designated representatives or security control assessors.

IT and ICS OWNER(s)

The *IT and ICS owner(s)* is responsible for the procurement, development, integration, modification, operation, maintenance, and disposal of an IT and ICS. The IT and ICS owner(s) is also responsible for addressing the operational interests of the user community (i.e., individuals who depend upon the IT and ICS to satisfy mission, business, or operational requirements) with cybersecurity requirements.

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 IT and ICS 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 IT and ICS 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 IT and ICS that meet the stated security requirements.

APPENDIX E

GOVERNANCE MODELS

APPROACHES TO CYBERSECURITY GOVERNANCE

Governance in the Electricity Sector can take many forms. Three approaches to cybersecurity governance can be used to meet organizational needs: (i) a *centralized* approach, (ii) a *decentralized* approach, or (iii) a *hybrid* approach. The authority, responsibility, and Decision making power related to cybersecurity and risk management differ in each governance approach. The appropriate governance structure for an organization varies based on many factors (e.g., mission and business functions, size of the organization, organizational operations, resources, and risk tolerance).

Centralized Governance

In centralized governance structures, the authority, responsibility, and decision making power are vested solely within a central body. The centralized body establishes the policies, procedures, and processes for ensuring an organization-wide involvement in the development and implementation of risk management and cybersecurity strategies, risk, and cybersecurity decisions, as well as in the creation of internal and external communication mechanisms. A centralized approach to governance requires strong, well-informed central leadership and provides consistency throughout the organization. Centralized governance structures also provide less autonomy for subordinate organizations that are part of the parent organization.

Decentralized Governance

In decentralized cybersecurity governance structures, the authority, responsibility, and decision making power are vested in and delegated to individual subordinate organizations within the parent organization (e.g., business units). Subordinate organizations establish their own policies, procedures, and processes for ensuring the development and implementation of risk management and cybersecurity strategies, decisions, and mechanisms to communicate across the organization. A decentralized approach to cybersecurity governance accommodates subordinate organizations with divergent mission and business needs and operating environments. The effectiveness of this approach is greatly increased by the sharing of risk-related information among subordinate organizations so that no subordinate organization is able to transfer risk to another without the latter's informed consent. It is also important to share risk-related information with parent organizations, as the risk decisions by subordinate organizations may have an effect on the organization as a whole.

Hybrid Governance

In hybrid cybersecurity governance structures, the authority, responsibility, and decision making power are distributed between the parent and the subordinate organizations. The central body establishes the policies, procedures, and processes for ensuring organization-wide involvement in the portion of the risk management and cybersecurity strategies and decisions affecting the entire organization (e.g., decisions related to shared infrastructure or common security services). Subordinate organizations, in a similar manner, establish appropriate policies, procedures, and processes for ensuring their involvement in the portion of the risk management and cybersecurity strategies and decisions that are specific to their mission and business needs and environments of operation. A hybrid approach to governance requires strong, well-informed leadership for the organization as a whole and for subordinate organizations, and provides consistency throughout the organization for those aspects of risk and cybersecurity that affect the entire organization.

APPENDIX F

TRUST MODELS

APPROACHES TO ESTABLISHING TRUST RELATIONSHIPS

The following trust models describe ways in which organizations in the Electricity Sector can obtain the levels of trust needed to form partnerships internal and external to the organization, collaborate with other organizations, and share or receive information. No single trust model is inherently better than any other model. Rather, each model provides organizations with certain advantages and disadvantages on the basis of their circumstances (e.g., governance structure, risk tolerance, and criticality of organizational mission and business processes).

Validated Trust

In the *validated trust model*, one organization obtains information regarding the actions of another organization (e.g., the organization's cybersecurity policies, activities, and risk-related decisions) and uses the information to establish a level of trust with other organizations. An example of validated trust is when one organization develops an IT and ICS application and provides evidence (e.g., security plan, assessment results) that the application meets certain security requirements. The evidence offered may not fully satisfy the trust requirements or expectations. Additional evidence may be needed between organizations to establish trust. Trust is linked to the degree of transparency between two organizations with regard to risk and cybersecurity-related activities and decisions.

Historical Trust

In the *historical trust model*, the track record exhibited by an organization in the past, particularly in its risk and cybersecurity-related activities and decisions, can contribute to and help establish a level of trust with other organizations. While validated trust models assume that an organization provides the required level of proof needed to establish trust, obtaining such proof may not always be possible. In such instances, trust may be based on other deciding factors, including the organization's historical relationship with other organizations or its recent experience in working with the other organizations. For example, if one organization has worked with a second organization for years doing some activity and has not had any negative experiences, the first organization may be willing to trust the second organization in working on another activity, even though the organizations do not share any common experience for that particular activity. Historical trust tends to build up over time, with the more positive experiences contributing to increased levels of trust between organizations. Conversely, negative experiences may cause trust levels to decrease among organizations.

Third-Party Trust

In the *third-party trust model*, an organization establishes a level of trust with another organization on the basis of assurances provided by a mutually trusted third party. For example, two organizations attempting to establish a trust relationship may not have a direct trust history between them but do have a trust relationship with a third organization. The third party, which is trusted by both organizations, brokers the trust relationship between the two organizations, thus helping to establish the required level of trust, also known as transitive trust.

Mandated Trust

In the *mandated trust model*, an organization establishes a level of trust with another organization on the basis of a specific mandate issued by a third party in a position of authority. This mandate can be established by the respective authority through legislation, directives, regulations, or policies (e.g., a policy from an organization directing that all subordinate components of the organization accept the results of security assessments conducted by any subordinate components of the organization). Mandated trust can also be established when an organization is decreed to be the authoritative source for the

provision of information resources, including IT products, systems, or services. For example, an organization may be given the responsibility and the authority to issue Public Key Infrastructure (PKI) certificates for a group of organizations.

Hybrid Trust

In general, the trust models described above are not mutually exclusive. Each of the trust models may be used independently, as a stand-alone model, or in conjunction with another model. Several trust models may be used at times within the organization. Since Electricity Sector organizations are diverse, it is possible that subordinate organizations may employ different trust models in establishing relationships with potential partnering organizations. The organizational governance structure may establish the specific terms and conditions for how the various trust models are employed in a complementary manner within the organization.

APPENDIX G
RISK RESPONSE STRATEGIES

Organizations develop risk mitigation strategies based on strategic goals and objectives, mission and business requirements, and organizational priorities. These strategies provide the basis for making risk-based decisions for acceptance on the security solutions associated with and applied to IT and ICS within the organization. Risk mitigation strategies are necessary to ensure that organizations are adequately protected against the growing threats to information processed, stored, and transmitted by organizational IT and ICS. The nature of the threats and the dynamic environments in which organizations operate, demand flexible and scalable defenses, as well as solutions that can be tailored to meet rapidly changing conditions. These conditions include, for example, the emergence of new threats and vulnerabilities, the development of new technologies, changes in missions/business requirements, and/or changes to environments of operation. Effective risk mitigation strategies support the goals and objectives of organizations, and established mission and business priorities are tightly coupled with enterprise architectures and cybersecurity architectures.

Organizational risk mitigation strategies reflect the following:

- Mission and business processes are designed with regard to cybersecurity requirements;[47]
- Enterprise architectures (including information security architectures) are designed with consideration for realistically achievable risk mitigations;
- Risk mitigation measures are implemented within organizational IT and ICS and their environments of operation by safeguards/countermeasure (i.e., security controls) consistent with cybersecurity architectures; and
- Cybersecurity programs, processes, and safeguards/countermeasures are highly flexible and agile with regard to implementation, recognizing the diversity in organizational mission and business functions, the variations in IT and ICS implementations and capabilities, and the dynamic environments in which the organizations operate.[48]

Traditional risk mitigation strategies, with regard to threats from cyber attacks, at first relied almost exclusively on monolithic boundary protection. These strategies assumed adversaries were outside of some established defensive perimeter, and the objective of organizations was to repel the attack. The primary focus of static boundary protection was penetration resistance of the IT products and systems employed by the organization, as well as any additional safeguards and countermeasures implemented in the environments in which the products and systems operated. Recognition that IT and ICS boundaries were permeable, or porous, led to defense-in-depth as part of the mitigation strategy, relying on detection and response mechanisms to address the threats within the protection perimeter. In today's world characterized by advanced persistent threats (APTs),[49] a more comprehensive risk mitigation strategy is needed—a strategy that combines traditional boundary protection with agile defense.

[47] In addition to mission- and business-driven information protection needs, cybersecurity requirements are obtained from a variety of sources (e.g., federal legislation, policies, regulations, standards, and corporate organizational policies).

[48] Dynamic environments of operation are characterized, for example, by ongoing changes in people, processes, technologies, physical infrastructure, and threats.

[49] An *advanced persistent threat (APT)* is an adversary that possesses sophisticated levels of expertise and significant resources that allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and deception). These objectives typically include establishing/extending footholds within the IT and ICS infrastructure of the targeted organizations for the purposes of exfiltrating information; undermining or impeding critical aspects of a mission, program, or organization; or positioning itself to carry out these objectives in the future. The APT (i) pursues its objectives repeatedly over an extended period of time, (ii) adapts to defenders' efforts to resist it, and (iii) is determined to maintain the level of interaction needed to execute its objectives.

Agile defense assumes that a small percentage of threats from purposeful cyber attacks will be successful by compromising organizational IT and ICS through the supply chain,[50] by defeating the initial safeguards and countermeasures (i.e., security controls) implemented by organizations, or by exploiting previously unidentified vulnerabilities for which protections are not in place or are inadequate. In this scenario, adversaries are operating inside the defensive perimeters established by organizations and may have substantial or complete control of organizational IT and ICS. Agile defense employs the concept of *information system resilience*—that is, the ability of systems to operate while under attack, even in a degraded or debilitated state, and to rapidly recover operational capabilities for essential functions after a successful attack. The concept of information system resilience can also be applied to the other classes of threats, including threats from environmental disruptions and/or human errors of omission/commission. The most effective risk mitigation strategies employ a combination of boundary protection and agile defenses, depending on the characteristics of the threat.[51] This dual protection strategy illustrates two important cybersecurity concepts known as defense-in-depth[52]and defense-in-breadth.[53]

The IT and ICS needed for mission and business success may be the same technologies through which threat actors cause mission and business failure. The risk response strategies developed and implemented by organizations may consider the type of IT and ICS and their functions and capabilities. Clearly defined and articulated risk response strategies help to ensure that senior executives take ownership and are ultimately responsible and accountable for risk decisions.

The purpose of risk response is to provide a consistent, organization-wide response by (i) developing alternative courses of action for responding to risk, (ii) evaluating the alternative courses of action, (iii) determining appropriate courses of action consistent with organizational risk tolerance, and (iv) implementing risk responses that are based on selected courses of action. There are five basic types of responses to risk: (i) accept, (ii) avoid, (iii) mitigate, (iv) share, and (v) transfer. While each type of response can have an associated strategy, there may be an overall strategy for selecting from among the basic response types. This overall risk response strategy and the strategy for each type of response are discussed below. In addition, specific risk mitigation strategies are presented, including a description of how such strategies can be implemented within organizations.

OVERALL RISK RESPONSE STRATEGIES

A decision to *accept* risk must be consistent with the stated organizational tolerance for risk. Yet, there is still need for a well-defined, established organizational process for selecting one or a combination of the risk responses of acceptance, avoidance, mitigation, sharing, or transfer. Organizations are often placed in situations in which there is greater risk than the designated senior executives desire to accept. Each of the risk responses are based on the organization's statement of risk tolerance at each tier. The objective of establishing a statement of risk tolerance is to identify, in clear and unambiguous terms, a limit for risk; that is, how far senior executives are willing to go with regard to accepting risk to organizational operations, resources, and other organizations.

[50] Draft NIST Interagency Report 7622 provides guidance on managing supply chain risk.

[51] Threat characteristics include capabilities, intentions, and targeting information.

[52] *Defense-in-depth* is a cybersecurity strategy integrating people, technology, and operations capabilities to establish variable barriers across multiple layers and missions of the organization.

[53] *Defense-in-breadth* is a planned, systematic set of multidisciplinary activities that seek to identify, manage, and reduce risk of exploitable vulnerabilities at every stage of the system, network, or subcomponent life cycle (system, network, or product design and development; manufacturing; packaging; assembly; system integration; distribution; operations; maintenance; and retirement).

RISK ACCEPTANCE STRATEGIES

Organizational risk acceptance strategies are essential companions to organizational statements of risk tolerance. Real-world operations, however, are seldom so simple as to make such risk tolerance statements the end statement for risk acceptance decisions. Risk acceptance includes the impact(s) resulting from the implementation of avoidance, sharing, transference, and/or mitigation response strategies. Organizational risk acceptance strategies place the acceptance of risk into a framework of organizational perspectives on dealing with the practical realities of operating with risk and provide the guidance necessary to ensure that the extent of the risk being accepted in specific situations is compliant with organizational direction. Inherent in the risk acceptance strategy is the identification of risk monitoring triggers to provide reasonable assurance that the risk accepted remains at or below the risk acceptance strategy.

RISK AVOIDANCE STRATEGIES

Risk avoidance entails restructuring processes or systems, or ending activities to eliminate potential exposure.

RISK SHARING AND TRANSFER STRATEGIES

Organizational risk sharing strategies and risk transfer strategies enable risk decisions for specific organizational missions and business functions through policies, contracts, and agreements. Risk sharing and transfer strategies both consider and take full advantage of a lessening of risk by sharing or transferring the potential impact across internal or external organizations. Transferring risk involves delegating full responsibility or accountability; sharing risk involves delegating only partial responsibility or accountability.

RISK MITIGATION STRATEGIES

Organizational risk mitigation strategies reflect an organizational perspective on what mitigations are employed and where the mitigations are applied to reduce risks to organizational operations and resources and to other organizations. Risk mitigation strategies are the primary link between organizational risk management programs and cybersecurity programs—with the former covering all aspects of managing risk and the latter being primarily a part of the risk response component of the RMP. Effective risk mitigation strategies consider the general placement and allocation of mitigations, the degree of intended mitigation, and cover mitigations at each tier.

Information has value and must be protected. Information systems (including people, processes, and technologies) are the primary vehicles employed to process, store, and transmit such information—allowing organizations to carry out their missions in a variety of environments of operation and to ultimately be successful.