DOE/OE-0003

ELECTRICITY SUBSECTOR CYBERSECURITY
RISK MANAGEMENT PROCESS

U.S. Department of Energy

May 2012

Acknowledgments

This electricity subsector cybersecurity 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 and utility-specific trade groups were included in authoring this guidance designed to be meaningful and tailored for the electricity sector. The primary goal of this guideline is to describe an RMP that is tuned to the specific needs of electricity subsector 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 cybersecurity standards further refine the definition and application of effective cybersecurity for all organizations in the electricity subsector. The NERC Critical Infrastructure Protection (CIP) cybersecurity standards are developed by a separate industry drafting team and are adopted through an industry balloting process that is not governed by the risk management guideline. While it is anticipated that entities subject to compliance with NERC CIP cybersecurity standards would use this guideline, compliance requirements are not altered in anyway by this guideline. Please consult your NERC CIP compliance authority for any questions on NERC CIP compliance.

DOE wishes to acknowledge and thank the senior leaders from 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, core development team, and subject matter expert team, 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

Charles H. Romine
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

Brian M. Harrell
Manager of Security Standards, Training, and Awareness

Risk Management Process Core Development Team

Andy Bochman
IBM

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

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

Fowad Muneer
ICF International

David Norton
Federal Energy Regulatory Commission

Scott Saunders
Sacramento Municipality Utility District

Anthony David Scott
Accenture

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 Pillitteri
Booz Allen Hamilton

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 Co., Inc.

Felix Kwamena
Natural Resources Canada

Scott Mix
North American Electric Reliability Corporation

Brian Evans-Mongeon
Utility Services, Inc.

Reynaldo De Leon
Southern California Edison

James W. Sample
Pacific Gas & Electric Company

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 subsector 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

CONTENTS

CONTENTS

List of Figures

List of Tables

1. Introduction

The electricity subsector[1] cybersecurity Risk Management Process (RMP) guideline has been developed by a team of government and industry representatives to provide a consistent and repeatable approach to managing cybersecurity risk across the electricity subsector. It is intended to be used by the electricity subsector, to include organizations responsible for the generation, transmission, distribution, and marketing of electric power, as well as supporting organizations such as vendors. The RMP is written with the goal of enabling organizations—regardless of size or organizational or governance structure—to apply effective and efficient risk management processes and tailor them to meet their organizational requirements. This guideline may be used to implement a new cybersecurity program within an organization or to build upon an organization's existing internal cybersecurity policies, standard guidelines, and procedures.

The authors recognize that risk management processes in an organization are not executed in a vacuum. Regulatory requirements already exist to include North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards, Nuclear Regulatory Commission (NRC) requirements, and a host of other Federal and State requirements. These requirements serve an important role in ensuring reliability, resilience, public safety, individual privacy, and protection of critical infrastructure. Within the RMP, these requirements are treated as inputs to the process and shape the risk management decisions made by an organization. Implementation of the RMP will provide organizations with greater agility in responding to new regulations or changes to existing regulatory requirements, allowing an organization to quickly identify the impact of new requirements and adjust their cybersecurity posture accordingly.

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. Whether caused willingly or unknowingly, damage to electricity subsector cyber systems can have a direct effect on the economic and national security interests of all nations.

[1] Homeland Security Presidential Directive 7 (HSPD-7) identifies Energy as one of the 17 critical infrastructure sectors of the Nation. Electricity is one of two subsectors. Oil and Natural Gas are treated as one.

INTRODUCTION

Cybersecurity risk is one of the components of the overall business risk environment and feeds into an organization's enterprise Risk Management Strategy and program. Cybersecurity risk, as with all risks, cannot be completely eliminated, but instead must be managed through informed decision making processes. The RMP is built on the premise that managing cybersecurity risk[2] is critical to the success of an organization's mission in achieving its business's goals and objectives, specifically the reliable generation and delivery of electric power. Implementation of the RMP will facilitate more informed decision making throughout an organization leading to more effective resource allocation, operational efficiencies, and the ability to mitigate and rapidly respond to cybersecurity risk. The goal is to reduce the likelihood and impact of a cyber event to an organization's operations, assets, and individuals. Implementation of the RMP across the electricity subsector will result in a common approach to managing cybersecurity risk, facilitating improved information exchange among organizations, between other stakeholders to include private sector and State and Federal agencies, and across international boundaries (Canada and Mexico). This will result in an improved dialogue that recognizes the need to manage this risk through an ongoing process to achieve the common goal of generating and delivering electric power.

Over the past few decades, the electricity subsector has become increasingly dependent on digital technology to reduce costs, increase efficiency, and maintain reliable operations. Information technology[3] (IT) and industrial control systems[4] (ICS) are vulnerable to malicious attacks and misuse. ICS are now being integrated with traditional business IT that provides corporate services (e.g., network, email). Data produced in the operation of ICS are increasingly used to support business decisions. 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 platforms and software applications, interconnected public and private networks, and remote support are moving organizations from an isolated environment into a global, interconnected environment. Technologies that drive the emerging smart grid will further integrate IT energy management systems, ICS, and business systems.

> The highly publicized Stuxnet worm is an example of how vulnerabilities within IT systems can be used to reach into ICS (in this case, a programmable logic controller). Stuxnet blends social engineering, use of Universal Serial Bus (USB) drives, COTS vulnerabilities, and ICS application vulnerabilities to compromise a physical control device.

[2] 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, standards, guidelines, procedures, and structures within organizations that influence or affect the design, development, implementation, and ongoing operation of IT and ICS.

[3] IT is a discrete system 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).

[4] An ICS is a general term that encompasses several types of control systems, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system configurations such as skid-mounted Programmable Logic Controllers (PLC) often found in the industrial sectors and critical infrastructures. Operations Technology (OT) is an emerging term within industry used to describe hardware and software systems used to operate industrial control devices. For purposes of this document the term ICS will be used though some organizations may use the term OT.

All IT and ICS have vulnerabilities that are subject to threats and 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 increasing number of vulnerabilities as well as the interconnectedness of systems could serve as a blueprint for attackers who wish to access Intelligent Electronic Devices (IED) (e.g., controllers, relays, reclosers), safety systems, critical decision data, support systems, and physical and cybersecurity systems. This can cause damage to an electricity subsector organization's assets or harm to individuals, and can even compromise the reliable delivery of electricity.

Today's mission and business needs are reducing separation between ICS and business and administrative networks, resulting in increased vulnerabilities. This guideline provides a process that organizations can implement to manage the increased risks that these new technologies are introducing into the electricity subsector.

To successfully execute organizational mission and business functions in the electricity subsector, using IT and ICS processes, an organization's leadership function 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 an efficient, effective, and sustained mission for business objectives across all electricity subsector organizations.

[5] For additional information on threat sources, see US-CERT Cyber Threat Source Descriptions at http://www.us-cert.gov/control_systems/csthreats.html.

2. Cybersecurity Risk Management Overview

Electricity subsector organizations deal with risk every day in meeting their business objectives. They may include financial risk, risk of failure of equipment, and personnel safety risk, to name just a few. These organizations have developed processes to evaluate risks associated with their business and to choose how to deal with those risks based on organizational priorities and both internal and external constraints. This management of risk is conducted as an interactive, ongoing process as part of normal operations. To this end, these organizations may have developed enterprise risk management processes and strategies to define how they will address both inherent and residual risk in accomplishing their missions. While recognizing the larger context of risk management within an organization, this document has been written to provide a consistent and scalable risk management process specific to the risks inherent in operating IT and ICS. For purposes of this document, the term, risk management, refers to the program and supporting processes used to manage cybersecurity risk to an organization's operations, its assets, and individuals.[6]

Everyone in the organization is responsible for cybersecurity, but regardless of the size or type of the organization, executive leadership/governing boards are responsible for how cybersecurity risk impacts the organization's mission and business processes. In developing a governance structure, the organization establishes a risk executive function responsible for the organization-wide strategy to address risks, establishing accountability. The risk executive is a functional role that provides a more comprehensive, organization-wide approach to risk management. This function could exist as a collection of executive managers, board of directors, or committee of a cooperative organization. The function serves as the common enterprise risk management resource for senior leaders or executives, mission and business process 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. In implementing the RMP, organizations have flexibility to determine how best to conduct the activities, including the sequence, degree of rigor, formality, and how the results or outputs of each activity are captured and shared across the organization and between organizations.

Electricity subsector 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 incorporate cybersecurity risk management within the existing structure. 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. The RMP described in this document is meant to supplement an organization's existing risk management framework and provide flexible guidelines that may be leveraged as needed. If the organization does not have

[6] Adapted from National Information Assurance Glossary, Committee on National Security Systems (CNSS) 4009.

an existing risk management framework, then the RMP described in this document may be used as a standalone framework.

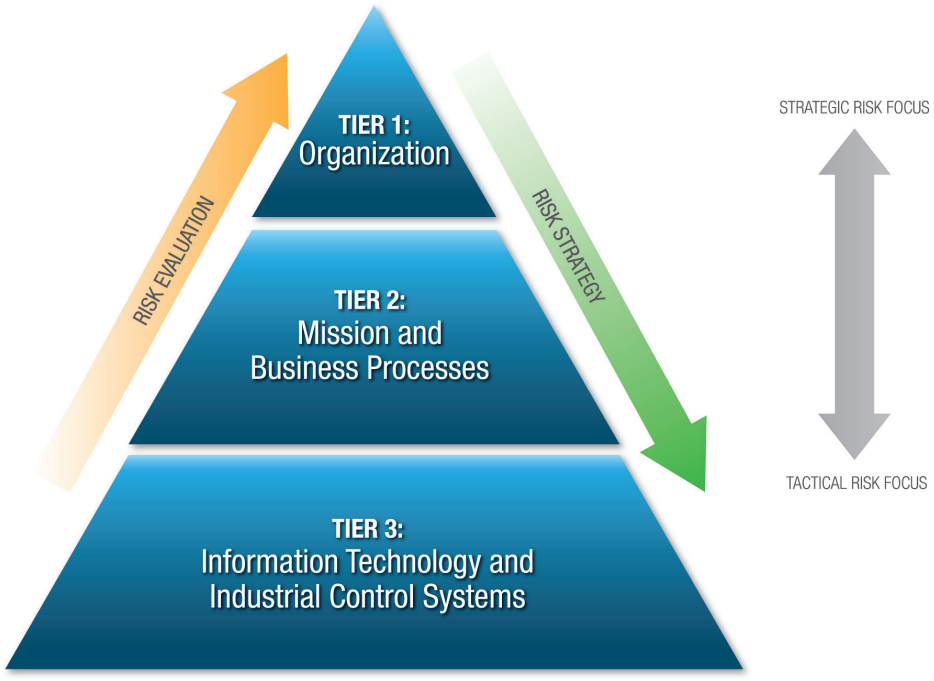
2.1 RISK MANAGEMENT MODEL

The risk management model[7] presented in this document uses a three-tiered structure to provide a comprehensive view of an electricity subsector organization. This structure can be applied to any organization regardless of size or operations. The three tiers of the risk management model are:

- Tier 1: Organization;
- Tier 2: Mission and Business Processes; and
- Tier 3: Information Technology and Industrial Control Systems.

This model represents an electricity subsector organization's strategic focus in Tier 1, the mission and business processes focus in Tier 2, and tactical focus in Tier 3. Figure 1 illustrates the tiered risk management model.

Figure 1: Risk Management Model



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

2.1.1 Tier 1: Organization

Tier 1 addresses risk from an organizational perspective by establishing and implementing a governance structure consistent with the strategic goals and objectives of the electricity subsector organization. Governance[8] structures provide direction and oversight for risk management activities conducted by an organization. The risk management decisions at Tier 1 are inputs to the activities carried out at Tier 2 and Tier 3. The Tier 1 risk management activities may include:

- Establishing and implementing a structure for risk management and governance;
- Identifying and prioritizing mission and business processes with respect to strategic goals and objectives;
- Establishing the recovery order for critical mission and business processes;
- Establishing the organization's risk tolerance;
- Defining techniques and methodologies for assessing cybersecurity risk;
- Defining risk management constraints and requirements; and
- Establishing the organization's cybersecurity Risk Management Strategy.[9]

2.1.2 Tier 2: Mission and Business Processes

Tier 2 addresses risk from a mission and business process perspective. This tier informs and is informed by the IT and ICS technical architecture. Tier 2 activities are inputs to activities in Tier 3, and provide feedback to Tier 1. Generally, operational management is involved at this tier. However, in some organizations, the executive management may perform some of the tier functions. Cybersecurity risk management at this level focuses on the execution of specific mission and business processes. The risk management activities for Tier 2 may include:

- Identifying and prioritizing assets necessary to support the mission and business processes of an organization defined in Tier 1;
- Identifying cybersecurity processes needed to successfully execute mission and business processes;
- Mapping cybersecurity requirements[10] against mission and business processes;
- Developing a disciplined and structured approach for managing IT and ICS assets that support 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.

[8] Additional information about governance models can be found in Appendix D, Governance Models.

[9] The cybersecurity Risk Management Strategy is a component within an organization's enterprise Risk Management Strategy. The enterprise Risk Management Strategy may consist of risk strategy components, such as 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.

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

2.1.3 Tier 3: Information Technology and Industrial Control Systems

Tier 3 addresses system risk from an IT and ICS perspective. It 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 IT and ICS in accordance with the cybersecurity architecture[11] developed by the organization. Activities at this level provide feedback to Tier 2 and Tier 1 on the organization's risk posture. Tier 3 risk management activities may include:

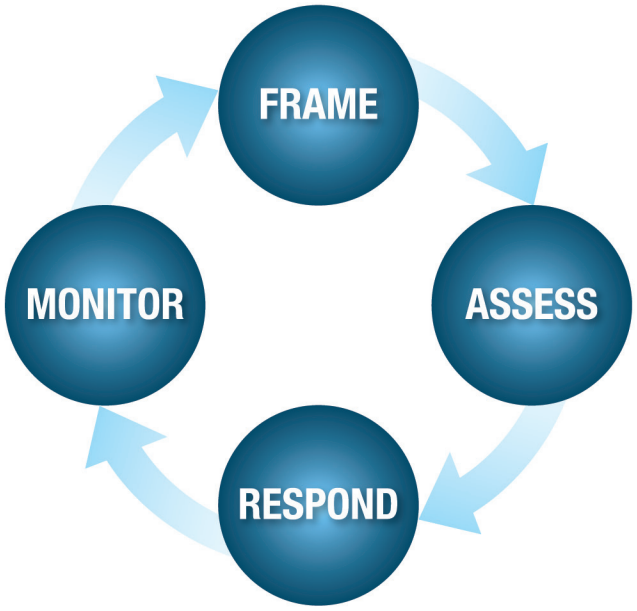
- Categorizing IT and ICS into levels by risk and value to mission and business processes;
- Allocating cybersecurity controls to systems and the environments in which they operate;
- Managing the selection, implementation, assessment, and monitoring of cybersecurity controls; and
- Establishing a process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

2.2 RISK MANAGEMENT CYCLE

The risk management cycle is an iterative and continuous process, constantly reinformed 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 Figure 2:

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

Figure 2: Risk Management Cycle



[11] 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.

The risk management cycle is a comprehensive process that requires organizations to (1) frame risk (i.e., establish the context for risk-based decisions), (2) assess risk, (3) respond to risk once determined, and (4) monitor risk on an ongoing basis, using effective organizational communications and an iterative 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 output of the risk management process is a strategy addressing how an electricity subsector organization intends to frame, assess, respond to, and monitor risk. The strategy makes explicit and transparent the risk perceptions that an organization in the electricity subsector routinely uses to make investment and operational decisions. The following sections briefly describe each of the four risk management components.

2.2.1 Risk Framing

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 subsector, identify:

- Assumptions about threats, vulnerabilities, impacts, and likelihood of occurrence;
- Constraints imposed by legislation, regulation, resource constraints (time, money, and people) and other factors identified by the organization;
- Risk tolerance, which identifies the level of acceptable risk;
- Priorities within mission and business processes, and trade-offs between different types of risk; and
- Trust relationships, such as physical interconnections, third-party service providers, reciprocity agreements, or device vendors.[12]

Risk framing includes 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.

[12] 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 about ways in which organizations can obtain levels of trust can be found in Appendix E, Trust Models.

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 subsector organizations. The purpose of the risk assessment element is for organizations to identify the following components of risk and evaluate these against mission and business processes:

- Threats;
- Vulnerabilities;
- Impact (consequence or opportunity); and
- Likelihood (probability or frequency an event will occur).

Identifying cyber threats and vulnerabilities is not confined to review of IT and ICSs. Governance structures, mission and business processes, enterprise and cybersecurity architectures, facilities, equipment, supply chain activities, and external service providers, etc. are all considered during the risk assessment. 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[13] 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 subsector organization responds to risk once that risk is assessed. The risk response element provides a consistent, organization-wide response to risk consistent with the organization's risk exposure. In this element, organizations:

- 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.

The output of the risk response element informs 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.

[13] Additional information about the responsibilities of organizational officials can be found in Appendix F, Roles and Responsibilities.

It may be determined through a cost-benefit analysis that during the risk response element certain response actions are not feasible to implement, are cost prohibitive, or are not relevant to electricity subsector operations. This may require implementation of compensating controls[14] to manage the risk in an acceptable way and meet the cybersecurity requirements. The risk response element is the point where organizations make choices on how best to deal with that risk.

2.2.4 Risk Monitoring

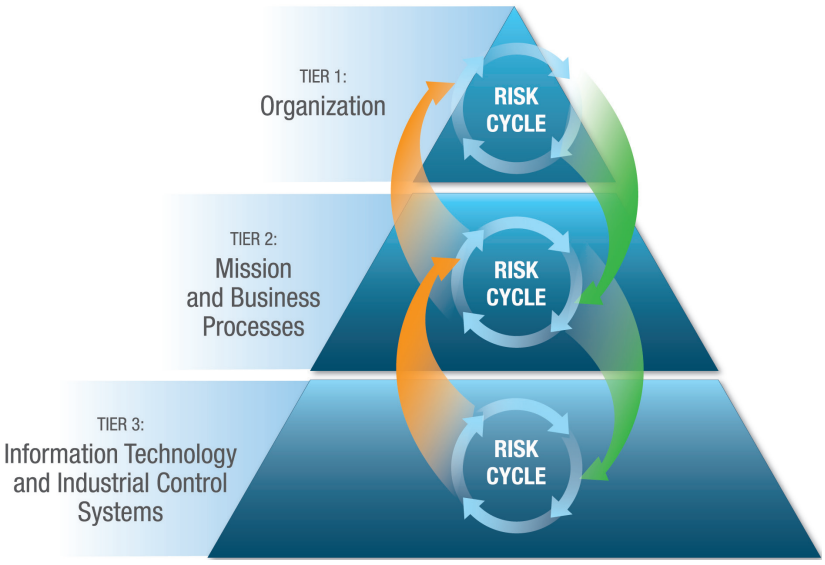
The risk monitoring element addresses how risks are monitored and communicated over time in an electricity subsector organization. During the risk monitoring element, organizations:

- Verify that risk response measures are implemented and that the cybersecurity requirements derived from the Risk Management Strategy are satisfied;
- Evaluate the ongoing effectiveness of risk response measures;
- Identify changes that may impact risk to an organization's IT and ICS and the operational environments;[15] and
- Define 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 develop a culture of cybersecurity at all levels of an organization. To facilitate these goals, further sections of this document will elaborate on the activities and outputs recommended to focus leaders, managers, security, and IT and ICS personnel on the practices of a strong risk program. The

Figure 3: Risk Management Process



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

[15] Operational environments include but are not limited to threats; vulnerabilities; 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.

outputs (often documents) will help to promote communications among stakeholders, maintain focus on cybersecurity risk, 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) promote a culture of security and improve risk communications.

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) exist in all electricity subsector organizations. These functions may be conducted by a single individual, committee, division, or any other organizational structure.

As Figure 4 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. General descriptions of the risk management cycle outputs at each tier are illustrated in Table 1. The RMP is a flexible process that allows organizations to implement it as appropriate to their organization. What is important is that all three tiers are engaged in the process. The sequencing and timing of the various activities will vary depending on the organization's structure, culture, and other factors.

Figure 4: RMP Information Flowchart

Table 1: Risk Management Process Overview

	TIER 1	TIER 2	TIER 3
RISK FRAMING	**Section 3.1** Produce a set of organizational policies, governance structure, and guidance that form the basis for the Risk Management Strategy	**Section 4.1** Establish risk assessment methodology and define the cybersecurity components of the enterprise architecture	**Section 5.1** Develop the cybersecurity plan that identifies the components, systems, hardware, and software of the IT and ICS
RISK ASSESSMENT	**Section 3.2** Determine risk to an organization's operations	**Section 4.2** Develop prioritized list of mission and business processes	**Section 5.2** Conduct risk assessment and develop cybersecurity risk assessment report
RISK RESPONSE	**Section 3.3** Decide on the appropriate courses of action to accept, avoid, mitigate, share, or transfer risk.	**Section 4.3** Using the prioritized list of processes, establish cybersecurity program and architecture	**Section 5.3** Develop and implement risk mitigation plan
RISK MONITORING	**Section 3.4** Determine the ongoing effectiveness of risk response measures	**Section 4.4** Measure the effectiveness of and level of conformance with the cybersecurity architecture	**Section 5.4** Monitor changes and measure effectiveness of cybersecurity controls

Table 1 above provides an overview of the entire risk management process and can be used as a resource for organizations implementing the RMP. Each cell summarizes the significant activities of the risk cycle across each tier.

The RMP defines and promotes a common understanding of risk tolerance and policy and communicates it across the organization. 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 facilitates a bottom-up communication of resource needs and implementation challenges.

3. Tier 1: Electricity Subsector Organization

The RMP at Tier 1 produces an initial cybersecurity risk management strategy (if one does not already exist) that includes a risk assessment methodology, a risk monitoring strategy, and a cybersecurity governance program. This strategy is iteratively informed and revised based on outputs from Tiers 2 and 3. 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, risk tolerance, priorities, and goals of addressing cybersecurity risks. Generally, at Tier 1, organizations identify and prioritize mission and business processes. The mission and business processes owners and IT and ICS managers use the Cybersecurity Risk Management Strategy to allocate resources in a prioritized manner and also provide feedback to senior management on the effectiveness of the risk management program. The executive leadership uses institution of a governance program to provide focused and structured oversight and systematic review of the RMP.

3.1 RISK FRAMING AT TIER 1

Risk framing establishes the context and provides a common perspective for how an electricity subsector organization manages risk. The risk content and perspective will vary across 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 has millions of 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.

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

	INPUTS	ACTIVITIES	OUTPUTS
RISK FRAMING	▪ Mission and vision statement ▪ Legislation ▪ Organizational policies ▪ Regulatory requirements ▪ Contractual relationships ▪ Financial limitations ▪ Trust relationships ▪ Organizational culture ▪ Governance structures ▪ Output from Tier 1 risk monitoring element ▪ Feedback from Tier 2 risk management cycle	▪ Define risk assumption – Threat sources – Vulnerabilities – Impact – Likelihood ▪ Identify risk management constraint ▪ Determine and implement risk tolerance ▪ Identify priorities ▪ Develop Risk Management Strategy	▪ Risk Management Strategy

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., 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;[16]
- Organizational culture, both internal and external to the organization;
- Governance structures;
- Outputs from the Tier 1 risk monitoring elements;[17] and
- Feedback from the Tier 2 risk management cycle.

[16] Additional information about trust relationships and trust models can be found in Appendix E, Trust Models.

[17] 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.

3.1.2 Activities

3.1.2.1 Define Risk Assumption

Risk assumption activities identify how risk is assessed, responded to, and monitored. As part of the framing element, the organization identifies and describes threat sources, vulnerabilities, impacts, and likelihood. This provides a common terminology and frame of reference throughout the organization for comparing and addressing risks across the disparate environment mission and business process 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.

Threats

Threats can introduce undesirable events with adverse impacts on organizational operations, assets, individuals, and other organizations in the electricity subsector. During the framing element, the organization broadly identifies types of threats to their organization. Threats may include:

- People (e.g., current/former employees, third-party personnel, the public);
- Processes (e.g., missing, deficient, or poorly implemented procedures);
- Technology (e.g., component failure through design, implementation, and/or maintenance);
- External disasters (e.g., natural or man-made); and
- Systemic, recurring cybersecurity incidents.

For all threats determined through the identification of threat sources, electricity subsector organizations should develop a concise description of:

- Types of tactics, techniques, and procedures employed by adversaries;[18]
- Threats mitigated by countermeasures (e.g., controls, safeguards);
- Threats not being addressed by countermeasures (e.g., controls, safeguards);
- Assumptions about threat targeting, intentions, and capabilities; and
- Credible and useful sources of threat information (e.g., electricity subsector Information Sharing and Analysis Center [ES-ISAC] and United States Computer Emergency Readiness Team [US-CERT]).

By identifying and describing threats at Tier 1, 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.

[18] 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 may exploit to cause adverse impacts to IT and ICS in electricity subsector organizations. At Tier 1, vulnerabilities can be associated with deficiencies or weaknesses in organizational governance structures or processes. The vulnerabilities can also be associated with the susceptibility of organizations to adverse issues from external sources (e.g., technology owned or managed by third parties). As part of the risk framing element at Tier 1, the organization may:

- Provide guidance on 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);
- Determine how vulnerability information is shared across the organization, through its governance structure and communication processes;
- Identify sources of credible and useful vulnerability information; and
- Make explicit any assumptions about the degree of organizational, IT, and ICS vulnerability to specific threats.

Impact

Electricity subsector organizations provide guidance on how to assess impacts to operations (i.e., mission disruption, financial loss, image, and reputation), assets, and individuals. At Tier 1, the organization's senior executive leadership identifies which business impacts related to cybersecurity are considered at Tier 2. Additional impacts may be identified by Tiers 2 and 3, iteratively informing the process. A cybersecurity event can have varying impacts on an organization 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 dissatisfied customers, legal and regulatory actions, or impact on reputation brand and corporate value.

Likelihood

An electricity subsector organization can employ a variety of approaches for determining the likelihood of cybersecurity threat events. It may prefer quantitative[19] risk assessments or qualitative[20] risk assessments, as is the case 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, attack trends, and frequencies of attacks), an organization may use empirical data and statistical analysis to determine specific probabilities of threat events occurring. It then selects a method consistent with its organizational culture and risk tolerance. To determine the likelihood of threats exploiting vulnerabilities, electricity subsector organizations can employ a variety of approaches, such as:

- Threat assumptions (e.g., historical data on cyber attacks, earthquakes);
- Threat modeling, such as comparison or perspective methods;
- Actual threat information (e.g., specific information on threat 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.

[19] Quantitative risk is the use of measurable, objective data to determine asset value, probability of loss, and associated risks.
[20] Qualitative risk is the measure of risk or asset value based on rank or separation into categories such as low, moderate, high.

3.1.2.2 Identify Risk Management Constraint

Identification of constraints assists in providing requirements, determining priorities, and in making cost-effective decisions. Some organizations may be compelled to meet strict regulatory requirements (e.g., NERC CIP cybersecurity standards) that limit risk response options, while other organizations may be constrained by resource availability, contractual obligation, culture, or timing. Many IT and ICS assets in the electricity subsector must operate for long periods (possibly decades) 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 to be considered by the organization include:

- Direct financial limitations (e.g., rate case agreements);
- Indirect financial limitations (e.g., financial obligations, debt financing);
- Legal, regulatory, and/or contractual requirements (e.g., divestiture obligations, union contracts);
- Organizational policies (e.g., restrictions on outsourcing);
- Organizational culture, which can impose indirect constraints on governance changes (e.g., precluding a shift from decentralized to hybrid governance structures); and
- Cultural constraints that limit the visibility into and between operational technology support and IT support organizations.

3.1.2.3 Determine and Implement Risk Tolerance

In the electricity subsector, organizations identify and communicate the level of risk tolerance acceptable in meeting their mission and business process objectives. At Tier 1, organizations will define their risk tolerance on the basis of the information developed in the risk framing element. There is no correct level of organizational risk tolerance. Rather, the degree of risk tolerance is (1) generally indicative of organizational culture, (2) potentially different for different types of losses/compromises, and (3) subject to the risk tolerance of executive leadership. The ramifications of risk management decisions that are based on risk tolerance are significant. They can vary between low risk tolerant organizations sacrificing critical business objectives in order to avoid an unacceptable risk and high risk tolerant organizations focusing on near-term business efficiencies at the expense of possible equipment failure.

It is important that the organization 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 risk tolerance. Additionally, risk tolerance is not determined solely by assessment of internal risks. Several external requirements (including regulation) may dictate that some risks cannot be accepted at all or that levels of risk mitigation may be predetermined. The 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.

3.1.3 Outputs

Outputs from the Tier 1 risk framing element produce a set of organizational policies, governance structure, and guidance that form the basis for the Risk Management Strategy and include:

- Scope of the organization's cybersecurity RMP (e.g., organizations covered, mission and business processes affected, how risk management activities are applied at Tier 1);
- 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 management constraints on executing risk management activities; and
- Organizational priorities relating to cybersecurity risk.

Many of 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 includes:

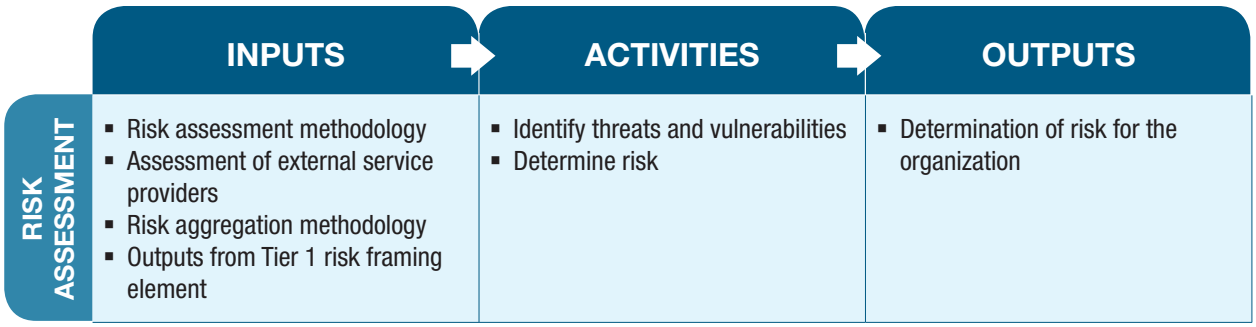
- Prioritizing investment strategies for business units or functions; and
- Establishing a standard risk assessment methodology or provide guidance for consistent implementation of risk assessment across the enterprise.

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

Risk assessments should be treated as a regularly repeated process and not a one-time activity. 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. The frequency of risk assessments is determined by the organization based on a number of variables such as criticality of functions, technological changes, and resource constraints.

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 subsector 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 processes), 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 processes.



3.2.1 Inputs

Inputs to the Tier 1 risk assessment element may include:

- Determining organizationally consistent risk assessment methodologies;[21]
- Determining breadth and depth of analysis employed during risk assessments;
- Defining the level of granularity required for assessing threats and vulnerabilities;
- Deciding whether and/or how to assess external service providers;
- Deciding whether and/or how to aggregate risk assessment results from different organizational entities or mission and business processes organization-wide; and
- Outputs from the risk-framing element in Tier 1.

Organizational expectations on Tier 1 risk assessment methodologies, techniques, and/or procedures are shaped heavily by governance structures, risk tolerance, risk management constraints, priorities, culture, and trust.

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

3.2.2 Activities

3.2.2.1 Identify Threats and Vulnerabilities

A Tier 1 risk assessment focuses on the identification of threats to and vulnerabilities of an organization. Threat analysis requires an examination of threats, data, and events to estimate capabilities, intentions, and targeting information from many sources. Threat 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.

In many organizations, risk scenarios are developed where decision tree style risk determinations are used. Vendors and various supporting government organizations develop threat scenarios that are helpful in identifying and analyzing threats and vulnerabilities. These risk scenarios are constantly changing and will require routine review of threat assumptions used in organizational risk determination.

3.2.2.2 Determine Risk

At Tier 1, the organization determines that risk exists to its operations, assets, and individuals in the event that threats were to exploit identified vulnerabilities. Organizations determine risk by considering the likelihood that threats may exploit vulnerabilities, resulting in adverse impacts if such exploitations occur. Organizations use threat and vulnerability information, along with likelihood and impact information, to determine risk. This risk determination may be accomplished qualitatively or quantitatively.

Risk Determination and Uncertainty

The Tier 1 guidance for determining risk uncertainty indicates how combinations of likelihood and impact are combined to determine the risk level. 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 a particular concern when a risk assessment considers advanced persistent threats (APTs)[22] for which analysis of interacting vulnerabilities may be needed, knowledge of the APT 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 risk assessments. As a result, risk assessors may reach different

[22] An 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 (1) pursues its objectives repeatedly over an extended period of time, (2) adapts to defenders' efforts to resist it, and (3) is determined to maintain the level of interaction needed to execute its objectives.

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 organization to adopt justified risk response actions. The defined and applied processes of an organization provide the means to identify inconsistent practices and include processes to identify and resolve such inconsistencies.

3.2.3 Outputs

The output of the risk assessment element is a determination of risk to the organization's operations, assets, and individuals. Risk determination is the primary input for selecting appropriate risk responses in subsequent tiers and elements. The information collected in assessment activities is used to iteratively inform the risk determination on a regular basis. There are a variety of risk assessment methodologies that an organization may choose to employ. Each methodology has its own strengths and weaknesses that must be considered in determining which methodology to apply.

A utility 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 utility finds its options to mitigate this risk to be highly limited and costly and, therefore, decides to take limited measures to address this risk. This would be an example of partial acceptance of risk by an electricity subsector organization at Tier 1.

Conversely, the same utility may have recently replaced all consumer meters with new meters that transmit data wirelessly. The risk is considered relatively low after the risk assessment is performed; however, consumer fears about privacy lead the small utility 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 RISK RESPONSE AT TIER 1

For the risk response element at Tier 1, the organization evaluates, decides upon, and implements appropriate courses of action to the organization's operations, assets, individuals, and other organizations. Decisions on how to employ risk response measures across an organization may be made at Tier 1, although the decisions are informed by risk-related information from the lower tiers.

	INPUTS	ACTIVITIES	OUTPUTS
RISK RESPONSE	▪ Risk assessment ▪ Vulnerabilities ▪ Risk response guidance from the organization's Risk Management Strategy	▪ Identify risk response – Risk acceptance – Risk avoidance – Risk mitigation – Risk sharing – Risk transference – Combination ▪ Evaluate alternatives ▪ Determine and implement risk response	▪ Risk response plan

3.3.1 Inputs

Inputs to the Tier 1 risk response element may include:

- Risk assessment; and
- Risk response guidance from the organization's Risk Management Strategy.

3.3.2 Activities

3.3.2.1 Identify Risk Response

At Tier 1, risk response requires identifying alternative courses of action to respond to risk as 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.[23]

These include:

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

If an electric utility operation relied on new IT for telemetry of line and device information, the risk of failure of these devices could affect reliability, cybersecurity, and the safety of assets. A risk response the utility could incorporate is backup communications channels for fail over.

Risk Acceptance

Risk acceptance is the appropriate risk response when the identified risk is within the risk tolerance of the electricity subsector organization. In some instances, organizations may accept risk deemed to be low or moderate, depending on particular situations or conditions. Conversely, organizations that are subject to regulatory authorities will have a lower risk tolerance and may be restricted from accepting risk for specific business functions.[24] Organizations may make determinations on 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.

[23] Additional information about how an organization responds to risks can be found in Appendix G, Risk Response Strategies.

[24] For example, per NERC Reliability Standards, organizations in the electricity subsector with components deemed part of the critical infrastructure may not accept certain risks for said components.

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 their 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 subsector to mitigate risk can involve a combination of risk response measures across all tiers.

Risk Sharing

Risk sharing is the appropriate risk response when an organization desires and has the resources to shift some risk liability and responsibility to 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 occurs when organizations determine that addressing risk requires expertise or resources that are better provided by other organizations.

Risk Transference

Risk transference is the appropriate risk response when an 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. 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 transferrence often occurs when organizations determine that addressing risk requires expertise or resources that are better provided by other organizations.

3.3.2.2 Evaluate Alternatives

In the risk response element, electricity subsector 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
- 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 and/or efficiency and long-term risk to mission and business processes. 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 subsector organization.

Risk prioritization evaluation also considers the issue of competing resources. The organization should 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.

3.3.2.3 Determine and Implement Risk Response

Decisions on appropriate courses of action include some form of prioritization. Some risks may be of greater concern than other risks. In such cases, 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 may 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[25] 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 decisionmakers. The specific beliefs and approaches that organizations embrace with respect to these risk-related concepts affect the courses of action selected by decisionmakers. Once a course of action is selected, it is incorporated into the Risk Management Strategy that is communicated throughout the organization and implemented.

When developing a Risk Management Strategy, each organization should consider options to effectively mitigate known risks while allocating justified resources. The balance between controlling costs and achieving risk management objectives requires analysis of all costs. Consequence costs resulting from a system breach are much harder to determine. Depending on the scope of systems and data involved in the Risk Management Strategy, organizations may consider the following elements to determine the cost of compromise:

- Impact from service disruption on both the organization and the clients it serves;
- Value of data lost;
- Brand damage;
- Shareholder value;
- Cost of incident response and recovery; and
- Fines, penalties, and potential litigation for damages.

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

Organizations have differing roles in the electricity subsector. Risk mitigation within the organization will vary depending upon the likelihood and severity of the consequences resulting from a security breach and the investment required.

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:

- Individuals or organizational elements responsible for the selected risk response measures and specifications of effectiveness criteria (i.e., articulation of key risk and performance 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 the organization 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 the operational environments. Analyzing the risk monitoring results provides the capability to maintain awareness of the risk being incurred, highlight the need to revisit the RMP, and initiate process improvement activities, as needed.[26] Organizations employ risk monitoring tools, techniques, and procedures to increase risk awareness. This enables senior leadership to develop a better understanding of the ongoing risk to organizational operations, assets, individuals, and other organizations. Risk monitoring is fundamental to strategic cybersecurity risk management because it improves threat awareness while providing the foundation to correlate controls in a way that moves beyond a singular defense strategy.

[26] 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.

Senior leadership in the organization determines and verifies the metrics for evaluating the 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 subsector organizations with the means to:

- Verify risk response implementation;[27]
- Determine the effectiveness of risk response measures; and
- Identify risk impacting changes to IT and ICS and the operational environments of operation.

Each organization may employ risk monitoring tools, techniques, and procedures to increase risk awareness. 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 that establishes accountability for deploying and maintaining controls. The metrics used to monitor program effectiveness and reporting frequency are determined by the level of risk being managed in each business process within the organization.

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.

	INPUTS	ACTIVITIES	OUTPUTS
RISK MONITORING	▪ Information on industry best practices, tools, and frequency ▪ Cybersecurity governance structure ▪ Performance information ▪ Comprehensive lists of identified risks	▪ Develop risk monitoring strategy – Monitoring implementation – Monitoring effectiveness – Monitoring changes – Automated versus manual monitoring – Frequency of monitoring ▪ Monitor risk	▪ Validation of existence and effectiveness of risk response measures ▪ Identification of changes to IT and ICS and their environments of operation ▪ Risk monitoring strategy

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

3.4.1 Inputs

Inputs to the Tier 1 risk monitoring element include the strategy and implementation courses of action determined during the risk response element. Inputs to Tier 1 risk monitoring may also include:

- Information on industry best practices, tools, and frequency;
- Cybersecurity governance structure;
- Performance information; and
- Comprehensive lists of identified risks.

3.4.2 Activities

3.4.2.1 Develop Risk Monitoring Strategy

The organization develops a risk monitoring strategy that includes the purpose, type, and frequency of monitoring activities. The objective of a risk monitoring program is to:

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

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 the organization may result in the organization continuing to be subject to identified risks and may introduce the potential for failing to comply with regulatory requirements (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 the governance structure from business process owners or function owners to determine whether implementation of the risk response strategy has been achieved.

Monitoring Effectiveness

Monitoring effectiveness is employed by the organization to determine if implemented risk response strategies have been successful in mitigating identified risks to the acceptable risk tolerance level. Although determining effectiveness is more complex than implementation monitoring, failure to achieve desired levels of effectiveness are indications that risk response measures are implemented incorrectly or not operating as intended. Additionally, risk response measures implemented and operating correctly 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 the operational environments after implementation of risk response measures.

Monitoring Changes

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

A utility determines that it has a good handle on its risk assessment and mitigation strategy. The organization wants to start a continuous monitoring program with automation tools to progress toward a systematic and higher level of cybersecurity for its organization. The utility begins 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 cybersecurity standards. This reporting offers a chance to reevaluate the tools and methods employed to achieve compliance with the NERC CIP cybersecurity standards.

Automated Versus Manual Monitoring

In Tier 1, monitoring typically involves reporting, analysis, and policy or strategy change recommendations. The governance structure within the organization assigns key metrics to track and evaluate on a routine basis. The 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 executive leadership/governing boards and shareholders.

Frequency of Monitoring

The frequency of risk monitoring (whether automated or manual) is driven by the mission and business processes 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 the organization 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 the operational environments;
- The potential impact of risk if not properly addressed through appropriate response measures; and
- The degree to which the threat environment is changing.

The frequency of monitoring can also be affected by the type of monitoring conducted (i.e., automated versus manual approaches). Continuous monitoring[28] 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 Monitor Risk

In the risk monitoring element in Tier 1, the organization monitors IT and ICS and the operational environments on an organization-defined metric to verify compliance, determine the effectiveness of risk response measures, and identify any changes. Once an organization completes 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 established during the risk framing element.

[28] Continuous monitoring is the process and technology used to detect risk issues associated with an electricity subsector organization's operational environment maintaining ongoing awareness to support organizational risk decisions.

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 undermine the overall effort to identify and address risk.

3.4.3 Outputs

The output from the Tier 1 risk monitoring element is a risk monitoring strategy that addresses the following:

- Verifying that required risk response measures are implemented;
- Verifying that cybersecurity requirements are derived from, and traceable to, the organizational mission and business processes;
- Determining the ongoing effectiveness of risk response measures; and
- Identifying changes to IT and ICS and the operational environments.

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 as one of the risk executive functions, serving 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. The Tier 1 function provides direction that management (at Tier 2 and Tier 3) uses to guide the operations of the organization. Providing a cybersecurity governance framework 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 exist at Tier 1 and can be enhanced to address cybersecurity risk issues.

The cybersecurity risk management program developed at Tier 1 is the high-level strategy that changes over time to direct the organization on how to analyze and prioritize cybersecurity risk, risk tolerance, organizational priorities, and the goals of addressing cybersecurity risks.

Table 2 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.

Table 2: Tier 1 RMP Overview

	INPUTS	ACTIVITIES	OUTPUTS
RISK FRAMING	▪ Mission and vision statement ▪ Legislation ▪ Organizational policies ▪ Regulatory requirements ▪ Contractual relationships ▪ Financial limitations ▪ Trust relationships ▪ Organizational culture ▪ Governance structures ▪ Output 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 and implement risk tolerance ▪ Identify priorities ▪ Develop Risk Management Strategy	▪ Risk Management Strategy
RISK ASSESSMENT	▪ Risk assessment methodology ▪ Assessment of external service providers ▪ Risk aggregation methodology ▪ Outputs from Tier 1 risk framing element	▪ Identify threat and vulnerability ▪ Determine risk	▪ Determination of risk for the organization
RISK RESPONSE	▪ Risk assessment ▪ Vulnerabilities ▪ Risk response guidance from the organization's Risk Management Strategy	▪ Identify risk response – Risk acceptance – Risk avoidance – Risk mitigation – Risk sharing – Risk transference – Combination ▪ Evaluate alternatives ▪ Develop and implement risk response	▪ Risk response plan
RISK MONITORING	▪ Information on industry best practices, tools, and frequency ▪ Cybersecurity governance structure ▪ Performance information ▪ Comprehensive lists of identified risks	▪ Develop risk monitoring strategy – Monitoring implementation – Monitoring effectiveness – Monitoring changes – Automated versus manual monitoring – Frequency of monitoring ▪ Monitor risk	▪ Validation of existence and effectiveness of risk response measures ▪ Identification of changes to IT and ICS and their environments of operation ▪ Risk monitoring strategy

4. Tier 2: Mission and Business Processes

At Tier 2, mission and business process owners consider cybersecurity risks from an operations perspective. They explicitly take into account any adverse impact a process may have on the mission objectives of the organization's operations. Within electricity subsector organizations, individual business units (i.e., lines of business) may be grouped into the domains of generation, transmission, distribution, markets, and field operations. The identification of the mission, along with corresponding business processes, assists in defining both the criticality and sensitivity of operational processes and associated information.

An enterprise cybersecurity architecture is an integral part of an organization's enterprise architecture. The enterprise cybersecurity architecture represents the portion of the enterprise architecture that specifically addresses IT and ICS resilience and security and provides information for the implementation of cybersecurity risk mitigation. The enterprise cybersecurity architecture is part of an organization's overall enterprise cybersecurity program, which relates to an organization's enterprise risk management program, overall IT/ICS governance, the enterprise architecture, and physical security activities. Cybersecurity program governance provides for the principles for security guidance, as well as development of policies, standards, guidelines, procedures, and audit enforcement processes. This governance structure ensures that cybersecurity requirements are consistently applied.

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 establishes 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 organization's objectives. Within Tier 2, the business units identify and map threats, vulnerabilities, consequences, and impacts to each of the mission and business processes identified.

Methodologies identified at Tier 1 are used to evaluate the impacts associated with the loss of confidentiality, integrity, and availability of IT and ICS resources, including information and data. The methodologies may be integrated into a risk measurement framework where risk assessment results from the evaluation of business processes can be harmonized. The resulting risks identified are rank-ordered as an input to the cybersecurity program. The resulting information from the risk assessments is used to determine management, technical, and operational controls and may be helpful in determining the appropriate mitigation of risk.

The organization may assess this information to determine appropriate resources and funding needed for development and implementation of the cybersecurity program.

	INPUTS	ACTIVITIES	OUTPUTS
RISK FRAMING	▪ Outputs from Tier 1: – Mission objectives – Risk Management Strategy – Governance structure – High-level security requirements – Risk management constraints – Risk tolerance ▪ Feedback from 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 ▪ Documented lists of the impacts ▪ Documented risk assessment methodologies ▪ Process-specific risk tolerances ▪ An inventory of applications, classifications, and owners that support mission and business processes

4.1.1 Inputs

Inputs to the risk framing element for Tier 2 may include the following outputs from Tier 1:

- Mission objectives;
- Risk Management Strategy;
- Governance structure;
- High-level security requirements;
- Constraints;
- Risk tolerance; and
- Feedback from the risk monitoring element at Tier 2 and Tier 3.

4.1.2 Activities

4.1.2.1 Identify Mission and Business Processes and Applications

In Tier 2, the organization inventories and documents its mission and business processes, as well as the applications[29] 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, such as 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 large organization, for example, may include a

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

number of vertical processes related to energy generation, transmission, distribution, 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 defining its business processes is a function of how the organization determines the highest level at which these business processes support a specific mission objective. These business 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 subsector organizations may find useful guidance for identifying process in the functions as defined in the NERC Functional Model.[30]

4.1.2.2 Establish Risk Tolerance and Risk Methodology

Once mission and corresponding 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 business process. Electricity subsector organizations may consider how regulatory and contractual constraints may influence the impact to the identified business 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;
- NERC reliability standards (CIP and others) for those organizations that are registered as NERC functional entities;
- 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 subsector organizations; and
- Corporate contracts and/or agreements (including outsourcing and third parties).

[30] For additional information, see NERC Functional Model at http://www.nerc.com.

Along 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. Additional inputs to process-specific risk tolerance include sources of information for cybersecurity threats. 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.

A customer relationship management process is relatively more tolerant of risks associated with loss of availability and integrity, but much less tolerant of risks associated with loss of confidentiality: unauthorized disclosure of personal identifiable information (PII) can have a high financial and reputation impact. On the other hand, processes associated with the reliable transmission and distribution of electric power are relatively more tolerant of risks associated with loss of confidentiality and less tolerant of risks associated with availability and integrity: inability to complete an operation in real time may result in loss of life or substantial damage to the electric infrastructure.

Risk assessment methodologies provide 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, any risk assessment methodology may define impact in different ways for groups of processes using qualitative analysis techniques. Generally, risk is calculated as a function of the threat, vulnerability, likelihood, and consequence/impact:

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

Adoption of standard risk assessment methodologies for determining the impacts associated with the loss of confidentiality, integrity, and availability of IT and ICS are essential in providing input to the risk assessment element. When information on threats and their likelihood is not well defined, an option for determining relative risk level may be to focus on consequence/impact.

4.1.2.3 Identify Cybersecurity Program and Architecture

For organizations that currently maintain a cybersecurity program 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 assist in the development of these areas for your organization.

4.1.2.4 Develop or Refine Enterprise Architecture

Enterprise architecture is a management practice employed by organizations to maximize the effectiveness of their IT and ICS resources in supporting achievement of mission and business objectives. By developing the enterprise architecture or refining the existing enterprise architecture, organizations gain:

- 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, business processes, and performance goals;
- Efficient, cost-effective, consistent, and interoperable cybersecurity capabilities to help the organization better protect mission and business functions; and
- The ability to segment, build redundancy, and eliminate single points of failure.

4.1.3 Outputs

Outputs from the Tier 2 risk framing activities may include:

- Identification of mission and business processes that support the organization's Risk Management Strategy from Tier 1;
- Documented lists of impacts associated with loss of confidentiality, integrity, and availability of business process information, including data elements, and IT and ICS resources for both business administrative services and operations of electricity subsector resources;
- Documented risk assessment methodologies to be applied across all mission and business processes;
- Process-specific risk tolerances; and
- An inventory of information systems, data and/or information classifications, and business process owners supporting 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 cybersecurity 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 functions, business processes, and the information systems supporting the organization. The assessment element includes the development of a prioritized list of processes based on the consequence/impact to the organization.

RISK ASSESSMENT	INPUTS	ACTIVITIES	OUTPUTS
	▪ Risk Management Strategy from Tier 1 ▪ Reports from threat and vulnerability sources 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 information systems from the framing element of Tier 2 ▪ List of the impacts associated with the loss of confidentiality, integrity, and availability of mission and business process information, data elements, IT and ICS	▪ 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 development of the cybersecurity program and architecture

4.2.1 Inputs

Inputs to the Tier 2 risk assessment element may include:

- The Risk Management Strategy from Tier 1;
- Reports from threats and vulnerability sources[31] 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 functions, business processes, and information systems developed from the framing element of Tier 2 that support the organization's mission objectives developed in Tier 1; and
- A documented list of impacts associated with loss of confidentiality, integrity, and availability of mission and business process information, data elements, and IT and ICS.

[31] When reviewing the process-specific cybersecurity threat and vulnerability reports, organizations should 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, the organization first determines the consequence/impact for each mission and business process and application. In prioritizing mission and business processes, the organization considers the consequence/impact to the organization and the reliability of the electricity subsector.

4.2.2.2 Determine Risk

In determining risk at Tier 2, the organization focuses on organizational operations and vulnerabilities associated with enterprise architecture 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 processes due to the potential impact across multiple IT and ICS mission environments. The organization reviews process-specific cybersecurity threat and vulnerability reports to decide whether these reports have provided enough information to determine threat likelihood.

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

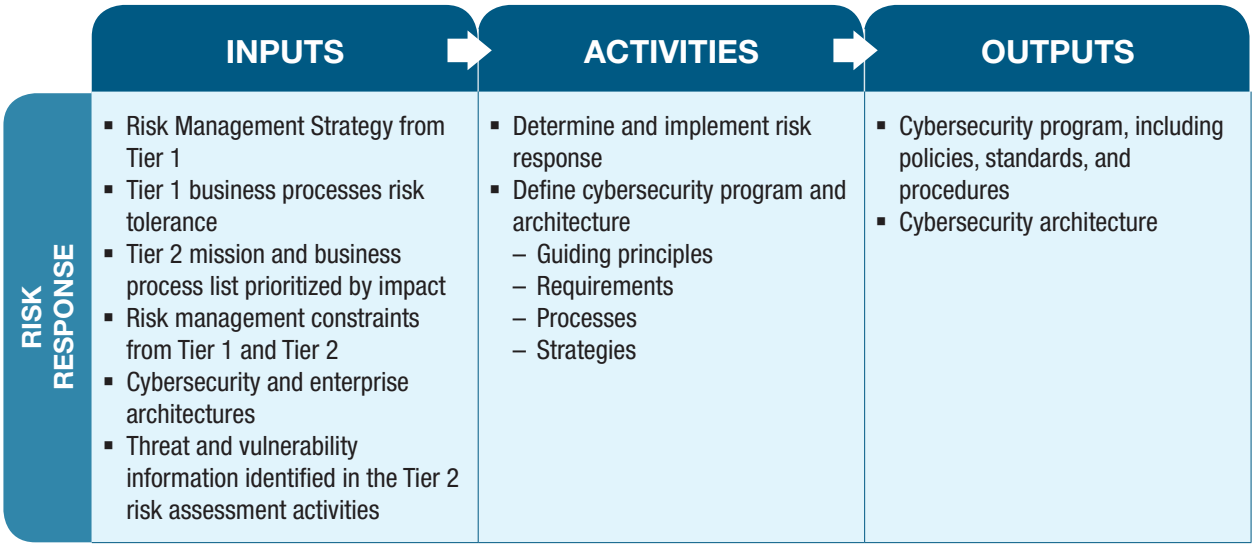
4.2.3 Outputs

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 subsector organizations use the list of mission and business processes prioritized by impact from the risk assessment element to determine the most appropriate risk response. 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;
- The Tier 1 business processes risk tolerance;
- A Tier 2 mission and business process list, prioritized by impact;
- The risk management 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 Determine and Implement Risk Response

Tier 2 risk response activities allow the organization to identify, evaluate, approve, and implement appropriate risk responses to accept, avoid, mitigate, share, or transfer risk to 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.[32]

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

4.3.2.2 Define Cybersecurity Program and Architecture

During the response element of Tier 2, organizations develop and/or refine their cybersecurity program and architecture. The organization considers how they can inject cybersecurity architecture-planning activities into the definition of the enterprise architecture. 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[33] 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 operational high-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 subsector may include the following items.

Guiding principles for the protection of enclave boundaries (e.g., network perimeter controls, access controls, monitoring)

Some cyber systems may need to establish, identify, and authorize access as part of the cybersecurity architecture. This includes defining ingress and egress filtering and documenting data flows. To facilitate this process, system logs need to be maintained and correlated to identify anomalous communication. Robust access controls should also provide for authentication, authorization, and accounting of people, process, and technology.

[33] A common cybersecurity control is one that is utilized and/or inherited throughout an organization. Additional information about common controls can be found in Appendix H, Common Controls.

Segmentation strategies for the various network enclaves 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 strategies provide guidance for the use of such controls as network firewalls (e.g., the use of various types of firewalls for controlling the ingress or egress of data from public networks or guidelines for network perimeter access to high value resources, and secured enclaves that are adjacent to business networks). Segmentation strategies for business processes (e.g., production, development, and test) that are determined by risk assessment to be high risk to mission and business processes may include increased intrusion detection and prevention monitoring.

Special requirements for generation plants, transmission, and distribution field assets

Many field assets have requirements for providing operational and nonoperational[34] data to engineering or business users for short- and long-term planning and analysis purposes. Organizations may provide standardized architectures to do this in a secure and controlled manner.

Data center and server farm environments

Organizations may provide standardized network architectures for providing secure services from network environments 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.

Separate 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. Organizations may provide a standardized architecture that would provide the level of cybersecurity controls commensurate with their risk profiles. Organizations should consider the threat environment

> In the area of interactive remote access, a sample electric subsector organization implements a standardized architecture that uses a terminal service approach with printing and file-sharing restrictions for general interactive remote access to business services. This approach mitigates vulnerabilities associated with shared file services and data exfiltration. For access to its operations networks, the organization has implemented a standardized multitiered bastion host (jump-host) architecture and strong multifactor authentication that minimizes vulnerabilities associated with connections of the source to the target system or network.

[34] Operational data are data used to operate the system, such as line flows and breaker positions. Nonoperational data are data about the system operations, such as configuration information, asset management information, or event analysis data.

for the business process or class of business processes and provide architectural options for remote access to the business process, as guidance to selecting actual controls at Tier 3.

Guiding principles for end point protection

Organizations may consider an adequate level of standardization to optimize the end point management, taking into consideration 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 subsector should consider the standard cybersecurity requirements included in supply chain sourcing business processes. The organization should have a standardized business process for evaluation for cybersecurity requirements, by using standard frameworks for vendor qualification, technical evaluation, commercial evaluation, and selection processes.

Standardized requirements for change management, testing, and production certification processes

Organizations may consider standardized architectural elements necessary to develop a framework for change control, configuration management, testing, and certification and accreditation business processes to ensure that cybersecurity effectiveness is maintained. These elements may include standardized software tools and methodologies for managing system changes and testing across the organization.

Human resource practices relevant to cybersecurity

Organizations should establish repeatable on-boarding and off-boarding business processes to assess the suitability of the workforce. On-boarding business processes should include a personnel risk assessment (also known as a background investigation or check) that performs 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 may need to establish an off-boarding program as well to ensure that all system and physical access is appropriately removed. For cases in which an employee is terminated, organizations may consider establishing repeatable procedures to forensically maintain workforce systems for investigations.

Standardized processes for cybersecurity incident response

Organizations may need to establish repeatable business processes that include training their workforce on how to identify, report, and respond to suspected cybersecurity incidents. The processes may 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 business continuity of the business and disaster recovery for operations

Organizations may need to develop repeatable processes that are based on the classification and recovery point objectives (RPOs) and recovery time objectives (RTOs) to ensure that information systems are available to the organization. The degree to which business continuity and disaster recovery are supported by the organization may be different for each mission function and business process application.

4.3.3 Outputs

Output for the Tier 2 risk response element includes:

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

4.4 RISK MONITORING AT TIER 2

In the risk monitoring element, the organization monitors and measures the effectiveness and level of conformance to their cybersecurity program and architecture. This process helps identify the risk impact of changes to IT and ICS operational environments.

	INPUTS	ACTIVITIES	OUTPUTS
RISK MONITORING	▪ Risk Management Strategy from Tier 1 ▪ Cybersecurity program and architecture ▪ Results of previous audits and 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 conformance to cybersecurity architecture ▪ Measure effectiveness of cybersecurity architecture ▪ Periodically reassess cybersecurity architecture ▪ Monitor changes to 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, which includes metrics, frequency, and scope of the monitoring processes

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 subsector organizations may take the following actions.[35]

4.4.2.1 Establish Metrics to Measure Conformance to Cybersecurity Architecture

A good measure of the appropriateness of 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 standard architecture and the rationales for these deviations, organizations can fine tune the architecture in an iterative process.

4.4.2.2 Measure Effectiveness of Cybersecurity Architecture

Measuring the effectiveness of 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.

[35] 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.

4.4.2.3 Periodically Reassess Cybersecurity Architecture

Organizations should define the frequency of comprehensive, organization-wide monitoring of the cybersecurity architecture to maintain its effectiveness and efficiency. Reassessment frequency should allow for comprehensive reviews and implementation of mitigation changes to the cybersecurity architecture.

> The proliferation and use of personal mobile devices, both for personal and corporate application use, necessitates the review of the enterprise architecture and the cybersecurity architecture to incorporate components and policies that will support the secure implementation of processes and applications in IT and ICS environments.

4.4.2.4 Monitor Changes to Environment

Electricity subsector organizations should establish business processes to review changes to the threat and vulnerability landscape for input to the risk response element. For example, the evolution of threats from simple threats based on basic scripts to sophisticated APTs changes the cybersecurity architecture needs for risk response. Deviations from enterprise architectures are evaluated by the defined governance structure.

4.4.3 Outputs

Outputs from the Tier 2 risk monitoring activities may include:

- Risk monitoring reports from effectiveness and efficiency reviews and the appropriate resulting mitigations and changes; and
- A risk monitoring strategy embedded in the cybersecurity program, which 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 business 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.

Table 3 provides an overview of the inputs, activities, and outputs from the risk framing, assessment, response, and monitoring elements in Tier 2 of the RMP.

Table 3: Tier 2 RMP Overview

	INPUTS	ACTIVITIES	OUTPUTS
RISK FRAMING	▪ Outputs from Tier 1: – Mission objectives – Risk Management Strategy – Governance structure – High-level security requirements – Risk management constraints – Risk tolerance ▪ Feedback from risk monitoring element at Tier 2 and Tier 3	▪ Identify mission and business processes and information systems ▪ Establish risk tolerance and risk methodology ▪ Identify cybersecurity program and architecture ▪ Develop or refine enterprise architecture	▪ Identification of the mission and business processes ▪ Documented lists of the impacts ▪ Documented risk assessment methodologies ▪ Process-specific risk tolerances ▪ An inventory of applications, classifications, and owners that support mission and business processes
RISK ASSESSMENT	▪ Risk Management Strategy from Tier 1 ▪ Reports from threat and vulnerability sources 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 information systems from the framing element of Tier 2 ▪ List of the impacts associated with the loss of confidentiality, integrity, and availability of mission and business process information, data elements, IT and ICS	▪ 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 development of the cybersecurity program and architecture
RISK RESPONSE	▪ Risk Management Strategy from Tier 1 ▪ Tier 1 business processes risk tolerance ▪ Tier 2 mission and business process list prioritized by impact ▪ Risk management 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 ▪ Define cybersecurity program and architecture – Guiding principles – Requirements – Processes – Strategies	▪ Cybersecurity program including policies, standards, guidelines, and procedures ▪ Cybersecurity architecture
RISK MONITORING	▪ Risk Management Strategy from Tier 1 ▪ Cybersecurity program and architecture ▪ Results of previous audits and 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 conformance to cybersecurity architecture ▪ Measure the effectiveness of cybersecurity architecture ▪ Periodically reassess cybersecurity architecture ▪ Monitor changes to environment	▪ Risk monitoring reports from the effectiveness and efficiency reviews and appropriate resulting mitigations and changes ▪ A risk monitoring strategy embedded in the cybersecurity program, which includes metrics, frequency, and scope of the monitoring processes

5. Tier 3: Information Technology and Industrial Control Systems

Tier 3 of the risk management model represents IT and ICS resources. At Tier 3, IT and ICS owners, common control providers, system and security engineers, and information system security officers make risk-based decisions on the implementation, operation, and monitoring of systems. To address risk at Tier 3, the risk management cycles use four elements—frame, assess, respond, and monitor—are applied. The major activities at Tier 3 use 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.

It is acknowledged that IT and ICS have different cybersecurity requirements. An ICS is primarily concerned with availability. The ICS communication is time critical, with specific determination requirements for jitter and latency. Conversely, delays within an IT system database or Web page access are not unexpected by IT users. While the use of encryption or packet authentication is more common with an IT system to protect confidentiality and integrity, the same use in an ICS may reduce the level of ICS performance. The activities at Tier 3 will assist in determining the controls and risk responses that apply to the cybersecurity requirements of the IT and ICS.

5.1 RISK FRAMING AT TIER 3

	INPUTS	ACTIVITIES	OUTPUTS
RISK FRAMING	▪ Risk Management Strategy from Tier 1 ▪ Threat and vulnerability information from Tier 2 ▪ Prioritized list of mission and business processes, and information systems by impact/ consequence from Tier 2 ▪ Catalog of cybersecurity controls ▪ Cybersecurity program and architecture ▪ Enterprise architecture ▪ Results from monitoring element of Tier 3 ▪ Inventory of current information systems and resources created at Tier 3	▪ Conduct IT and ICS inventory ▪ Define or refine cybersecurity plans	▪ Baseline cybersecurity plan, which includes the inventory of IT and ICS and identification of boundaries, and the list of threats and vulnerabilities

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 mission and business processes and information systems by impact/consequence from Tier 2;
- Catalog of cybersecurity controls;
- Cybersecurity program and architecture;
- Enterprise architecture;
- Results from monitoring element of Tier 3; and
- Inventory of current information systems and resources from Tier 3.

5.1.2 Activities

5.1.2.1 Conduct IT and ICS Inventory

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

5.1.2.2 Define or Refine Cybersecurity Plans[36]

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

The results of the cybersecurity plan development process influence both the selection and refinement of appropriate cybersecurity controls for IT and ICS, as well as the minimum assurance

> 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. Some organizations may have separate documents that contain different components of the cybersecurity plan. The RMP provides organizations the flexibility to decide whether their plan is one document or a collection of documents.

[36] Cybersecurity plan development outlines are provided by organizations such as the National Rural Electric Cooperative Association and NIST SP 800-18.

requirements. The cybersecurity plan process reviews organizational responsibilities for each information system in order to establish clear ownership to assess and respond to risk. 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:

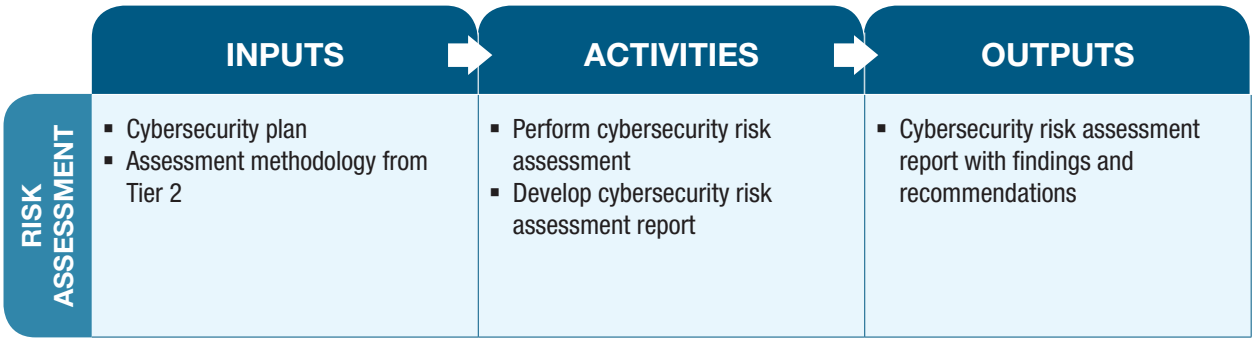
- Full descriptive name, including associated acronym;
- Owner and risk official, including contact information;
- Parent or governing organization that manages, owns, and/or controls it;
- Location and environment of operations (narrative and diagram views);
- Version or release number of the IT and 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;
- Types and sensitivity of information processed, stored, and transmitted;
- Boundary for risk management and cybersecurity authorization purposes;
- Applicable laws, policies, regulations, or standards affecting cybersecurity;
- Architectural description, including network topology;
- Hardware, firmware, operating system and application software, and system interfaces (internal and external);
- Subsystems, components, and mechanisms (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 controls that include shared accounts, administrative account, and user account management;
- Organizational affiliations, access rights, and privileges;
- Business continuity and/or disaster recovery requirements for RPO/RTO;
- Incident response points of contact;
- Cybersecurity assessment procedures; and
- Other information as required by the organization.

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 include a baseline cybersecurity plan that includes 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 methodology from Tier 2.

5.2.2 Activities

5.2.2.1 Perform Cybersecurity Risk Assessment

This activity assesses the existing cybersecurity risk by using the risk assessment procedures defined in the cybersecurity plan.[37] The cybersecurity risk assessment considers new threats and vulnerabilities to guide the adjustment of existing controls and the selection of new controls. This is done 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 IT and ICS. Following the cybersecurity risk assessment, the organization determines the consequence/impact of the residual risk 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 Develop Cybersecurity Risk Assessment Report

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

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

5.2.3 Outputs

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

5.3 RISK RESPONSE AT TIER 3

	INPUTS	ACTIVITIES	OUTPUTS
RISK RESPONSE	▪ Cybersecurity plan ▪ Cybersecurity risk assessment report	▪ Determine and implement risk response – Risk acceptance – Risk avoidance – Risk mitigation – Risk sharing – Risk transference – Combination of the above ▪ Select and refine cybersecurity controls ▪ Accept cybersecurity plan ▪ Develop and implement risk mitigation plan	▪ Risk acceptance decision ▪ Refined cybersecurity plan ▪ Risk mitigation plan

5.3.1 Inputs

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

- Cybersecurity plan; and
- Cybersecurity risk assessment report.

5.3.2 Activities

5.3.2.1 Determine and Implement Risk Response

Based on the results of the cybersecurity risk assessment, organizations determine the appropriate risk response action.[38] These risk Response Actions may be:

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

The choice of available risk responses may be constrained by regulatory compliance regimes or other mandates. For example, the acceptance of risk is not available as part of the NERC CIP cybersecurity standards. Organizations are required to select and deploy the specific controls as defined by the standards.

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

5.3.2.2 Select and Refine Cybersecurity Controls

Cybersecurity controls will be selected and refined based on the cybersecurity system categorization of 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 Accept Cybersecurity Plan

Upon completion of the cybersecurity plan, the senior executive (Tier 1) and system owner (Tier 2) review the plan and accept the response actions identified in the plan. This process documents the organizational acceptance of risk.

5.3.2.4 Develop and Implement 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, 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 operational environment. 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;
- 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 MONITORING AT TIER 3

Ongoing monitoring of cybersecurity controls is essential for maintaining an effective cybersecurity plan. Organizations need to develop a strategy for the continuous monitoring of cybersecurity controls, to include review of any proposed or actual changes to 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 IT and ICS;
- Assessment of selected cybersecurity controls employed; and
- Cybersecurity status reporting.

	INPUTS	ACTIVITIES	OUTPUTS
RISK MONITORING	▪ Cybersecurity program and architecture ▪ Refined cybersecurity plan ▪ Risk mitigation plan ▪ Threat and vulnerability information ▪ Monitoring methodology from Tier 2	▪ Manage configurations and changes ▪ Assess cybersecurity controls ▪ Monitor new threats and vulnerabilities ▪ Monitor cybersecurity mitigation plan ▪ Report cybersecurity status ▪ Implement decommissioning strategy	▪ 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

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 Manage Technology Acquisition, Configuration, and Changes

Organizations implement processes that ensure technology acquisition and configuration accounts for risks to mission and business processes. A disciplined and structured approach to managing, controlling, and documenting changes to the IT and ICS operational environments is an essential element of an effective governance around the 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 Assess Cybersecurity Controls

Organizations should assess a selected subset of the technical, management, and operational cybersecurity controls employed within, and inherited by, 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 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 Monitor 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 should establish and maintain a schedule for checking applicable information sources and identify the personnel responsible for the task.

5.4.2.4 Monitor Cybersecurity Mitigation Plan

During the monitoring element, an organization should periodically evaluate the mitigation plan to correct weaknesses or deficiencies identified during the cybersecurity control assessment. Organizations may use this as a means to report 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 Report Cybersecurity Status

Organizations should report IT and ICS cybersecurity status to the appropriate governance structure on an ongoing basis and in accordance with their monitoring strategy. This reporting includes the effectiveness and efficiency of cybersecurity controls employed within or inherited by IT and ICS. Organizations may need to review the reported cybersecurity status of 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:

- Organizational leadership with information on the cybersecurity state and the effectiveness and efficiency 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 executive leadership/governing boards; and
- A summary of changes to cybersecurity plans and cybersecurity assessment reports.

5.4.2.6 Implement Decommissioning Strategy

Organizations should implement a decommissioning strategy when resources are removed from service. When a resource is removed from operation, a number of risk management actions are required. Organizations should ensure that:

- Cybersecurity controls addressing system removal and decommissioning (e.g., media sanitization, configuration management, and control) are implemented; and
- 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 baselines and risk assessments. Mitigation plans are used to monitor the progress of how and when identified residual risks are addressed during the cybersecurity risk assessment. The outputs of Tier 3 provide feedback to the Tier 2 and Tier 1 framing elements to reinform the risk assessment.

Table 4 provides an overview of the inputs, activities, and outputs from the risk framing, assessment, response, and monitoring elements in Tier 3 of the RMP.

Table 4: Tier 3 RMP Overview

	INPUTS	ACTIVITIES	OUTPUTS
RISK FRAMING	▪ Risk Management Strategy from Tier 1 ▪ Threat and vulnerability information from Tier 2 ▪ Prioritized list of mission and business processes and information systems by impact/ consequence from Tier 2 ▪ Catalog of cybersecurity controls ▪ Cybersecurity program and architecture ▪ Enterprise architecture ▪ Results from monitoring element of Tier 3 ▪ Inventory of current information systems and resources from Tier 3	▪ Conduct IT and ICS inventory ▪ Define or refine cybersecurity plans	▪ Baseline cybersecurity plan that includes the inventory of IT and ICS and identification of boundaries, and the list of threats and vulnerabilities
RISK ASSESSMENT	▪ Cybersecurity plan ▪ Assessment methodology from Tier 2	▪ Perform cybersecurity risk assessment ▪ Develop cybersecurity risk assessment report	▪ Cybersecurity risk assessment report with findings and recommendations
RISK RESPONSE	▪ Cybersecurity plan ▪ Cybersecurity risk assessment report	▪ Determine and implement risk response – Risk acceptance – Risk avoidance – Risk mitigation – Risk sharing – Risk transference – Combination of the above ▪ Select and refine cybersecurity controls ▪ Develop and implement 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	▪ Manage technology acquisition, configuration, and changes ▪ Assess cybersecurity controls ▪ Monitor new threats and vulnerabilities ▪ Monitor cybersecurity mitigation plan ▪ Report cybersecurity status ▪ Implement decommissioning strategy	▪ 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

Appendix A References

LEGISLATION, POLICIES, DIRECTIVES, STANDARDS, AND GUIDELINES

1. American Recovery and Reinvestment Act (P.L. 111-5), February 2009.
2. Canada's Cyber Security Strategy, 2010.
3. *Canada-United States Action Plan for Critical Infrastructure*, 2010.
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. Energy Sector Control Systems Working Group, *Roadmap to Achieve Energy Delivery Systems Cybersecurity*, September 2011.
11. Federal Information Security Management Act (P.L. 107-347, Title III), December 2002.
12. International Electrotechnical Commission 62443, *Security for Industrial Automation and Control Systems Series*.
13. ISO/IEC 15408:2005, *Common Criteria for Information Technology Security Evaluation*, 2005.
14. ISO/IEC 73:2009, *Risk Management—Vocabulary*, 2009.
15. ISO/IEC 31000:2009, *Risk Management—Principles and Guidelines*, 2009.
16. ISO/IEC 27000:2009, *Information Technology—Security Techniques—Information Security Management Systems—Overview and Vocabulary*, 2009.
17. ISO/IEC 27005:2011, *Information Technology—Security Techniques—Information Security Risk Management*, 2011.
18. National Institute of Standards and Technology Federal Information Processing Standards Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004.
19. National Institute of Standards and Technology Federal Information Processing Standards Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006.
20. National Institute of Standards and Technology Interagency Report 7628, *Guidelines for Smart Grid Cyber Security*, August 2010.
21. National Institute of Standards and Technology Interagency Report 7298, Revision 1, *Glossary of Key Information Security Terms*, February 2011.

APPENDIX A REFERENCES

22. National Institute of Standards and Technology Special Publication 800-18, Revision 1, *Guide for Developing Security Plans for Federal Information Systems*, February 2006.
23. 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.
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 800-70, Revision 1, *National Checklist Program for IT Products—Guidelines for Checklist Users and Developers*, September 2009.
26. 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.
27. 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.
28. 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.
29. National Institute of Standards and Technology Special Publication 1108, Release 1, *NIST Framework and Roadmap for Smart Grid Interoperability Standards*, January 2010.
30. National Institute of Standards and Technology Special Publication 800-30, Revision 1, *Guide for Conducting Risk Assessments*, (Projected Publication Spring 2011).
31. National Institute of Standards and Technology Special Publication 800-39, Revision 1, *Managing Information Security Risk: Organization, Mission, and Information System View*, March 2011.
32. National Institute of Standards and Technology Special Publication 800-82, *Guide to Industrial Control Systems (ICS) Security*, June 2011.
33. North American Electric Reliability Corporation, *Version 4 Critical Infrastructure Protection Reliability Standards*, April 2012.
34. Office of Management and Budget, Circular A-130, Appendix III, Transmittal Memorandum #4, *Management of Federal Information Resources*, November 2000.
35. 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 information technology (IT) and industrial control system (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 used 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.

APPENDIX B GLOSSARY

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 in order 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 System	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.

APPENDIX B GLOSSARY

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 subsector 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 used by an electricity subsector organization in order to meet its 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 (1) the adverse impacts that would arise if the circumstance or event occurs and (2) 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.
Risk Evaluation	A component of the risk assessment element in which observations are made on 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 (1) establishing the context for risk-related activities, (2) assessing risk, (3) responding to risk once determined, and (4) monitoring risk over time.
Risk Management Strategy	Any strategic-level decisions on how executive leadership/governing boards manage risk to an organization's operations, resources, and other organizations.

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	Security objectives are generally categorized as Confidentiality (*preventing unauthorized disclosure*), Integrity (*preventing modification or destruction of information*), and Availability (*preventing disruption of access to or use of information or an information system*).
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**

APT	Advanced Persistent Threat
CIO	Chief Information Officer
CIP	Critical Infrastructure Protection
CNSS	Committee on National Security Systems
COTS	Commercial Off-the-Shelf
DOE	Department of Energy
ES-ISAC	Electricity Subsector Information Sharing and Analysis Center
FISMA	Federal Information Security Management Act
FS-ISAC	Financial Services Information Sharing and Analysis Center
IA	Information Assurance
ICS	Industrial Control System
ICS-CERT	Industrial Control Systems Cyber Emergency Response Team
ISO/IEC	International Organization for Standardization/International Electrotechnical Commission
IT	Information Technology
IT-ISAC	Information Technology Information Sharing and Analysis Center
NERC	North American Electric Reliability Corporation
NIST	National Institute of Standards and Technology
NRC	Nuclear Regulatory Commission
OCTAVE	Operationally Critical Threat, Asset, and Vulnerability Evaluation
PRA	Probabilistic Risk Assessment
RAM-E	Risk Assessment Methodology for Energy Infrastructures
RMP	Risk Management Process
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SP	Special Publication
SQUARE	Security Quality Requirements Engineering

Appendix D Governance Models

APPROACHES TO CYBERSECURITY GOVERNANCE

Governance in the electricity subsector can take many forms. Three approaches to cybersecurity governance can be used to meet organizational needs: (1) a *centralized* approach, (2) a *decentralized* approach, or (3) 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 processes, size of the organization, organizational operations, resources, and risk tolerance).

Centralized Governance Model

In centralized governance structures, the authority, responsibility, and decision making power are vested solely within a central body. The centralized body establishes the policies, standards, guidelines, procedures, and processes for ensuring enterprise-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 Model

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, standards, guidelines, 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 Model

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, standards, guidelines, procedures, and processes for ensuring enterprise-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, standards, guidelines, procedures, and processes for ensuring their involvement in the portion of risk management and cybersecurity strategies and decisions that are specific to their mission and business process needs and operational environments. 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 E Trust Models

APPROACHES TO ESTABLISHING TRUST RELATIONSHIPS

The following trust models describe ways in which electricity subsector organizations 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 Model

In the *validated trust model*, one organization obtains information on 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 information technology (IT) or industrial control system (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 Model

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 or its recent experience in working with 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.

APPENDIX E TRUST MODELS

Third Party Trust Model

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 Model

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 Model

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 subsector 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 F Roles and Responsibilities

KEY PARTICIPANTS IN THE RISK MANAGEMENT PROCESS (RMP)

The following sections describe the roles and responsibilities of key participants involved in an organization's RMP.[1] 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).[2] 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;

[1] Organizations may define other roles (e.g., facilities manager, human resources manager, systems administrator) to support the RMP.
[2] Caution is exercised when one individual fills multiples roles in the RMP to ensure that the individual retains an appropriate level of independence and remains free from conflicts of interest.

- 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 (1) designating a chief information security officer; (2) developing and maintaining cybersecurity policies, procedures, and control techniques to address all applicable requirements; (3) overseeing personnel with significant responsibilities for cybersecurity and ensuring that the personnel are adequately trained; (4) assisting senior organizational officials concerning their security responsibilities; and (5) coordinating with other senior officials.

INFORMATION OWNER

The *information owner* is an organizational official with statutory, management, or operational authority for specified information and is responsible 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 information technology (IT) and industrial control system (ICS) may or may not be the same as the IT and ICS owner. Information owners provide input to IT and ICS owners about 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 (1) possesses professional qualifications, including training and experience, required to administer the cybersecurity program functions; (2) maintains cybersecurity duties as a primary responsibility; and (3) heads an office with the mission and resources to assist the organization in achieving more secure information and IT and ICS.

IT AND ICS OWNER(S)

The *IT and ICS owner(s)* is/are responsible for the procurement, development, integration, modification, operation, maintenance, and disposal of an IT and ICS. The IT and ICS owner(s) also ensures/ensure 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 their environments 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.

INFORMATION SECURITY ARCHITECT

The *information security architect* is an individual, group, or organization responsible for ensuring that the information security requirements necessary to protect the organizational missions/business functions are adequately addressed in all aspects of enterprise architecture, including reference models, segment and solution architectures, and the resulting information systems supporting those missions and business processes. The information security architect serves as the liaison between the enterprise architect and the information system security engineer. In addition, information security architects advise the chief information officer, chief information security officer, and risk executive on a range of security-related issues, including, for example, assessing the severity of weaknesses and deficiencies in the information system, risk mitigation approaches, security alerts, and potential adverse effects of vulnerabilities.

INFORMATION SYSTEM SECURITY ENGINEER

The *information system security engineer* is an individual, group, or organization responsible for conducting information system security engineering activities. Information system security engineering is a process that captures and refines information security requirements and ensures that the requirements are effectively integrated into IT component products and information systems through purposeful security architecting, design, development, and configuration. Information system security engineers employ best practices in software engineering methodologies, system/security engineering principles, secure design, secure architecture, and secure coding techniques. System security engineers coordinate their security-related activities with the information security architects, chief information security officer, information system owners, and other security risk and compliance stakeholders.

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 information systems (information technology [IT] and industrial control system [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 mission/business requirements, and/or changes to the operational environment. 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;
- Enterprise architectures (including cybersecurity architectures) are designed with consideration for realistically achievable risk mitigations;
- Risk mitigation measures are implemented within organizational IT and ICS and their operational environments by cybersecurity controls (i.e., safeguards or countermeasures) consistent with cybersecurity architectures; and
- Cybersecurity programs, processes, and cybersecurity controls are highly flexible and agile with regard to implementation, recognizing the diversity in organizational mission and business processes, the variations in IT and ICS implementations and capabilities, and the dynamic environments in which the organizations operate.[1]

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 cybersecurity controls implemented in the environments in which the products and systems operated.

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

APPENDIX G RISK RESPONSE STRATEGIES

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), a more comprehensive risk mitigation strategy is needed—a strategy that combines traditional boundary protection with agile defense.

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,[2] by defeating the initial cybersecurity 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.[3] This dual protection strategy illustrates two important cybersecurity concepts known as defense-in-depth[4] and defense-in-breadth.[5]

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 executive leadership/governing boards take ownership and be ultimately responsible and accountable for risk decisions.

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

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

[4] *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.

[5] *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).

The purpose of risk response is to provide a consistent, enterprise-wide response by (1) developing alternative courses of action for responding to risk, (2) evaluating the alternative courses of action, (3) determining appropriate courses of action consistent with organizational risk tolerance, and (4) implementing risk responses that are based on selected courses of action. There are five basic types of responses to risk: (1) accept, (2) avoid, (3) mitigate, (4) share, and (5) 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 business 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 executive leadership/governing boards 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 executive leadership/governing boards are willing to go with regard to accepting risk to organizational operations, resources, and other organizations.

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.

APPENDIX G RISK RESPONSE STRATEGIES

RISK AVOIDANCE STRATEGIES

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

RISK SHARING STRATEGIES

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

RISK TRANSFER STRATEGIES

Organizational risk transfer strategies enable risk decisions for specific organizational missions and business functions through policies, contracts, and agreements. Risk transfer strategies consider and take full advantage of transferring the potential impact across internal or external organizations. Transferring risk involves delegating full 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.

Appendix H Common Controls

INTRODUCTION

Common controls are security controls employed at the organization level that typically serve multiple information systems. By centrally managing and documenting the development, implementation, assessment, authorization, and monitoring of common controls, organizations can amortize security costs across multiple information systems. Examples of business process areas having common controls include contingency planning, incident response, security training and awareness, personnel security, physical and environmental protection, and security program management. These business process areas are generally good candidates for common controls.

IDENTIFICATION

Common controls are generally identified through an enterprise-wide exercise with the active involvement of the risk executive (function) and information technology (IT) and industrial control system (ICS) owners. The enterprise-wide exercise considers the cybersecurity risks and risk mitigation strategies of the organization. Common controls may be assigned to specific organizational entities (designated as common control providers) for development, implementation, assessment, and monitoring. Common control providers may also be the IT and ICS owners when the common controls reside in the IT or ICS system.

IMPLEMENTATION AND ASSESSMENT

The electricity subsector organization consults IT and ICS owners when identifying common controls to ensure that the security capability provided by the inherited controls is sufficient to deliver adequate protection. When the common controls provided by the organization are not sufficient for information systems inheriting the controls, the information system owners supplement the common controls with system-specific or hybrid controls to achieve the required protection for the system and/or accept greater risk.

Tier 1 ensures that common control providers keep common control information current since the controls typically support multiple organizational information systems. Common controls are documented in the cybersecurity plan and IT and ICS information system-specific cybersecurity plans for the information systems inheriting those controls.

Electricity subsector organizations ensure that common control providers have the capability to rapidly broadcast changes in the status of common controls that adversely affect the protections

being provided by and expected of the common controls. Common control providers are able to quickly inform information system owners when problems arise in the inherited common controls (e.g., when an assessment or reassessment of a common control indicates the control is flawed in some manner, or when a new threat or attack method arises that renders the common control less than effective in protecting against the new threat or attack method).

EXTERNAL PROVIDERS

If common controls are provided to the organization (and its information systems) by entities external to the organization (e.g., shared and/or external service providers), arrangements are made with the external/shared service providers by the organization to obtain information on the effectiveness of the deployed controls.

DOE/OE-0003