Draft NISTIR 8286

Integrating Cybersecurity and Enterprise Risk Management (ERM)

Kevin Stine
Stephen Quinn
Greg Witte
Karen Scarfone
R. K. Gardner

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8286-draft

National Institute of
Standards and Technology
U.S. Department of Commerce

Draft NISTIR 8286

Integrating Cybersecurity and Enterprise Risk Management (ERM)

Kevin Stine
Applied Cybersecurity Division
Information Technology Laboratory

Greg Witte
Huntington Ingalls Industries
Annapolis Junction, MD

Stephen Quinn
Computer Security Division
Information Technology Laboratory

Karen Scarfone
Scarfone Cybersecurity
Clifton, VA

R. K. Gardner
New World Technology Partners
Annapolis, MD

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8286-draft

March 2020

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Walter Copan, NIST Director and Under Secretary of Commerce for Standards and Technology

National Institute of Standards and Technology Interagency or Internal Report 8286
53 pages (March 2020)

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8286-draft

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies, may be used by federal agencies even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, federal agencies may wish to closely follow the development of these new publications by NIST.

Organizations are encouraged to review all draft publications during public comment periods and provide feedback to NIST. Many NIST cybersecurity publications, other than the ones noted above, are available at https://csrc.nist.gov/publications.

Public comment period: *March 19, 2020* through ~~*April 20, 2020*~~ *May 20, 2020*

National Institute of Standards and Technology
Attn: Applied Cybersecurity Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930
Email: nistir8286@nist.gov

All comments are subject to release under the Freedom of Information Act (FOIA).

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems.

Abstract

The increasing frequency, creativity, and variety of cybersecurity attacks means that all enterprises should ensure cybersecurity risk is getting the appropriate attention within their enterprise risk management (ERM) programs. This document is intended to help individual organizations within an enterprise improve their cybersecurity risk information, which they provide as inputs to their enterprise's ERM processes through communications and risk information sharing. By doing so, enterprises and their component organizations can better identify, assess, and manage their cybersecurity risks in the context of their broader mission and business objectives. Focusing on the use of risk registers to set out cybersecurity risk, this document explains the value of rolling up measures of risk usually addressed at lower system and organization levels to the broader enterprise level.

Keywords

cybersecurity risk management; cybersecurity risk measurement; cybersecurity risk profile; cybersecurity risk register; enterprise risk management (ERM); enterprise risk profile.

Acknowledgments

The authors wish to thank all individuals, organizations, and enterprises that contributed to the creation of this document.

Audience

The primary audience for this publication is cybersecurity professionals, from the Chief Information Security Officer (CISO) on down, who understand cybersecurity but may be unfamiliar with the details of enterprise risk management (ERM). The secondary audience is corporate officers and high-level executives and others who understand ERM but are probably unfamiliar with the details of cybersecurity.

Trademark Information

All registered trademarks and trademarks belong to their respective organizations.

Note to Reviewers

This draft is provided to promote greater understanding of the relationship between cybersecurity risk management and ERM, and the benefits of integrating those approaches. It is the first in a planned series to address integrating cybersecurity risk management and ERM. NIST welcomes comments on any aspects of this draft, and requests that reviewers especially consider the following questions.

Does this draft adequately and appropriately:

- define cybersecurity risk management and ERM?
- define the relationship and distinguish between cybersecurity risk management and ERM?
- define and distinguish between systems, organizations, and enterprises?
- explain the value of integrating cybersecurity risk management and ERM?
- provide information in a manner that is comprehensible by the cybersecurity and enterprise risk managers who are intended to benefit from the publication?
- illustrate ways in which organizations and enterprises may integrate cybersecurity risk management and ERM?

Also, what additional topics that are introduced or clarified in this document should NIST further decompose in this or a future document?

Call for Patent Claims

This public review includes a call for information on essential patent claims (claims whose use would be required for compliance with the guidance or requirements in this Information Technology Laboratory (ITL) draft publication). Such guidance and/or requirements may be directly stated in this ITL Publication or by reference to another publication. This call also includes disclosure, where known, of the existence of pending U.S. or foreign patent applications relating to this ITL draft publication and of any relevant unexpired U.S. or foreign patents.

ITL may require from the patent holder, or a party authorized to make assurances on its behalf, in written or electronic form, either:

a) assurance in the form of a general disclaimer to the effect that such party does not hold and does not currently intend holding any essential patent claim(s); or

b) assurance that a license to such essential patent claim(s) will be made available to applicants desiring to utilize the license for the purpose of complying with the guidance or requirements in this ITL draft publication either:

    i. under reasonable terms and conditions that are demonstrably free of any unfair discrimination; or
    ii. without compensation and under reasonable terms and conditions that are demonstrably free of any unfair discrimination.

Such assurance shall indicate that the patent holder (or third party authorized to make assurances on its behalf) will include in any documents transferring ownership of patents subject to the assurance, provisions sufficient to ensure that the commitments in the assurance are binding on the transferee, and that the transferee will similarly include appropriate provisions in the event of future transfers with the goal of binding each successor-in-interest.

The assurance shall also indicate that it is intended to be binding on successors-in-interest regardless of whether such provisions are included in the relevant transfer documents.

Such statements should be addressed to: nistir8286@nist.gov

Executive Summary

Enterprise risk management (ERM) calls for understanding all of the negative risks (from threats) and positive risks (from opportunities) facing an enterprise, determining how best to address those risks, and ensuring the necessary actions are taken. Cybersecurity risk is only one portion of an enterprise's risks. Other commonly identified risk types include, but are not limited to, financial, legal, legislative, operational, privacy, reputational, and strategic risks. [1] As part of an ERM program, enterprises manage the combined set of risks holistically.

The individual organizations comprising every enterprise are experiencing an increasing frequency, creativity, and variety of cybersecurity attacks. All organizations and enterprises, regardless of size or type, should ensure that cybersecurity risk gets the appropriate attention as they carry out their ERM functions. This document offers NIST's cybersecurity risk management expertise to help organizations improve the cybersecurity risk information they provide as inputs to their enterprise's ERM processes.

Many resources document ERM frameworks and processes. They generally include similar approaches: identify context, identify risks, analyze risk, estimate risk importance, determine and execute the risk response, and identify and respond to changes over time. The critical risk document used to track and communicate risk information for all these steps throughout the enterprise is called a *risk register*.[1] [2] For example, *cybersecurity risk registers* are a key aspect of managing and communicating about those particular risks. Each register is updated, evolves, and matures as other risk activities take place.

At higher levels in the enterprise structure, those cybersecurity and other risk registers ideally are aggregated, normalized, and prioritized into *risk profiles*. A risk profile is defined by Office of Management and Budget (OMB) Circular A-123 as "a prioritized inventory of the most significant risks identified and assessed through the risk assessment process versus a complete inventory of risks." [3] Enterprise-level decision makers use those risk profiles to choose which enterprise risks to address and then to delegate responsibilities to appropriate risk owners.

Cybersecurity risk inputs to ERM processes should be documented and tracked in written cybersecurity risk registers. However, most enterprises do not communicate their cybersecurity risk in consistent, repeatable ways. Methods such as quantifying cybersecurity risk in dollars and aggregating cybersecurity risks are largely ad hoc and are not performed with the same rigor as other types of risk within the enterprise. Improving the risk measurements and risk analysis methods used in cybersecurity risk management, along with widely adopting the use of cybersecurity risk registers, would improve the quality of the risk information communicated to ERM. In turn, this practice would promote better management of cybersecurity risk—and risks in general—at the enterprise level.

[1] Office of Management and Budget (OMB) Circular A-11 defines a risk register as "a repository of risk information including the data understood about risks over time." [2]

Table of Contents

List of Appendices

List of Figures

List of Tables

1 Introduction

The terms *organization* and *enterprise* are often used interchangeably.[2] However, for the purposes of this document, an *organization* is defined as an entity of any size, complexity, or positioning within a large organizational structure (e.g., a federal agency or company). [5] An *organization* also may be defined as a "person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its objectives." [6] An *enterprise* is an organization by these definitions, but it exists at the top level of the hierarchy and accordingly has unique risk management responsibilities. In terms of cybersecurity risk management, most responsibilities tend to be carried out by individual organizations within an enterprise. The remaining responsibilities are performed by officers at the highest level of governance and direction for the enterprise.

Figure 1 depicts a notional enterprise with subordinate organizations and illustrates that one of those subordinate units has its own enterprise considerations. Both government and industry are represented in this depiction. Consider the White House as the higher-level enterprise, with each lower-level enterprise a department and each organization an agency. Regarding industry, consider mergers and acquisitions where an enterprise purchases another company, which itself was an enterprise, and then subordinates it within the higher-level enterprise's conglomeration of organizations and systems.[3] (See Section 2.2.4 for more information on what *systems* are.)

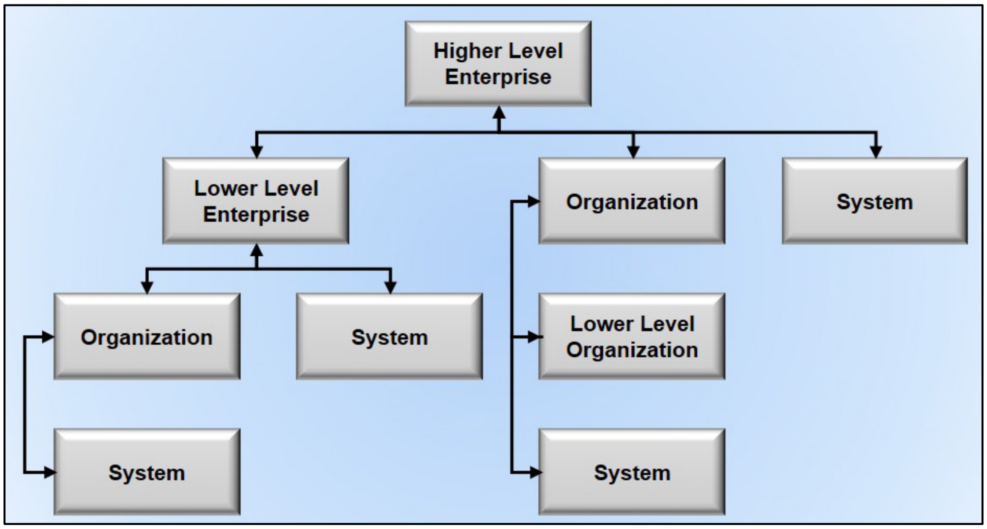


Figure 1: Enterprise Hierarchy for Cybersecurity Risk Management

[2] For example, NIST IR 8170 [4] uses *enterprise risk management* and *organization-wide risk management* interchangeably. The scope of IR 8170 includes smaller enterprises than this publication does, so an *enterprise* as defined in IR 8170 may be comprised of a single organization. The enterprises being discussed in this publication have more complex compositions.

[3] An enterprise can be thought of structurally as a portfolio (or set of portfolios). Just as a portfolio can be a combination of programs, projects, and lower-level portfolios, so too can an enterprise be comprised of one or more systems, organizations, and subordinate enterprises.

1.1 Purpose and Scope

The purpose of this document is to help improve communications and risk information sharing between and among systems' cybersecurity professionals, organizations' high-level executives, and enterprises' corporate officers. The goal is to help the personnel in those enterprises and their subordinate organizations and systems to better identify, assess, and manage their cybersecurity risks in the context of their broader mission and business objectives.[4] This document will help high-level executives and corporate officers understand the challenges cybersecurity professionals face in providing them the information they are accustomed to getting for other types of risk. This document also will help cybersecurity professionals to understand what executives and corporate officers need to carry out enterprise risk management (ERM). This includes but is not limited to what data to collect, what analysis to do, and how to consolidate low-level risk information so that it provides usable inputs for ERM processes.

Government and private industry ERM processes are similar, but often involve different oversight and reporting requirements such as Congressional testimony versus a regulatory filing. This document references some materials that are specifically intended for use by federal agencies, but the concepts and approaches should be useful for all organizations.

1.2 Document Structure

The remainder of this document is organized into the following major sections:

- Section 2 explains the basics of ERM and cybersecurity risk management, then highlights high-level gaps between current practices for ERM and cybersecurity risk management.
- Section 3 discusses cybersecurity risk considerations throughout the ERM process in detail, highlighting use of the risk register to document cybersecurity risk as ERM input.
- Section 4 examines adopting a portfolio view of risk at the enterprise level based on normalizing and aggregating risk registers into an Enterprise Risk Register.
- The References section lists the references for the document.
- Appendix A contains acronyms used in the document.
- Appendix B provides a glossary of terminology used in the document.
- Appendix C lists federal government sources for identifying risks as defined in *Playbook: Enterprise Risk Management for the U.S. Federal Government* [1].

An Informative Reference that crosswalks between the contents of this document and the NIST Cybersecurity Framework will be posted as part of the National Cybersecurity Online Informative References (OLIR) Program.[5]

[4] Figure 1 depicts the correlation of cybersecurity professional (system), high-level executive but without fiduciary reporting requirements (organization), and corporate officer with fiduciary reporting requirements (enterprise), respectively.

[5] See https://www.nist.gov/cyberframework/informative-references for an overview of OLIR.

2 Gaps in Managing Cybersecurity Risk Versus Enterprise Risk

Today's digital information and technologies impact every aspect of enterprise environments. This publication focuses on *cybersecurity risk*[6] management in the enterprise. It complements other NIST documents by informing and extending existing guidance to ensure coverage of all types of risk to an enterprise's information, data, and technology. This first necessitates understanding the basics of ERM and the current state of cybersecurity risk management, and then seeing and bridging the gaps between those practices.

2.1 Overview of ERM

ERM calls for understanding all the types of risk an enterprise faces, determining how to address that risk, and ensuring the necessary actions are taken. Cybersecurity risk is only one portion of the spectrum of an enterprise's risks that ERM addresses. Appendix A of *Playbook: Enterprise Risk Management for the U.S. Federal Government* [1] defines 11 risk types, including compliance, cybersecurity ("cyber information security"), financial, legal, legislative, operational, reputational, and strategic. In ERM, enterprises manage the combined set of enterprise risks holistically.[7]

The publication *Enterprise Risk Management—Integrating with Strategy and Performance* defines ERM as the "culture, capabilities, and practices that organizations integrate with strategy-setting and apply when they carry out that strategy, with a purpose of managing risk in creating, preserving, and realizing value." [9] The function of ERM is to ensure that the enterprise's mission, finances (e.g., net revenue, capital, and free cash flow), and reputation (e.g., stakeholder trust) are assured in the face of natural, accidental, and adversarial threats. Effective management results from balancing the achievement of a mission and objectives while optimizing the application of resources (which are often limited) and risk.

This document draws on ERM principles regarding integration with culture, strategy, and performance. Among those principles is that an "organization must manage risk to strategy and business objectives in relation to its *risk appetite*—that is, the types and amount of risk, on a broad level, it is willing to accept in its pursuit of value." [9] Another important ERM concept is *risk tolerance*—the organization's or stakeholders' readiness to bear the remaining risk after risk response in order to achieve its objectives, with the consideration that such tolerance can be

[6] *Cybersecurity risk* is an effect of uncertainty on or within a digital context. Cybersecurity risks relate to the loss of confidentiality, integrity, or availability of information, data, or information (or control) systems and reflect the potential adverse impacts to organizational operations (i.e., mission, functions, image, or reputation) and assets, individuals, other organizations, and the Nation. (Definition based on International Organization for Standardization [ISO] Guide 73 [7] and NIST Special Publication [SP] 800-60 Vol. 1 Rev. 1 [8])

[7] "OMB Circular A-123 establishes an expectation for federal agencies to proactively consider and address risks through an integrated, organization-level view of events, conditions, or scenarios that impact mission achievement." [4]

influenced by legal or regulatory requirements.[8] [7] Risk appetite is usually defined at the enterprise or organizational level, while risk tolerance is usually defined at the system level.[9] [4]

2.1.1 Common Use of ERM

Public officials or corporate boards typically measure and weigh the impact and likelihood of each type of significant threat (e.g., market, operational, labor, geopolitical, cyber) to determine their individual and total impact on the enterprise's mission, finances, and reputation. They then determine risk appetite and resource allocations for each type of risk, commensurate with impact and likelihood, and balanced among all enterprise risk exposures. Public officials or board members also provide guidance to corporate officers at the enterprise level and high-level executives at the organizational level (see Figure 1), and that guidance includes capital expenditures (CapEx) and operating expenses (OpEx) ceilings and free cash flow objectives. They also then issue guidance to continue, accelerate, reduce, delay, or cancel significant enterprise initiatives. At the same time, these executives make decisions about what constitutes prudent risk disclosures in order to balance the competing objectives of informing stakeholders and overseers (including regulators). This includes required filings and statements at hearings, and protection of sensitive information from competitors and adversaries.

2.1.2 ERM Framework Steps

There are many resources that document ERM frameworks and processes. Table 1 provides a notional crosswalk among several of these resources. They all generally include the same approaches: identify context, identify risks, analyze risk, estimate risk importance, determine and execute the risk response, and identify and respond to changes over time. The resources used in Table 1 are the ERM Playbook [1], International Organization for Standardization (ISO) 31000 [10], OMB Circular A-123 [3], the U.S. Government Accountability Office (GAO) Standards for Internal Control in the Federal Government (Green Book) [11], and three of the core publications for the NIST Risk Management Framework: SP 800-30 Revision 1, *Guide for Conducting Risk Assessments* [12], SP 800-37 Revision 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy* [13], and SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View* [14].

[8] Similar guidance comes from OMB Circular A-123: "Risk must be analyzed in relation to achievement of the strategic objectives established in the Agency strategic plan (See OMB Circular No. A-11, Section 230), as well as risk in relation to appropriate operational objectives. Specific objectives must be identified and documented to facilitate identification of risks to strategic, operations, reporting, and compliance." [3]

[9] NIST SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View* [14] uses the term "risk tolerance" to collectively refer to what this publication differentiates into two terms: "risk tolerance" and "risk appetite." NIST SP 800-39 also uses the term "organizational culture," which "refers to the values, beliefs, and norms that influence the behaviors and actions of the senior leaders/executives and individual members of organizations. […] The organization's culture informs and even, to perhaps a large degree, defines that organization's risk management strategy." In other words, an organization's culture directly informs its risk appetite.

Table 1: Notional Crosswalk Among Selected ERM and Risk Management Frameworks

ERM Playbook	ISO 31000:2009		OMB A-123	GAO Green Book	NIST Risk Management Framework		
					SP 800-30 Rev. 1	SP 800-37 Rev. 2	SP 800-39
Identify the Context	Establish External Context (5.3.2), Establish Internal Context (5.3.3)		Establish Context	Define objectives and risk tolerances (6.01)	Preparing for the Risk Assessment (3.1)	Prepare (3.1)	Framing Risk (3.1)
Identify the Risks	Risk Assessment	Risk Identification (5.4.2)	Identify Risks	Identification of Risks (7.02)	Task 2-1: Identify and characterize threat sources of concern (3.2), Task 2-2: Identify potential threat events, threat sources (3.2), Task 2-3: Identify vulnerabilities/predisposing conditions (3.2)	Prepare (3.1), Task P-14, Risk Assessment - System, Risk Assessment Report (RAR) Assess (3.5)	
Analyze the Risks		Risk Analysis (5.4.3)	Analyze and Evaluate	Analysis of Risks (7.05)	Task 2-5: Determine the adverse impacts from threat events (3.2), Task 2-4: Determine the likelihood (3.2), Task 2-6: Determine the risk to the organization (3.2) Risk Assessment Report (Appendix K)		Assessing Risk (3.2)
Assess Impact		Calculate Level of Risk		Management estimates the significance of a risk, considering the magnitude of impact, likelihood of occurrence, and nature of the risk			
Assess Likelihood							
Prioritize Risks							
Calculate Exposure							
Plan and Execute Response Strategies		Risk Evaluation (5.4.4)	Develop Alternatives	Response to Risks (7.08)	Task 3-1: Communicate Risk Assessment Results Task 3-2: Share Risk-Related Information (3.3) Also See 800-37 Rev. 2 See 800-39	Categorize (3.2), Select (3.3), and Implement (3.4)	Responding to Risk (3.3)
	Risk Treatment (5.5)		Respond to Risks			Implement (3.4), Authorize (3.6), Residual Risk reflected in POA&M	
Monitor, Evaluate, and Adjust	Monitoring and review (5.6)		Monitor and Review	Identification of Change (9.02) Analysis of and Response to Change (9.04)	Task 4-1: Conduct ongoing monitoring of the risk factors (3.4) Task 4-2: Update Risk Assessment	Monitor (3.7)	Monitoring Risk (3.4)

This document utilizes the processes of the ERM Playbook [1] (column 1 in Table 1) to address cybersecurity risks. Figure 2 from the ERM Playbook depicts an example of an ERM framework. The steps in Figure 2 are used as the basis for structuring the rest of this document, but this is not meant to imply that all enterprises should use these particular steps. Enterprises should use whatever ERM approach they favor, with the assumption that it will contain the content of these steps in some way. The top row within Figure 2 depicts six steps, with the arrows indicating sequence. The lower row of boxes explains the output of each step. The element at the bottom of the figure indicates that communication and consultation occur throughout all steps. Section 3 discusses each of these steps in detail:

1. **Identify the context.** Context is the environment in which the enterprise operates and is influenced by the risks involved.
2. **Identify the risks.** This means identifying the comprehensive set of positive and negative risks—determining which events could enhance or impede objectives, including the risks entailed by failing to pursue an opportunity.
3. **Analyze the risks.** This involves estimating the likelihood that each identified risk event will occur and the potential impact of the consequences described.
4. **Prioritize the risks.** The exposure is calculated for each risk based on likelihood and potential impact, and then the risks are prioritized based on their exposure.
5. **Plan and execute risk response strategies.** The appropriate response is determined for each risk, with the decisions informed by risk guidance from leadership.
6. **Monitor, evaluate, and adjust.** Continual monitoring ensures that enterprise risk conditions remain within the defined risk appetite levels as cybersecurity risks change.

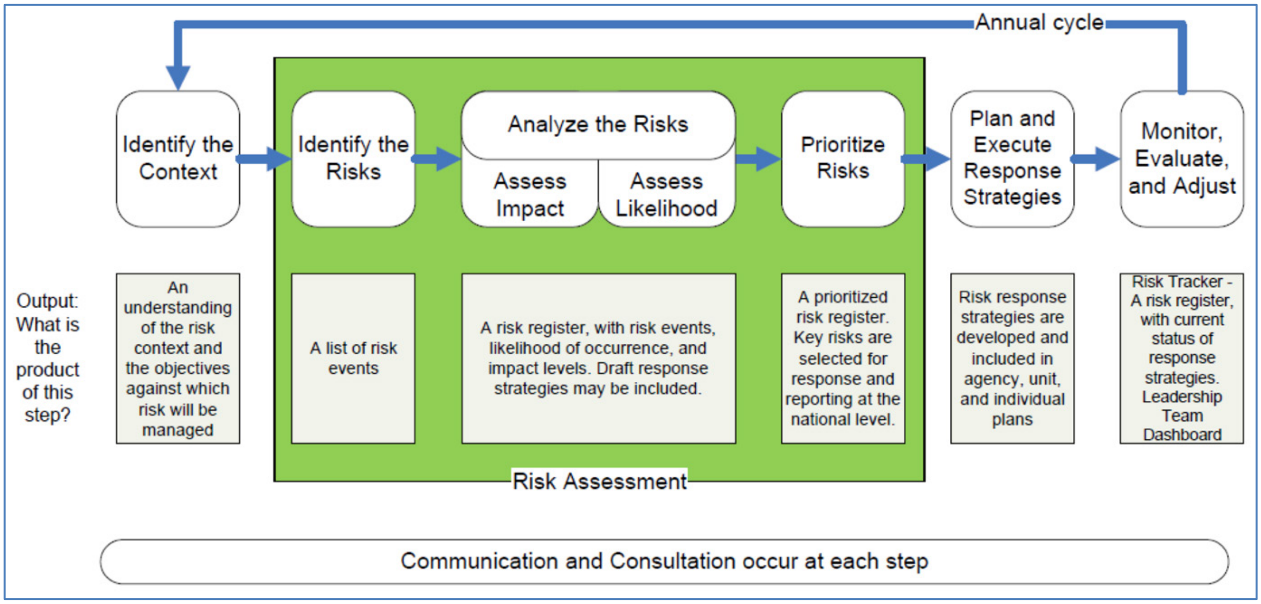

Annual cycle
Identify the Context
Identify the Risks
Analyze the Risks
Assess Impact
Assess Likelihood
Prioritize Risks
Plan and Execute Response Strategies
Monitor, Evaluate, and Adjust
Output: What is the product of this step?
An understanding of the risk context and the objectives against which risk will be managed
A list of risk events
A risk register, with risk events, likelihood of occurrence, and impact levels. Draft response strategies may be included.
A prioritized risk register. Key risks are selected for response and reporting at the national level.
Risk response strategies are developed and included in agency, unit, and individual plans
Risk Tracker - A risk register, with current status of response strategies. Leadership Team Dashboard
Risk Assessment
Communication and Consultation occur at each step

Figure 2: ERM Framework Example

Cybersecurity risk that should become an ERM input needs to be documented and tracked in cybersecurity risk registers. OMB Circular A-11 describes a *risk register* as “a repository of risk information including the data understood about risks over time.” It also states, “Typically, a risk register contains a description of the risk, the impact if the risk should occur, the probability of its occurrence, mitigation strategies, risk owners, and a ranking to identify higher priority risks.” [2] Cybersecurity risk registers are a key aspect of managing cybersecurity risks within an enterprise. Each register evolves and matures as other risk activities take place. OMB Circular A-123 [3] recommends (and for federal users, requires) that risks be recorded in a risk register of appropriate content and format. Section 3 of this document contains more information on cybersecurity risk registers.

There are many publications with more information on ERM fundamentals. Examples include:

- OMB Circular A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*[10] [3]
- *Enterprise Risk Management Integrating with Strategy and Performance* [9]
- *Playbook: Enterprise Risk Management for the U.S. Federal Government* [1]

2.2 Shortcomings of Typical Approaches to Cybersecurity Risk Management

Cybersecurity risk management, which functions at a lower level (system and organization) than ERM (enterprise), follows the same high-level principles as the ERM framework. However, cybersecurity risk management is typically executed quite differently, and its outputs are often inadequate as direct ERM inputs. Common reasons for these shortcomings are described below.

2.2.1 Lack of Asset Information

Keeping track of an organization's computing assets, especially end user devices and data, has always been a challenge. However, it has been exacerbated with the proliferation of mobile devices (e.g., smartphones, tablets), the Internet of Things (IoT), and cloud computing. It is increasingly difficult to know which computing devices the organization uses and where the organization's data are stored, especially when devices and data are changing constantly. The lack of computing asset information poses obvious challenges for identifying cybersecurity risk.

2.2.2 Lack of Measures

Cybersecurity risk measurement has been extensively researched for decades, but relatively little progress has been made. As measurement techniques have evolved, the complexity of digital assets has greatly increased, making the measurement problem more difficult to solve. Some low-level measures have been standardized, like the estimated likelihood and impact of a particular vulnerability being exploited, but even those measures are qualitative and subjective. [15] Still, this is better than most other aspects of cybersecurity risk, where there are no standard measures at all. Without quantitative measures—and in most cases, without even qualitative measures—there is little basis for analyzing risk or expressing risk in comparable ways across digital assets and the systems composed of those assets.

[10] "This Circular defines management's responsibilities for enterprise risk management (ERM) and internal control. The Circular provides updated implementation guidance to federal managers to improve accountability and effectiveness of federal programs as well as mission-support operations through implementation of ERM practices and by establishing, maintaining, and assessing internal control effectiveness. The Circular emphasizes the need to integrate and coordinate risk management and strong and effective internal control into existing business activities and as an integral part of managing an agency." [4]

2.2.3 Informal Analysis Methods

Given the lack of asset information and measures, risk analysis tends to be informal for cybersecurity risk management. Decisions are often made based on an individual's instinct and knowledge of conventional wisdom and typical practices. For example, many security controls are automatically applied to protect a new device without first doing analysis to determine how those controls would affect risk. In addition, there is usually no analysis performed after control deployment to determine if risk has been reduced to a level deemed acceptable.

2.2.4 Focus on the System Level

Management of cybersecurity risk is conducted in different ways at the various levels including at the system, organization, and enterprise level, as depicted in Figure 1. A *system* is defined as "a discrete set of information resources organized expressly for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information." [5] A common practice is for individual system-level teams to be responsible for tracking relevant risks. Typically, there is no mechanism in place to consolidate the cybersecurity risk data for systems to the organization level, much less to the enterprise level, so cybersecurity risk management tends to struggle with understanding cybersecurity risk at higher levels and seeing the big picture.

2.2.5 Increasing System and Ecosystem Complexity

Many systems upon which agencies and institutions rely are complex adaptive "systems-of-systems," composed of thousands of interdependent components and myriad channels. They operate in a rapidly changing socio-political-technological environment that presents threats from individual, group, and state actors with shifting alliances, attitudes, and agendas.

The constant introduction of new technologies has changed and complicated cyberspace. Wireless connections, big data, cloud computing, and IoT present new complexities and concomitant vulnerabilities. Information and technology no longer represent the automated file system. Rather, they have become the central nervous system, often the very assets, of most organizations. This ecosystem's increasing complexity gives rise to systemic risks and exploitable vulnerabilities that, once triggered, can have a runaway effect, with multiple, severe enterprise and national consequences. Managing cybersecurity risk for these ecosystems is incredibly challenging because of their dynamic complexity.

More information on cybersecurity risk management is available from numerous NIST documents, including SP 800-37 Revision 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy* [13] and the *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1* [16]. They reference a "risk-based approach," which enables an organization to determine the risks that are relevant to its mission throughout the operational lifecycle, and to apply appropriate resources to respond to those risks to an acceptable level. Implementation of such an approach will vary depending upon the relevant stakeholders' risk appetite, risk tolerance, and available resources.

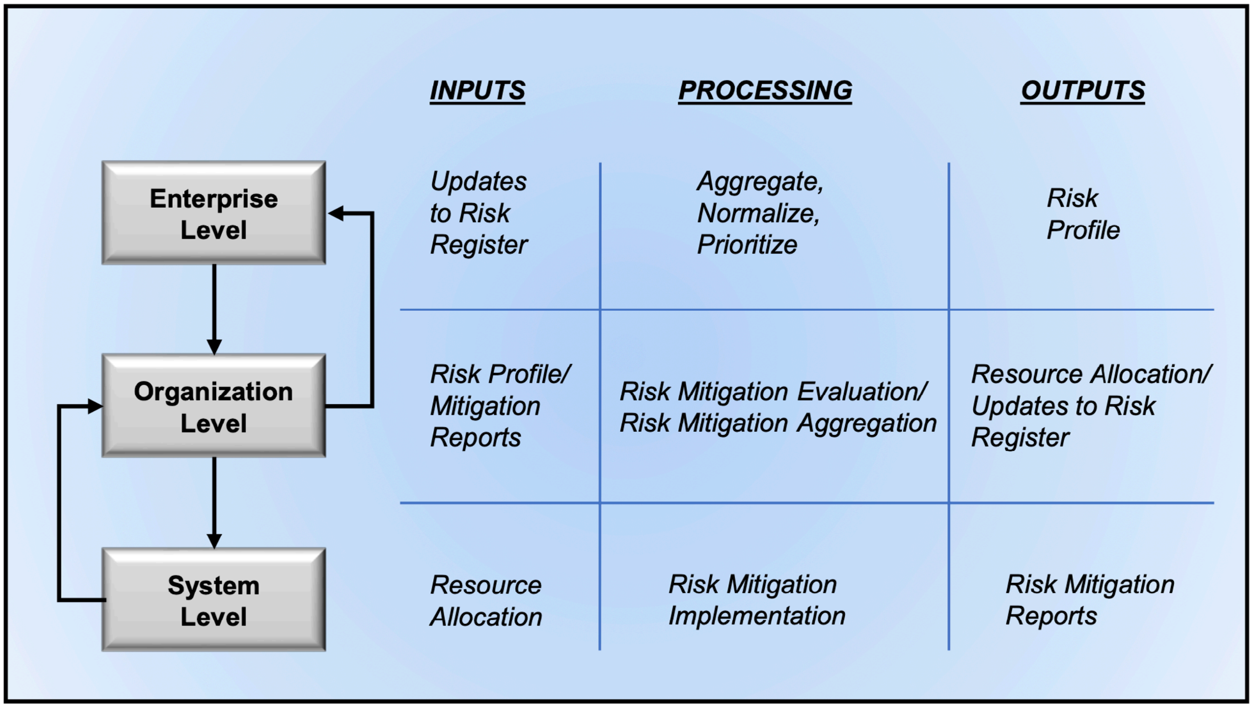
Note that while the focus of this publication is cybersecurity risk, its high-level approaches should also be relevant for privacy risk. See *NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management* for a privacy risk management approach. [17]

2.3 The Gap Between Cybersecurity Risk Management Output and ERM Input

For ERM purposes, each system should have a cybersecurity risk register, which would be primarily informed by the enterprise's cybersecurity objectives. At higher levels in the enterprise, the contents of those registers will be aggregated, normalized, and prioritized. This allows easy transfer of cybersecurity risk knowledge from cybersecurity risk management to ERM. Figure 3 highlights the flow of information. To align cybersecurity risk with enterprise risk, organizations should utilize a cybersecurity risk register for these risk management activities:

1. Aggregating risks from adversary threats and system failures that result in compromised information or control signals. *Aggregation* is the consolidation of similar or related information.
2. Normalizing information across organizational units to provide enterprise executives with information needed to measure mission, finances, and reputation exposure. *Normalization* is the conversion of information into consistent representations and categorizations.
3. Prioritizing operational risk mitigation activities by combining risk information with enterprise mission and budgetary guidance to implement appropriate responses

However, currently most organizations are not providing these in consistent, repeatable ways. Methods such as quantifying cybersecurity risk in dollars and aggregating cybersecurity risks are largely ad hoc and are not performed with the rigor used for other types of risk. Improving the risk measurement and analysis methods used in cybersecurity risk management, along with using cybersecurity risk registers, would improve the quality of the risk information provided to ERM, which promotes better management of cybersecurity risk at the enterprise level.



	INPUTS	PROCESSING	OUTPUTS
Enterprise Level	Updates to Risk Register	Aggregate, Normalize, Prioritize	Risk Profile
Organization Level	Risk Profile/ Mitigation Reports	Risk Mitigation Evaluation/ Risk Mitigation Aggregation	Resource Allocation/ Updates to Risk Register
System Level	Resource Allocation	Risk Mitigation Implementation	Risk Mitigation Reports

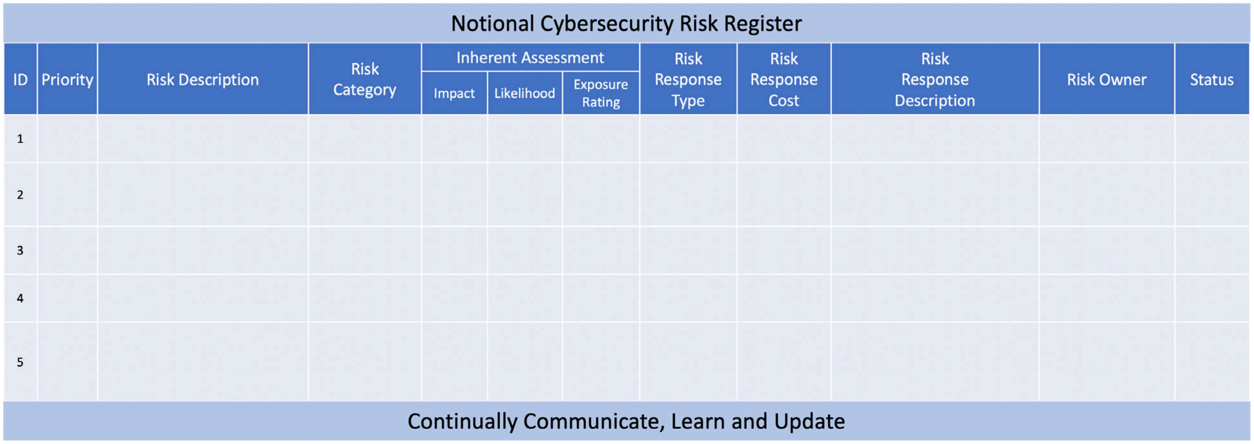
Figure 3: Information Flow Between System, Organization, and Enterprise Levels

At its core, managing cybersecurity risk is balancing the benefit of applying information and technology against the potential impact and likelihood of the consequences of that application deployed at the system, organization, or enterprise level. An enterprise that avoids all cybersecurity risk might stifle innovation or efficiencies to the point where little value would be produced. Conversely, an enterprise that applies technology without regard to cybersecurity risk might fall victim to undesirable consequences. Effectively balancing the benefits of technology with the potential consequences of a threat event will result in effective cybersecurity risk management that supports a comprehensive ERM approach. Practitioners should consider the influence of cybersecurity risks on core ERM measures including mission, finances, and reputation. They also need to take into account relevant policy decisions and regulatory impact.

According to NISTIR 8170, enterprises "develop policies to identify, assess, and mitigate adverse effects with cybersecurity dependencies across various types of enterprise risks. […] Many of these other types of risk may also have cybersecurity risk implications or be impacted by cybersecurity. Some employ different terminologies and risk management approaches to make decisions. […] Organizations may have established a unique lexicon for ERM that should be considered when communicating risks. […] This necessitates coordination with existing ERM functions on how to best incorporate and communicate cybersecurity risks at the organization and system levels." [4]

3 Cybersecurity Risk Considerations Throughout the ERM Process

Adopting the cybersecurity risk register model provides consistency throughout the ERM process, beginning with the identification of relevant risk scenarios, then providing a framework for organizing and communicating information about risk assessment, evaluation decisions, risk response, and monitoring activities from system levels to organization levels, and finally to the top-level enterprise. Figure 4 shows a notional cybersecurity risk register template. It includes many of the elements suggested by OMB Circular A-11, which states that "typically, a risk register contains a description of the risk, the impact if the risk should occur, the probability of its occurrence, mitigation strategies, risk owners, and a ranking to identify higher priority risks." [2]



Notional Cybersecurity Risk Register

ID	Priority	Risk Description	Risk Category	Inherent Assessment			Risk Response Type	Risk Response Cost	Risk Response Description	Risk Owner	Status
				Impact	Likelihood	Exposure Rating					
1											
2											
3											
4											
5											

Continually Communicate, Learn and Update

Figure 4: Notional Cybersecurity Risk Register Template

Table 2 describes each of the elements in the notional cybersecurity risk register template.

Table 2: Descriptions of Notional Cybersecurity Risk Register Template Elements

Register Element	Description
ID (Risk Identifier)	A sequential numeric identifier for referring to a risk in the risk register (e.g., 1, 2, 3)
Priority	A relative indicator of the criticality of this entry in the risk register, either expressed in ordinal value (e.g., 1, 2, 3) or in reference to a given scale (e.g., high, moderate, low)
Risk Description	A brief explanation of the cybersecurity risk scenario impacting the organization and enterprise. Risk descriptions are often written in a cause and effect format, such as "if X occurs, then Y happens".
Risk Category	An organizing construct that enables multiple risk register entries to be consolidated (e.g., using SP 800-53 Control Families: Access Control (AC), Audit and Accountability [AU]). This value is important for comparing across risk registers during the risk aggregation step of ERM.
Inherent Assessment—Impact	Analysis of the potential benefits or consequences resulting from this scenario if no additional response is provided.[11] On the first iteration of the risk cycle, this may also be considered the **initial assessment.**

[11] An inherent assessment based on the assumption that no controls are in place is usually difficult to estimate because in most environments there are already several layers of controls.

Register Element	Description
Inherent Assessment—Likelihood	An estimation of the probability, before any risk response, that this scenario will occur. On the first iteration of the risk cycle, this may also be considered the **initial assessment.**
Inherent Assessment—Exposure Rating	A calculation of the likely risk exposure based on the inherent likelihood estimate and the determined benefits or consequences of the risk. Throughout this report, the combination of impact and likelihood is referred to as *exposure*. Other common frameworks use different terms for this combination, such as *level of risk* (ISO 31000, NIST SP 800-30 Rev. 1). On the first iteration of the risk cycle, this may also be considered the **initial assessment.**
Risk Response Type	The risk response (sometimes referred to as the risk strategy or risk treatment) for handling the identified risk. Values for risk response types are listed in Table 3 and Table 4 of this document.
Risk Response Cost	The estimated cost of applying the risk response
Risk Response Description	A brief prose description of the risk response
Risk Owner	One or more parties that are responsible for managing and monitoring the selected risk response
Status	A field for tracking the current condition of this risk and any next steps

This section discusses how risk registers are used within organizations and how a risk register's contents are prioritized to serve as the basis of a risk profile. Section 4 explains what happens at the enterprise level when the risk profiles of its organizations are correlated, aggregated, normalized, and deconflicted, with the key risks compiled into the Enterprise Risk Profile (such as the Agency Risk Profile described in OMB Circular A-123 Section B1). [3]

> Appendix K of NIST SP 800-30 Revision 1 [12] describes relevant cybersecurity risk elements that might be recorded in what is called a *cybersecurity Risk Assessment Report (RAR)*, providing a detailed record of the planning and execution of evaluation of a relevant set of risks. Elements that match those described in Table 2 of this document might be added to cybersecurity risk registers, and creating a cybersecurity RAR can be considered a prerequisite to creating a cybersecurity risk register. Doing so would allow those seeking additional information about a given cybersecurity risk register entry to readily find such information recorded in the corresponding RAR.

3.1 Identify the Context

The first step in managing cybersecurity risks to the organization is understanding *context*—the environment in which the organization operates and is influenced by the risks involved. As shown in Figure 4, the context is not directly recorded in the cybersecurity risk register, but it provides important input into that register by documenting the expectations and drivers to be considered in the register's development and maintenance. The risk context includes two factors:

- **External context** involves the expectations of outside stakeholders that affect and are affected by the organization, such as customers, regulators, and business partners. These stakeholders have objectives, perceptions, and expectations about how risk will be communicated, managed, and monitored. External stakeholders may include adversaries, since they have an interest in the organization and may also affect it by instigating, exacerbating, and exploiting risk-related information.

- **Internal context** relates to many of the factors within the organization. This context includes any internal factors that influence risk management, including the organization's objectives, governance, culture, risk appetite, and policies and practices.

Several NIST frameworks begin with determining these context factors. For example, the Risk Management Framework [13] includes a *Prepare* step to identify organization strategy, management methods, and roles. Similarly, the Cybersecurity Framework [16] and Privacy Framework [17] identify in *Profiles* organization mission drivers and priorities that are used for subsequent assessment and planning.

Throughout implementation of the risk management cycle, as tracked and managed by the use of cybersecurity risk registers and risk profiles, stakeholder communications are critical. In this way, the external and internal context provide direction that enables cybersecurity risk officers[12] to identify relevant cybersecurity risks, as described in Section 3.2. Assumptions may occur at all levels of the organization, so it is important to determine internal and external stakeholders' expectations regarding risk communications, including strategic objectives, organizational priorities, decision-making processes, and risk reporting/tracking methodologies (e.g., regular risk management committee discussions and meetings).

Strategic risk direction from leadership usually includes guidance regarding risk appetite and risk tolerance, including acceptable levels of risk at the system and organization levels. Risk guidance can also include direction regarding how risk register entries should be categorized. The use of common risk categories supports aggregation of various types of risk, such as ordered by the nature of the risk (e.g., supplier risks, access management risks) or by analysis results (e.g., high risks, risks to payroll).

As cybersecurity risks are recorded, tracked, and reassessed throughout the risk lifecycle, this foundation ensures that all agree about how various types of risk will be communicated, managed, and escalated to ensure adherence to risk guidance and expectations.

3.2 Identify the Risks

The second step in Figure 2 involves identifying the comprehensive set of positive risks (from opportunities) and negative risks (from threats) and recording them in the risk register. This involves determining which events could enhance or impede objectives, including the risks entailed by failing to pursue opportunities. Note that Circular A-123 [3] requires that the risk register consider both inherent and residual risk. Those terms are described in the following way [9]:

[12] The cybersecurity risk officer has the expertise to identify relevant cybersecurity risks, versus an enterprise risk officer who would receive reports on such risks. The importance of the cybersecurity risk officer role is increasingly being recognized.

- "Inherent risk is the risk to an entity in the absence of any direct or focused actions by management to alter its severity.
- Target residual risk is the amount of risk that an entity prefers to assume in the pursuit of its strategy and business objectives, knowing that management will implement, or has implemented, direct or focused actions to alter the severity of the risk.
- Actual residual risk is the risk remaining after management has taken action to alter its severity. Actual residual risk should be equal to or less than the target residual risk."

Cybersecurity risk identification is comprised of four necessary inputs, each of which is discussed in more detail below:

- Identification of the organization's relevant assets and their valuation;
- Determination of potential information and technology opportunities that might benefit the organization, and potential threats that might jeopardize the confidentiality, integrity, and availability of those assets;
- Consideration of vulnerabilities of those assets; and
- High-level evaluation of potential consequences of risk scenarios.

3.2.1 Inventory and Valuation of Assets

The Cybersecurity Framework describes *assets* as "the data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes." [16] An asset could be a communications circuit, a staff member, or a piece of information, such as intellectual property. Potential impact on assets cannot be determined without a comprehensive asset inventory, so that inventory is often among the first inputs needed. Such an inventory should also provide a method for tracking the owner/manager of each asset and the asset's relative importance (or value).

Increasingly, many of the assets on which an organization depends are not within its direct control. External technical assets may include cloud-based software or platform services, telecommunications circuits, and video monitoring. Personnel may include the internal workforce, external service providers, and third-party partners.

3.2.2 Determination of Potential Opportunities and Threats

Cybersecurity risk is not inherently good or bad—it represents the effect of uncertain circumstances—so it is valuable to consider a broad array of potential positive and negative risks. Section 3.5.1 includes an example of an *opportunity*, which describes a condition that may result in a beneficial outcome (a *positive risk*). A *threat* represents anything that can act against an asset in a manner that can result in harm (a *negative risk*). The threat occurs due to the action of a *threat source*, which could represent a malicious person with harmful intent but could just as easily represent an unintended or unavoidable event such as a natural disaster, technical failure, or human error. Similarly, an opportunity occurs due to the action of an *opportunity source* (more often called a *source of opportunity)*, which might consume more resources and increase risk in order to generate a greater payback.

One commonly used method for identifying potential cybersecurity risk outcomes is a SWOT analysis (Strengths, Weaknesses, Opportunities, Threats). Applying a SWOT analysis helps users to identify opportunities that arise from organizational strengths (such as a well-respected software development team) and threats (such as supply chain issues) arising from organizational weakness. The use of SWOT analysis helps the organization to compare these in relationship to the context described in Section 3.1, including internal factors (the strengths and weaknesses internal to the organization), external factors (the opportunities and threats presented by the external environment), and ways in which these factors offset each other.

Numerous threat modeling techniques are available for analyzing cybersecurity-specific threats. It may be helpful to consider both a top-down approach (reviewing critical/sensitive assets for what could potentially go wrong regardless of threat source) and a bottom-up approach (considering the potential impact of a given set of threat/vulnerability scenarios). For example, the Software Engineering Institute's (SEI) OCTAVE® uses the top-down approach to help produce a catalog of potential harmful outcomes based upon the effect of various threat sources and their motives. [18] Other threat modeling techniques include Microsoft's STRIDE [19] and DREAD [20] models and MITRE's ATT&CK™ [21], a knowledge base of adversary tactics and techniques based on real-world observations. There are also numerous industry sources of cybersecurity-specific threat information, including commercial organizations and public-sector sources like the United States Computer Emergency Readiness Team (US-CERT).

Methods for identifying cybersecurity-specific opportunities are also available and could be as simple as an employee suggestion box. Industry publications such as those from commercial industry associations and from agencies such as NIST regularly provide information and ideas regarding potential innovations or advances that may represent cybersecurity opportunities.

Numerous formal methods are available for identifying opportunities, including:

- **Brainstorming**—a group innovation technique, often led by a facilitator, that elicits views from participants to identify and describe opportunities
- **Delphi**—a procedure to gain consensus from a group of subject matter experts using one or more individual questionnaires that are then collected and collated to identify opportunities to be pursued
- **Ideation**— a consistent process of observing an environment, discerning opportunities for improvement, experimenting with possible resolutions, and developing innovative solutions

The same formal methods can be used for determining other inputs, such as those described in Section 3.2.3 and Section 3.2.4.

An extensive amount of information has already been published regarding identification of internal and external threats. An important source of information regarding what could happen in the future is what already has occurred within the organization and to organizational peers. This is exemplified in a 2017 statement by the U.S. Securities and Exchange Commission (SEC): "Given the frequency, magnitude and cost of cybersecurity incidents, the Commission believes that it is critical that public companies take all required actions to inform investors about material cybersecurity risks and incidents in a timely fashion, **including those companies that are**

subject to material cybersecurity risks but may not yet have been the target of a cyber-attack [emphasis added].” [22] Essentially, in building a register of potential cybersecurity risks, the organization should consider those negative risks that have already occurred in similar organizations.

Another source of potential threat information is high-level risk assessment results from application of the NIST Cybersecurity Framework [16] and NIST Privacy Framework [17]. Each of those frameworks includes steps for creating a high-level description of the inherent conditions for a given enterprise or organization (a current-state profile), which can be assessed to determine threat scenarios.

Whatever means is used to determine potential threats, it is important to consider these in terms of both the *threat actors* (the instigators of risks with the capability to do harm) acting on the threat sources and the threat events caused by their actions.

Consideration should also be given to combinations of multiple risks. For example, if one risk in the register refers to a website outage and another risk refers to an outage of the customer help desk, there may need to be a third risk in the register that considers the likelihood and impact of an outage affecting **both** services at once. It is also important to identify cascading risks where one primary risk event may trigger a secondary and even a tertiary event. Analysis of the likelihood and impact of these first-, second-, and third-order risks is described in Section 3.3.

It is important for the cybersecurity risk officer to look out for and mitigate instances of cognitive bias in risk identification. Some common issues from bias include:

- **Overconfidence**—the tendency for stakeholders to be overly optimistic about either the potential benefits of an opportunity or the ability to handle a threat
- **Group Think**—making decisions as a group in a way that discourages creativity or individual responsibility; the Delphi Technique is helpful in circumventing this pitfall
- **Following Trends**—blindly following the latest hype or craze without detailed analysis of the specific benefit to the organization

3.2.3 Determination of Exploitable and Susceptible Conditions

The next key input to risk identification is understanding the potential conditions that enable the risk event to occur. For positive risks this involves exploring any factors (e.g., improved market share, technical advancement) that could be exploited with a beneficial result.

Consideration of negative risks is heavily influenced by examining vulnerabilities that impact the assets. It is important to consider all types of vulnerabilities in all assets, including people, facilities, and information. For the purposes of this document, think of a *vulnerability* as simply a condition that enables a threat event to occur; it could be an unpatched software flaw, a system configuration error, a person who is susceptible to malicious persuasion, or a physical condition, like a wooden structure being flammable. The presence of a vulnerability does not cause harm in itself, as there needs to be a threat present to exploit it. Moreover, a threat that does not have a corresponding vulnerability may not result in a negative risk. Identification of negative risks includes understanding the potential threats and vulnerabilities to organizational assets, which can then be used to develop scenarios describing potential risks.

3.2.4 Evaluation of Potential Consequences

The final component of risk identification is documenting the potential consequences of each risk listed in the register. Many organizations incorrectly express risks outside of their context. For example, a stakeholder might say, "I'm worried about floods" or "I'm concerned about a denial of service attack." These examples cannot be analyzed or considered without knowing the full picture. In light of the above factors, an effective example of an identified risk in cause and effect terminology might be, "If a hurricane causes a storm surge, then it could flood the data center and damage multiple critical file servers."

3.3 Analyze the Risks

In step 3 of Figure 2, each risk in the cybersecurity risk register is analyzed to estimate the likelihood that the risk event will occur, and the potential impact of the consequences described.

3.3.1 Risk Analysis Types

As described in Section 2.2.3, the informal analysis of risk factors may impair effective decision support for cybersecurity risk management. To aid in more accurate estimation, a broad array of risk analysis methodologies are available to the cybersecurity risk officer, including NIST SP 800-30 [12], International Electrotechnical Commission (IEC) 31010:2019 [23], and FAIR [24]. Types of methods for risk analysis include:

- *Qualitative analysis*, which is based on the assignment of a descriptor such as low, medium, or high. The scale used can be formed or adjusted to suit the circumstances, and different descriptions may be used for different risk. Qualitative analysis is helpful as an initial assessment or where intangible aspects of risk are to be considered.
- *Quantitative analysis*, where numerical values are assigned to both impact and likelihood. These values are based on statistical probabilities and monetarized valuation of loss or gain. The quality of the analysis depends on the accuracy of the assigned values and the validity of the statistical models used. Consequences may be expressed in terms such as financial, technical, or human impact.
- S*emi-qualitative analysis*, with qualitative categories assigned numeric values to allow for the calculation of numeric results. These values reflect only an estimate of risk, and it is important to consider the limitations and assumptions of this process.

Each of these analysis types has advantages and disadvantages, so the type performed should be consistent with the risk management context. The method(s) to be selected and under what circumstances depend on many organizational factors and might be included in the risk management discussions described in Section 3.1. While qualitative methods are commonplace, the cybersecurity risk officer may benefit from considering a more quantitative methodology, with a more scientific approach to estimating likelihood and impact of consequences. This may, for example, help to better prioritize risks or to prepare more accurate risk exposure forecasts.

3.3.2 Techniques for Estimating Likelihood and Impact of Consequences

Since one of the primary goals of cybersecurity risk management is to identify potential risks most likely to have a significant impact, accurate reflection of risk factors is critical. Fortunately, risk management has been practiced for many years and there are many effective techniques for analyzing risk in comparison with risk appetite and risk tolerance. IEC 31010 describes 17 techniques for analyzing controls, understanding consequence and likelihood, analyzing dependencies and interactions, and measuring overall risk. [23] Estimation of risk levels (or exposure) employs a combination of analysis methods. In addition to modeling techniques like those described below, understanding of likelihood and potential impact will also draw upon experimentation, investigation into previous risk events, and research into risk experiences of similar organizations.

The likelihood and impact elements of a risk can themselves be broken into subfactors. For example, consider a risk scenario where a critical business server becomes unavailable for use by an organization's financial department. The age of the server, the network on which it resides, and the reliability of its software all influence the likelihood of a failure. The impact of this scenario can also be considered through various factors. If another server is highly available through a fault-tolerant connection, the loss of the initial server may have little consequence. Other factors also impact risk analysis, such as timing. If the financial server supports an important payroll function, the impact of a loss shortly before payday may be significantly higher than it would be after paychecks are distributed. Impact may vary greatly depending on whether the server is used for archiving legacy records or for performing urgent stock trades. This illustration demonstrates that there are many considerations that go into estimating exposure and the events that can trigger them.

Calculation of multiple or cascading impacts is an important consideration, and each permutation should be included in the cybersecurity risk register. For example, while the organization might consider a risk that a telecommunications outage would result in the loss of availability of a critical web server, there may also be secondary loss events, including loss of customers from frustration with unavailable services, or penalties resulting from failure to meet contractual service levels. Analysis of cascading risks should include consideration of triggers that would lead to a secondary risk (either positive or negative).

Examples of techniques for a more scientific estimation of the probability that a risk event will occur include:

- **Bayesian Analysis**—a model that helps inform statistical understanding of probability as more evidence or information becomes available
- **Monte-Carlo**—a simulation model that draws upon random sample values from a given set of inputs, performing calculations to determine results, and then iteratively repeating the process to build up a distribution of the results
- **Event Tree Analysis**—a modeling technique that represents a set of potential events that could arise following an initiating event, from which quantifiable probabilities could be considered graphically

In considering the potential consequences of risk events, the cybersecurity risk officer should take into account both tangible (such as direct financial losses) and less tangible impacts (such as reputational damage and impairment of mission). These are connected since direct losses will affect reputation, and reputational risk events will nearly always result in risk response expenses. OMB Circular A-123 shares that "reputational risk damages the reputation of an Agency or component of an Agency to the point of having a detrimental effect capable of affecting the Agency's ability to carry out mission objectives." [3] There is a broad range of stakeholders to be considered when estimating reputational risk, including workforce, partners, suppliers, regulators, legislators, public constituents, and clients/customers.

The estimation of the likelihood and impact of a risk event should be based upon consideration of existing and planned controls. The ERM Playbook provides the following guidance:

> "Identifying existing controls is an important step in the risk analysis process. Internal controls (such as separation of duties or conducting robust testing before introducing new software) can reduce the likelihood of a risk materializing and the impact. […] One way to estimate the effect of a control is to consider how it reduces the threat likelihood and how effective it is against exploiting vulnerabilities and the impact of threats. Execution is key—the presence of internal controls does not mean they are necessarily effective." [1]

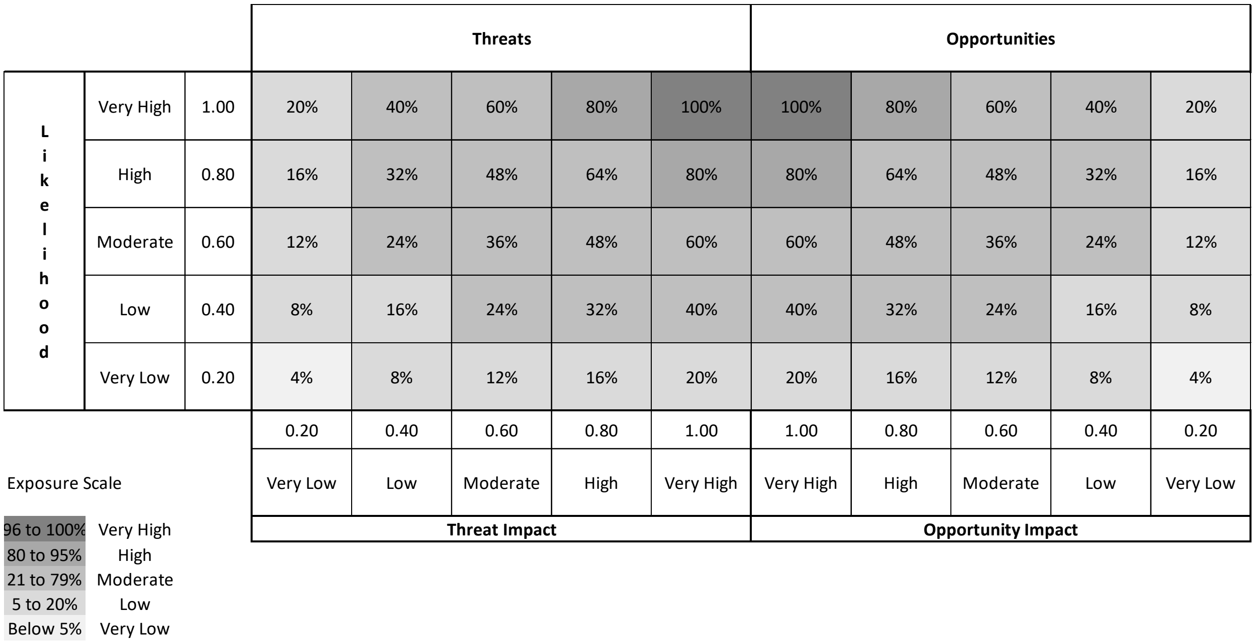
The estimated impact and likelihood for each risk are recorded in the inherent impact and likelihood columns within the cybersecurity risk register. After risk responses are determined (see Section 3.5), the analysis will be repeated in light of those risk responses, and the results will be recorded in the residual risk columns.

3.4 Prioritize Risks

Having identified and analyzed applicable risks and recorded those in the risk register, the next step involves creating a risk profile from the risk register. This is accomplished by prioritizing those risks based on exposure and selecting which ones require responses. That activity includes identifying who will make that determination. If a risk has likely impact with enterprise consequences (such as those that will impact key strategic objectives), it should be prioritized by senior enterprise leaders. Prioritizing other types of risks may be done at the discretion of the C-suite or other operating executive staff. Prioritization should include the following considerations:

- How calculation of likelihood and impact levels should be combined to determine *exposure*
- How the potential benefits of pursuing the risk activity should be considered
- When further guidance should be sought to evaluate the exposure levels, such as for risks in a particular area of focus

An example model for rating exposure and prioritizing both negative and positive risks is the Probability and Impact Matrix, shown in Figure 5. Each risk is considered in light of the likelihood and impact determined during risk analysis. The thresholds for ranges of exposure can be established and published as part of the enterprise governance model, and then used by stakeholders to prioritize each risk in the register.



			Threats					Opportunities				
Likelihood	Very High	1.00	20%	40%	60%	80%	100%	100%	80%	60%	40%	20%
	High	0.80	16%	32%	48%	64%	80%	80%	64%	48%	32%	16%
	Moderate	0.60	12%	24%	36%	48%	60%	60%	48%	36%	24%	12%
	Low	0.40	8%	16%	24%	32%	40%	40%	32%	24%	16%	8%
	Very Low	0.20	4%	8%	12%	16%	20%	20%	16%	12%	8%	4%
			0.20	0.40	0.60	0.80	1.00	1.00	0.80	0.60	0.40	0.20
Exposure Scale			Very Low	Low	Moderate	High	Very High	Very High	High	Moderate	Low	Very Low
			Threat Impact					Opportunity Impact				

96 to 100%	Very High
80 to 95%	High
21 to 79%	Moderate
5 to 20%	Low
Below 5%	Very Low

Figure 5: Probability and Impact Matrix Example

Prioritizing risk is a similar process for the risk officers at the system, organization, and enterprise levels of an organization. Upon determination of the exposure for each risk, the risks in the register should be sorted to reflect their priority. The risk priority can be determined directly from the exposure result or can be based on exposure and other factors, such as enterprise context or stakeholder objectives during the cost/benefit analysis. As the results from each system and organization's risk register are completed, these should be provided to the designated risk officers at the relevant level (i.e., system or organization) and shared with the corporate officers and high-level executives to conduct the following actions:

- Correlate common risks among the various systems
- Identify and resolve any conflicting risks
- Aggregate risks in similar categories into a more concise view
- Normalize definitions and values as recorded by various enterprise entities

Prioritization at the system and organizational levels of the enterprise is an iterative activity, since the activities of the risk oversight authority may result in additional risk guidance to the organization. In this way, these cybersecurity risks continue to be managed and tracked by the risk owner(s) at the organization level, but the enterprise risk officers stay aware of the risk inventory and the resulting exposure calculations.

The aggregated and prioritized risk register represents a risk profile that enables key executive stakeholders to stay aware of critical risks, including those that are cybersecurity related. For some organizations, this information will need to be provided to Board of Directors-level risk management committees, or to other enterprise entities that have a fiduciary duty to remain aware of and help manage risks (discussed in Section 4). In this way, enterprise leaders will have the necessary information and deliberation opportunity to consider cybersecurity exposure as factors for budget implications or corporate balance sheet reporting.

For federal agencies, this aggregated and prioritized risk register can represent or be part of an enterprise risk profile.[13] OMB Circular A-123 points out that the "primary purpose of a risk profile is to provide a thoughtful analysis of the risks an Agency faces toward achieving its strategic objectives arising from its activities and operations, and to identify appropriate options for addressing significant risks. The risk profile assists in facilitating a determination around the aggregate level and types of risk that the agency and its management are willing to assume to achieve its strategic objectives." [3] As a prioritized inventory of the most significant risks, this risk profile helps consider risks from a portfolio perspective and provides the executive leaders with an understanding of sources of uncertainty, both positive (opportunities) and negative (threats). Key risks are selected for evaluation of risk response strategies, as described next.

3.5 Plan and Execute Risk Response Strategies

The fifth step from Figure 2 is to determine the appropriate response to each risk. The goal for effective risk management, including cybersecurity risks, is to identify ways to keep risk within tolerable levels in as cost-effective a way as possible. In this stage, the cybersecurity risk officer will determine whether the exposure associated with each risk in the register is within acceptable levels. If not, that risk officer can identify and select cost-effective risk response options to achieve mission, financial, and reputational objectives.

Planning and executing risk responses is an iterative activity. The response selected for each risk will be informed by executives' guidance regarding risk appetite and risk tolerance; as the risk oversight authorities monitor the success of those responses, they will provide financial and mission guidance back to operational leaders to inform future risk management activities. In some cases, risk evaluation may lead to a decision to undertake further analysis to confirm estimates or more closely monitor results (as described in Section 3.6).

While there is some variance among the terms used by various risk management frameworks, in general there are four types of actions available for responding to negative cybersecurity risks: accept, transfer, mitigate, and avoid. These are explained in Table 3.

[13] Special treatment and communication flow germane to enterprise-level treatment of risk prioritization is discussed in Section 4 of this document.

Table 3: Response Types for Negative Cybersecurity Risks

Type	Description
Accept	Accept cybersecurity risk within risk tolerance levels without the need for additional action.
Transfer	For cybersecurity risks that fall outside of tolerance levels, reduce them to an acceptable level by sharing a portion of the consequences with another party (e.g., cybersecurity insurance). While some of the financial consequences may be transferrable, there are often consequences that cannot be transferred, like loss of customer trust.
Mitigate	Apply actions (e.g., security controls discussed in Section 3.5.1) that reduce the threats, vulnerabilities, and impact of a given risk to an acceptable level.
Avoid	Apply responses to ensure the risk does not occur. Avoiding a risk may be the best option if there is not a cost-effective method for reducing the cybersecurity risk to an acceptable level. The cost of the lost opportunity associated with such a decision should be considered as well.

Likewise, there are four generally used response types for positive cybersecurity risks, as explained in Table 4.

Table 4: Response Types for Positive Cybersecurity Risks

Type	Description
Exploit	Eliminate uncertainty to make sure the opportunity is taken advantage of.
Share	Allocate ownership to another party that is better able to capture the opportunity.
Enhance	Increase the probability and positive impact of an opportunity (e.g., invest in or participate with a promising cybersecurity technology).
Accept	Take advantage of an opportunity if it happens to present itself (e.g., hire key staff, embrace new cybersecurity technology).

Often risk response will involve creating a *risk reserve* to avoid or mitigate an identified negative risk, or to exploit or enhance an identified positive risk. A risk reserve is similar to other types of management reserves in that funding or labor hours are set aside and employed if a risk is triggered to ensure the opportunity is realized or threat is avoided. For example, the technical skill of subject matter experts to recover after a cybersecurity attack may not be available from current staffing resources. A risk reserve can also be used with the *accept* response type to address this by setting aside funds during project planning to employ a qualified third party to augment the internal incident response and recovery effort.

3.5.1 Applying Security Controls to Reduce Risk Exposure

In many cases, mitigation to bring exposure to negative cybersecurity risks to within risk tolerance levels is accomplished using security controls. The Risk Response Type column of the risk register (see Figure 2) can be updated with a response type from Table 3 and the comments field updated with the selected cybersecurity mitigation(s), such as those described in NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations* that address negative risks. This comprehensive publication provides a catalog of technical and non-technical (i.e., administrative) controls that act as “safeguards or countermeasures prescribed for an information system or an organization to protect the confidentiality, integrity, and availability of the system and its information.” It also describes privacy controls that “are the administrative, technical, and physical safeguards employed within an agency to ensure compliance with applicable privacy requirements and to manage privacy risks." [5]

Various types of controls may be applied to achieve the acceptable level of risk:

- **Preventative**: Reduce or eliminate specific instances of a vulnerability
- **Deterrent**: Reduce the likelihood of a threat event by dissuading a threat actor
- **Detective**: Provide warning of a successful or attempted threat event
- **Corrective**: Reduce exposure by offsetting the impact of consequences after a risk event
- **Compensating**: Apply one or more controls to adjust for a weakness in another control

Consider an organization that identifies several high-exposure negative cybersecurity risks, including that poor authentication practices (e.g., weak or reused passwords) could enable disclosure of sensitive customer financial information, and that employees of the software provider might gain unauthorized access and tamper with the financial data. The organization can apply several deterrent controls (documenting the applied control identifiers and any applicable notes in the risk register comments column), including warning banners and threat of prosecution for any threat actors that intentionally attempt to gain unauthorized access. Preventative controls include applying strong identity management policies and using multi-factor authentication tokens that help reduce authentication vulnerabilities. The software provider has installed detective controls that monitor access logs and alert the organization's security operations center if internal staff connect to the customer database without a need for access. Furthermore, the financial database is encrypted so it protects its data if the file system is exfiltrated.

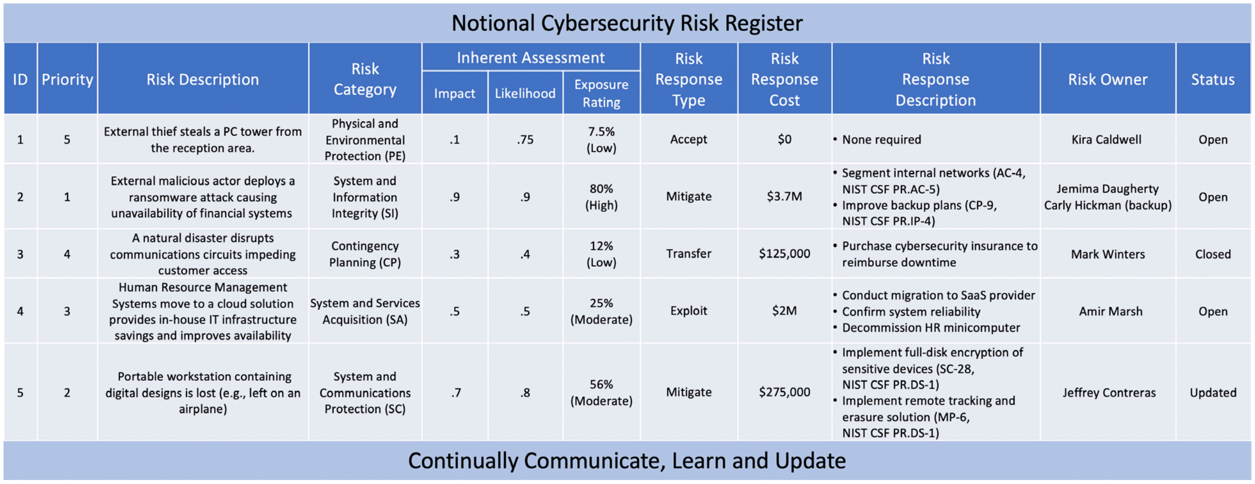
To confirm that the intended mitigation techniques are effective (and cost-effective), the application of the controls should be evaluated by a competent assessor. Because this example includes several third-party supply chain partners, that assessment will likely include multiple parties. NIST SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations* provides detailed criteria for examining application of controls and processes, testing control effectiveness, and conducting interviews to confirm that the mitigation techniques are likely to achieve their intended result. [25]

Regarding positive risk response, consider the example of an organization that has identified the positive risk of significant cost savings by moving a major financial business system to a Software-as-a-Service (SaaS) cloud solution. Analysis of the risk has determined that the opportunity would be highly beneficial to the enterprise. The solution also provides a moderate opportunity to improve availability because of the highly resilient cloud architecture. The Risk Response Type column of the risk register should also be updated using a response type from Table 4, the comment field updated to contain information pertinent to the opportunity, and the residual risk uncertainty of not realizing the opportunity calculated as discussed in Section 3.5.2.

With these controls and methods in place, and having assessed them as effective, the remaining risks can be analyzed as described in Section 3.3 to determine the residual impact, likelihood, and exposure. If the residual exposure falls within risk tolerance levels, then stakeholders can proceed in gaining the benefits of the opportunity. Each of these values is added to the risk register for enterprise reporting and monitoring.

3.5.2 Responding to Residual Risk

Section 3.2 briefly introduced the concept of residual risk. *Residual risk*, also referred to as post-mitigated risk, is risk that remains after risk responses (listed in Table 3 and Table 4) have been documented in the cybersecurity risk register and performed against the inherent risk listed in the same row, as depicted in Figure 6. The residual risk can be calculated using the same methods for calculating inherent risk discussed in Section 3.3. If the residual risk is outside the acceptable level of risk, a cost/benefit analysis should be performed. Through this process, the appropriate level of management should make a decision as to when the risk planning process will stop. Those residual risks for which no risk responses are planned must be clearly communicated to the team and management.



Notional Cybersecurity Risk Register

ID	Priority	Risk Description	Risk Category	Inherent Assessment			Risk Response Type	Risk Response Cost	Risk Response Description	Risk Owner	Status
				Impact	Likelihood	Exposure Rating					
1	5	External thief steals a PC tower from the reception area.	Physical and Environmental Protection (PE)	.1	.75	7.5% (Low)	Accept	$0	• None required	Kira Caldwell	Open
2	1	External malicious actor deploys a ransomware attack causing unavailability of financial systems	System and Information Integrity (SI)	.9	.9	80% (High)	Mitigate	$3.7M	• Segment internal networks (AC-4, NIST CSF PR.AC-5) • Improve backup plans (CP-9, NIST CSF PR.IP-4)	Jemima Daugherty Carly Hickman (backup)	Open
3	4	A natural disaster disrupts communications circuits impeding customer access	Contingency Planning (CP)	.3	.4	12% (Low)	Transfer	$125,000	• Purchase cybersecurity insurance to reimburse downtime	Mark Winters	Closed
4	3	Human Resource Management Systems move to a cloud solution provides in-house IT infrastructure savings and improves availability	System and Services Acquisition (SA)	.5	.5	25% (Moderate)	Exploit	$2M	• Conduct migration to SaaS provider • Confirm system reliability • Decommission HR minicomputer	Amir Marsh	Open
5	2	Portable workstation containing digital designs is lost (e.g., left on an airplane)	System and Communications Protection (SC)	.7	.8	56% (Moderate)	Mitigate	$275,000	• Implement full-disk encryption of sensitive devices (SC-28, NIST CSF PR.DS-1) • Implement remote tracking and erasure solution (MP-6, NIST CSF PR.DS-1)	Jeffrey Contreras	Updated

Continually Communicate, Learn and Update

Figure 6: Example Cybersecurity Risk Register

A key factor in achieving effectiveness is through the use of a cost/benefit analysis (CBA). IEC 31010 states, "Cost/benefit analysis weighs the total expected costs of options in monetary terms against their total expected benefits in order to choose the most effective or the most profitable option." [23] Through this analysis, the cybersecurity risk officer can consider the exposure factor cost (the likely cost of exposure based on the likelihood and impact of a residual risk, as recorded in the risk register) as compared with the potential cost of the risk response for that residual risk. For example, consider Risk #5 from Figure 6. The risk owner might determine that a potential breach resulting from a misplaced or stolen laptop with sensitive design plans could cost $750,000 in disclosed research and missed opportunity. The labor and software to apply full disk encryption and remote tracking on laptops containing sensitive data would cost $275,000, so the benefit outweighs the cost of the countermeasures.

Once it has been determined that residual risk will remain after the implementation of the initial risk response, the inherent risk should be closed. As is generally done, the residual risk should be moved to a primary position on the risk register, prioritized according to the methods discussed in Section 3.4. The purpose of this move is to focus attention on this risk. Once moved to the inherent risk position, the risk response should be reviewed and updated, if necessary. If a risk response was also entered into the risk register at the time the residual risk was identified, it should be reviewed for applicability and determined if it is the better response or if the two responses should be merged, blended, or completely redrafted.

Upon approval of the risk response for each risk description and determination of one or more accountable risk owners, the risk register is updated to reflect that information.

Federal agencies develop *a plan of action and milestones* for each system to document the risk responses being planned for its residual risks. A plan of action and milestones "identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones." It also "describes the measures planned to correct deficiencies identified in the controls […] and to address known vulnerabilities or security and privacy risks. The content and structure of plans of actions and milestones are informed by the risk management strategy developed as part of the risk executive (function)…." For more information, see NIST SP 800-37 Revision 2. [13]

3.5.3 When a Risk Event Passes Without Triggering the Event

Risk responses often will evolve as opportunities and threats evolve. This is similar to the "Cone of Uncertainty" described in project management study—over time, additional understanding about an identified risk will come to light. One mitigation technique for these types of risk factors is the use of risk reserves introduced in Section 3.5. If this risk response is selected, it is critical that the risk owners collaborate with the acquisition or procurement teams and budget owners. With appropriate budget planning, risk reserves can be released after the risk period has expired, and the funds can be used to exploit a positive risk.

While many industry-based enterprises can return the unused funds to shareholders or pay down corporate debt, for government agencies unused reserve is more difficult to use without preplanning. Most government procurement cycles are rigid based on the government fiscal year. Identified opportunities can be planned for in government procurement cycles as "optional" tasking or purchases. For example, if the information technology (IT) refresh budget for the current fiscal year only allows for the purchase of half the required materials, an option can be created for the other half of the materials (but not funded at the time of the contract award). When the cybersecurity risk officer liberates the risk reserve after the chance of the negative risk occurring has passed, the positive risk can be exploited by exercising the already awarded option that lacked the initial funding when the contract was awarded. Exercising an option can be trivial (often 30 days or less) when compared to the long lead time for contract procurements. See the "Integrate and Align Cybersecurity and Acquisition Processes" section of NIST IR 8170 [4] for more information on preplanning for government agencies.

3.6 Monitor, Evaluate, and Adjust

The risk register is the formal communication vehicle for ERM. From the first understanding of internal/external context to discussion and authorization of risk response, continual dialogue needs to occur among all relevant stakeholders. While such discussion often occurs within a given business unit or subordinate organization, the enterprise will benefit from frequent and transparent communication regarding risk options, decisions, changes, and adjustments. The evolving cybersecurity risk registers and profiles provide a formal method of communicating institutional knowledge and decisions regarding cybersecurity risks and their contributions to ERM.

3.6.1 Continuous Risk Monitoring

Because cybersecurity risks and their inherent impact on other risks frequently change, enterprise risk conditions should be continually monitored to ensure they remain within acceptable levels. For example, such monitoring could determine when negative cybersecurity risks for a system are approaching the risk tolerance level, triggering a review of the risk that could result in a higher priority for the risk and the implementation of additional risk responses. Risk monitoring benefits from a positive risk-aware culture within the enterprise. Such a culture leads to a cohesive, team-based approach to monitoring and managing risks. Supporting such a culture includes proactive activities, such as the examples listed in Table 5.

Table 5: Examples of Proactive Activities

Activity Example	Description
Cultural Risk Awareness	Encourage employees to look for cybersecurity risk issues before they become significant.
Risk Response Training	Train employees and partners on enterprise strategy, risk appetite, and selected risk responses.
Risk Management Performance	Discuss the impact of cybersecurity risk on every employee and partner, and why effective management of risks is an important part of everyone's job.
Risk Response Preparedness	Conduct exercises to provide practical and meaningful experience in recognizing, reporting, and responding to cybersecurity risk scenarios.
Risk Management Governance	Remind staff of organizational policies and procedures that are established to help improve risk awareness and response.
Risk Transparency	Enable an environment where employees and partners may openly and proactively report potential risk situations without fear of reprisals.

Each risk in the register is assigned a risk owner, as described in Table 2. The risk owner is accountable for applying the priority described in Section 3.4 to select and apply appropriate risk responses considering business objectives and performance targets. ERM policies and processes should specify the approved frequency and methods for monitoring, evaluating the effectiveness of, and adjusting risk responses.

An element of risk monitoring is determining and publishing accountable risk management roles throughout the enterprise, including those in organizations. The relationships among these entities should be communicated clearly, such as how a formal enterprise risk committee may be informed by subordinate risk councils or working groups. They can help ensure crosscommunication among other groups that support risk management, such as human resources, legal, auditing, and compliance management.

While this report focuses on cybersecurity risks as they contribute to ERM, many enterprise risks are interdependent. A common industry example: while cybersecurity risk and credit risk are different elements of the ERM portfolio, it is quite possible that a cybersecurity breach could result in a credit downgrade. Because of these interdependencies, it is important that enterprise managers collaborate and communicate, and do not treat information and technology risks as isolated issues.

If the risk response for a given risk (or set of risks) requires a management funding or schedule reserve, specific monitoring and measurement milestones can be included in the associated risk response plan. The risk owner then can identify performance measures or trends (e.g., deliverable artifacts or software development achievements) that represent milestones in addressing the risk. Having achieved those milestones may trigger release or repurposing of the associated management reserve resources. This process can be especially helpful in enterprises that manage funding by periodic increments, such as fiscal years. In such an enterprise, it can be beneficial for the monitoring process to identify that a given risk is unlikely to occur, giving the risk owner sufficient time to reallocate those reserves before other funding deadlines occur.

3.6.2 Key Risk Indicators

One method for improving monitoring is through the use of Key Risk Indicators (KRIs) at various levels. KRIs represent specific metrics that can either provide leading indicators of future risk issues or lagging indicators that track the success or failure of previous risk initiatives. Cybersecurity KRIs can be positive, such as the number of critical business systems that require strong authentication, or negative, such as the number of severe customer disruptions in the last 90 days. Additional metrics may include compliance measures, performance targets for positive risk, and objectives for balancing risk and reward.

Based on risk metrics monitoring and reporting, the enterprise and subordinate levels need to identify and provide processes for reassessing risk. Changes in the risk landscape, including those from modifications in industry regulation, may require periodic review of risk appetite, tolerance, and capacity.

Based upon an ongoing review of cost/benefit analysis, the enterprise should continually monitor the risk register, including those entries that may have been deferred or declined in the past. By maintaining the continual refreshment of the risk register and risk profile artifacts described in this report, this monitoring and adjustment activity will be straightforward. An important element of this monitoring and adjustment activity is the need to communicate and benefit from lessons learned from previous practice and actual risk events. By examining adverse events/losses from the past and by reviewing missed opportunities (including those missed due to a risk-averse mindset), the enterprise can improve the risk management model.

Some of the same types of quantitative and semi-qualitative methods described above may be helpful in conducting such analyses. For example, quantitative KRIs might track customer downtime and could support root-cause analysis of trends to avoid fines from a missed customer service level agreement. Similarly, monitoring the successful implementation of a data loss prevention tool could quantify sensitive messages that had been quarantined, with successful mitigation of financial and reputational losses. These observations help identify where processes could have been improved or errors might have been avoided, supporting opportunities for training and for updating procedures.

3.6.3 Continuous Improvement

A risk-aware culture should be looking for chances to improve—reinforcing effective practices and adjusting to correct deficiencies. While all should be accountable and held responsible for any negligent activity, there is value in fostering a community that is pursuing opportunities within risk appetite levels while also being prepared for and continually thwarting threat actors that would exploit vulnerabilities.

The Plan-Do-Check-Act approach is a well-known model for achieving ongoing effectiveness of any process, and it applies well to cybersecurity risk management. Earlier in Section 3, this report describes methods for the Plan and Do elements—essentially planning based on enterprise direction and then doing activities to achieve an acceptable level of cybersecurity risk. Section 3.6.1 describes the Check element, where the cybersecurity risk officer determines whether the intended activities accomplished objectives and to what extent. The remaining element, Act, helps determine what should be done next to adjust and improve.

An element of adjustment relates to learning from open and transparent feedback throughout ERM communications processes. Figure 2 points out that communication takes place throughout the risk management life cycle, including risk direction, identification of threats and opportunities, analysis of resulting exposure, and implementation of responses, and the risk register is the vehicle for all those communications. Each of these activities provides a chance for feedback and documenting lessons learned to drive subsequent improvement. By staying aware of changes to the risk landscape, such as through subscriptions to community alerts (e.g., InfraGard, US-CERT, commercial threat feeds), industry and public-sector workshops, and publications (e.g., NIST publications and postings), cybersecurity risk officers can adjust risk identification and assessment processes for emerging and evolving threats and opportunities.

As risk register and profile information is collected and aggregated (described in detail in Section 4), leaders can provide feedback to improve processes and adjust risk criteria. Perhaps a new online service offering provides an opportunity to innovate, so leadership has directed the organization to take a little more risk and potentially improve revenues. Alternatively, perhaps other business units have suffered some cybersecurity attacks and stakeholders have re-evaluated the likelihood and impact criteria. In either case, the ability to adjust effective management of cybersecurity risk supports broad enterprise objectives as part of ERM.

4 Cybersecurity Risk Management as Part of a Portfolio View

The objective of ERM deliberations and related decisions is to provide resource allocation and mission guidance to enterprises and to prepare prudent risk position disclosures to appropriate stakeholders. OMB Circular A-123 recommends a portfolio view of risk that "provides insight into all areas of organizational exposure to risk […] thus increasing an Agency's chances of experiencing fewer unanticipated outcomes and executing a better assessment of risk associated with changes in the environment." [3] This portfolio view is valuable to all enterprises, public and private. While many ERM processes are written from a commercial perspective, agency "enterprises" operate differently but experience similar financial and reputation risk impacts. In fact, the federal budget presents the same income, capital, and cash flow statements as public companies. Likewise, federal ERM best practices and guidelines are like those of commercial practice.

To make resource and guidance decisions commensurate with enterprise risk, ERM officials require subordinate organizations' risk registers and profiles to be normalized and aggregated into an Enterprise Risk Register with mission, financial, and reputation consequences (described in Section 4.1). NIST often references a strategic view at the enterprise level, supported by business units that implement that strategy, in turn supported by information and systems that enable tactical implementation of the enterprise objectives. That view is illustrated by the Information and Decision Flows diagram from the NIST Cybersecurity Framework [16] shown in Figure 7.

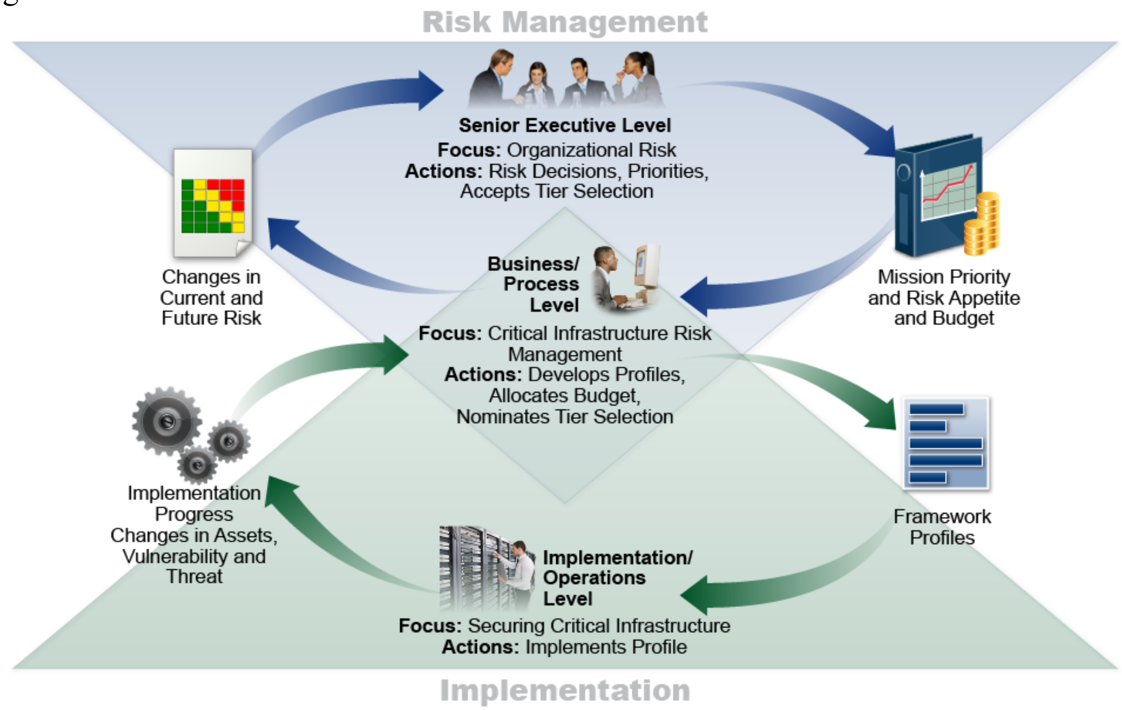

Risk Management
Senior Executive Level
Focus: Organizational Risk
Actions: Risk Decisions, Priorities, Accepts Tier Selection
Changes in Current and Future Risk
Mission Priority and Risk Appetite and Budget
Business/ Process Level
Focus: Critical Infrastructure Risk Management
Actions: Develops Profiles, Allocates Budget, Nominates Tier Selection
Implementation Progress Changes in Assets, Vulnerability and Threat
Framework Profiles
Implementation/ Operations Level
Focus: Securing Critical Infrastructure
Actions: Implements Profile
Implementation

Figure 7: Notional Information and Decision Flows Diagram from NIST Cybersecurity Framework

4.1 Applying the Enterprise Risk Register

As risk information is transmitted from lower tiers of the organization up to higher tiers, each tier's risk register contains the pertinent information to create a prioritized risk profile for the tier immediately above. Subordinate organizations' impacts may be different or similar, conflicting, overlapping, or unavailable, and must be properly combined by financial and mission analysis at the tier immediately above the reporting organization. While cost impact and risk weighted assets may be determined at lower levels, cash flow and capital implications can only be normalized and aggregated in the Enterprise Risk Register by enterprise fiduciaries (e.g., Chief Financial Officers [CFOs]). Similarly, enterprise mission impacts must be aggregated and expressed by those senior executives most directly accountable to stakeholders.

Consolidation of these organizational risk profiles into the enterprise risk profile supports the governance and management of risk in several ways:

- **Prioritization**—Executives can evaluate priority from a portfolio perspective based on the various impact factors described. While the same risks may post a differing priority at subordinate levels, enterprise priority reflects overall mission, financial, and reputational impact.
- **Risk Category**—Enterprise leaders select a set of categories most relevant to the industry the enterprise represents. For example, banks often draw from Basel II guidance [26] to organize risk into credit, market, and operational risk, where risks such as reputation, counterparty, and political risk are embedded in the operational risk category.
- **Financial Impact**—Various risk scenarios are converted into actual capital and operational expenses, enabling executive leaders to conduct a fiscally responsible cost/benefit analysis in light of the recommended strategies for risk response.
- **Reputation Impact**—While subordinate risk registers describe risk scenarios, including those that may impact reputation, executive leaders record evaluation of consequences on the *enterprise's* reputation. This also supports consideration of other downstream impacts, such as financial losses or credit risk, likely to result from damage to reputation.
- **Mission Impact**—Executive leaders record evaluation of consequences on the overall ability for the enterprise to conduct its mission and achieve strategic objectives.
- **Risk Owner**—This supports assignment of accountable actions through enterprise roles and responsibilities, in turn enabling monitoring metrics, performance reporting, and ongoing oversight by enterprise leadership.

Table 6 provides an example Enterprise Risk Register reflecting this portfolio evaluation of the various organizational risk profiles. This information, having been populated and prioritized, can directly support creation of an Agency or Corporate formal Risk Profile.

Table 6: Example Enterprise Risk Register

ID	Priority	Risk Description	Risk Category	Inherent Assessment					Risk Response	Risk Owner	Status
				Financial Impact	Reputation Impact	Mission Impact	Likelihood	Exposure Rating			
1	5	Retiring staff lead to personnel shortages	Operational Risk	OpEx M CapEx L	L	M	M	M	• Improve hiring diversity • Improve employee benefits packages per recent survey and discussions	Human Resources Department	Open
2	6	A strategic opportunity to hire a globally recognized technologist leads to establishing a new satellite communications initiative	Operational Risk	OpEx M CapEx L	H	M	M	M	• Allocate funds for compensation package • Initiate strategic recruiting plan	Human Resources Department	Open
3	1	A social engineering attack on enterprise workforce leads to a breach or loss	Cyber Information Security Risk	OpEx M CapEx L	H	M	H	H	• Update corporate IT security training • Implement phishing training service • Update email security products per recommendations from IT Risk Council	CISO	Open
4	3	A security event at a third-party partner results in data loss or system outage	Cyber Information Security Risk	OpEx L CapEx L	H	H	M	M	• Chief Financial Officer and Chief Executive Officer to agree on plans for likely secondary financial impact from the high-rated reputational risk impact • Update procurement contract requirements to include protection, detection, and notification clauses per 11/3/2019 report from Legal Dept • Implement 3rd Party Partner Assessment for Tier 1 providers per CIO & CISO recommendations	Procurement	Open
5	7	Sales reduction due to tariffs leads to reduced revenues	Financial Risk	OpEx M CapEx L	L	L	L	L	• Increase marketing in target areas • Ensure competitive pricing in target markets	VP Sales	Open
6	8	Customer budget tightening results in reduced revenue and profits	Financial Risk	OpEx M CapEx L	L	L	M	M	• Implement customer surveys to better forecast potential changes in purchasing patterns • Improve cost-cutting measures to offset reductions and maintain profitability	VP Sales	Open
7	9	Failure to innovate results in market share erosion	Strategic Risk	OpEx M CapEx M	M	L	M	L	• Approve CIO proposal to increase Internal Research & Development (IRAD) funding by 10% to spur and expand internal innovation • Update technical training to include design thinking methodologies	VP, Product Development	Open

ID	Priority	Risk Description	Risk Category	Inherent Assessment					Risk Response	Risk Owner	Status
				Financial Impact	Reputation Impact	Mission Impact	Likelihood	Exposure Rating			
									• Implement customer surveys in target areas to ensure adequate product coverage		
8	2	Company intellectual property data is disclosed through employee error or malicious act	Cyber Information Security Risk	OpEx M CapEx M	H	H	M	M	• Review employee background screening controls and improve, if necessary • Update corporate security training to reinforce the need for diligence • Implement data loss prevention tools per CISO recommendation	CISO	Closed
9	10	A flaw in product quality leads to reputational damage, reducing sales	Reputational Risk	OpEx M CapEx M	H	H	L	L	• Update continuous improvement process • Implement Baldrige Excellence Framework • Update external provider quality standards	VP, Product Development	Open
10	4	A regulatory compliance failure exposes the company to fines, penalties, and legal fees	Compliance Risk	OpEx M CapEx L	H	L	M	M	• Create & maintain a centralized register of compliance requirements • Update employee training based on updated understanding of corporate requirements • Review business impact assessment (BIA) templates to ensure that information and technology requirements include regulatory and contractual obligation criteria	Legal Dept.	Open

Table 7 describes each of the elements in the example Enterprise Risk Register.

Table 7: Descriptions of Example Enterprise Risk Register Elements

Register Element	Description
ID (Risk Identifier)	A sequential numeric identifier for referring to a risk in the risk register (e.g., 1, 2, 3)
Priority	A relative indicator of the criticality of this entry in the risk register, either expressed in ordinal value (e.g., 1, 2, 3) or in reference to a given scale (e.g., high, moderate, low). Note that this prioritization may differ from similar risks in individual risk profiles from subordinate organizations.
Risk Description	A brief explanation of the cybersecurity risk scenario impacting the enterprise

Register Element	Description
Risk Category	An organizing construct that helps to evaluate similar types of risk at the enterprise level. Categories also help with consolidation and normalization of information from subordinate risk registers. Organizations draw from many available taxonomies of risk categories; these examples use the taxonomy described in the US Government Federal ERM Playbook [1].
Inherent Assessment—Financial Impact	Analysis of the financial potential benefits or consequences resulting from this scenario. While this element could be quantitative, at the enterprise level it is often qualitative (e.g., high, moderate, low). Financial considerations may be expressed as (1) capital expenditures (CapEx) that represent a longer-term business expense such as property, facilities, or equipment; and (2) operating expenses (OpEx) that support day-to-day operations.
Inherent Assessment—Reputation Impact	Analysis of the potential benefits or consequences that the scenario might have on the stature, credibility, or effectiveness of the enterprise. Some enterprises perform a formal sentiment analysis using commercial services or other technical tools to support assessment.
Inherent Assessment—Mission Impact	Analysis of the potential benefits or consequences that the scenario might have on the ability of the enterprise to successfully achieve mission objectives
Inherent Assessment—Likelihood	An estimation of the probability, before any risk response, that this scenario will occur
Inherent Assessment—Exposure Rating	A calculation of the likely risk exposure based on the inherent likelihood estimate of probability and the determined mission, financial, and reputational benefits or consequences of the risk
Risk Response	A brief prose description of the selected risk response strategy
Risk Owner	One or more parties that are responsible for managing and monitoring the selected risk response
Status	A field for tracking the current condition of this risk and any next steps

Reputation exposure is similarly determined in the Enterprise Risk Register (e.g., by the Chief Risk Officer [CRO]) by combining high-impact attacks, enterprise sector, and consequences with histograms (trend) analysis of stakeholder sentiment (for each stakeholder type). The Enterprise Risk Register reflects impact and likelihood assessments for mission, financial, and reputation exposures. At the top enterprise tier, ERM officials have the prerogative to add their own judgment of likelihood and impact. While the ERM process helps drive discussion and calculation of likely risk scenarios, recent natural disasters have demonstrated that actual consequences can far exceed initial loss expectations. Enterprise executives should continually observe industry trends and actual occurrences to readjust predictions and reserves based on a changing risk landscape. Enterprise Risk Registers should also reflect comparable occurrence incidents and trends for the subject enterprise and peer organizations.

4.2 Information and Decision Flows in Support of ERM

Senior enterprise executives provide risk guidance (including advice regarding mission priority, risk appetite and tolerance guidance, and capital and operating expenses to manage known risks) to the organizations within their purview. Based on those governance structures, organization managers achieve their business objectives by managing and monitoring processes that properly balance the risks and resource utilization with the value created by information and technology. The left side of Figure 8 represents important information flow in support of ERM. Prioritized risk profile information is developed at each level and also normalized and summarized for enterprise consideration. Through reports of success, challenges, opportunities, and increased risk, as reflected in risk registers, enterprise-level managers can manage, monitor, and report potential implications to (and from) the risk profile with a portfolio perspective.

Enterprise-focused activities do not relieve risk owners of their responsibilities within their own organizations. There is a well-known phrase: “Think globally, act locally.” While it was not coined to support cybersecurity risk, the notion applies. Individual cybersecurity risks are managed and tracked within each organization and will likely be handled differently in each. Each organization risk officer develops its assessment of risks (through the risk profile) relative to its business objectives and risk tolerance. Enterprise risk officers then consider the overall set of risks to determine how the composite set compares to the overall risk appetite. Those enterprise risk officers might maintain the current course of action or take additional steps to reduce risk. They might determine that the overall risk is significantly less than the enterprise risk appetite and decide to motivate organization risk officers to accept greater risk in targeted areas in order to enhance that organization’s value.

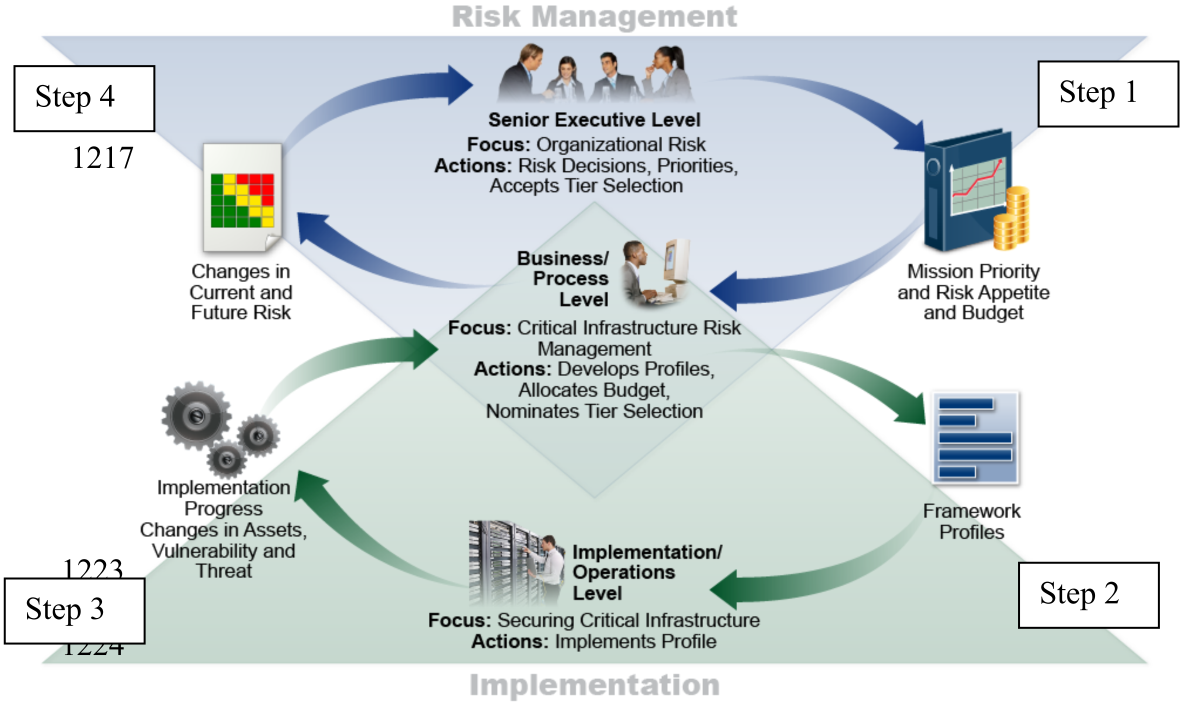

Risk Management
Step 4
Step 1
Senior Executive Level
Focus: Organizational Risk
Actions: Risk Decisions, Priorities, Accepts Tier Selection
Changes in Current and Future Risk
Mission Priority and Risk Appetite and Budget
Business/ Process Level
Focus: Critical Infrastructure Risk Management
Actions: Develops Profiles, Allocates Budget, Nominates Tier Selection
Implementation Progress Changes in Assets, Vulnerability and Threat
Framework Profiles
Step 3
Step 2
Implementation/ Operations Level
Focus: Securing Critical Infrastructure
Actions: Implements Profile
Implementation

Figure 8: Notional Information and Decision Flows Diagram with Steps Numbered

The following process considers the information and decision flows depicted in Figure 8.

- **Step 1** involves risk direction. Senior executive leaders (e.g., public officials such as department secretaries or agency directors and immediate subordinate executives, corporate boards and their executive fiduciaries) consider the relative importance of various environmental factors. External factors may include political, economic, social, technological, legal, and environmental considerations; internal factors include the enterprise’s capital assets, people, processes, and technology. These leaders may determine how those factors contribute to potential exposure, such as mission, finances, and reputation. With the factors in mind, senior executive leaders determine risk acceptance levels and resource allocations for all risk types, commensurate with impact and likelihood, balanced among and between all enterprise risk exposures.

The result is mission and financial guidance to operational leaders at the business/process level, including direction regarding available budget ceilings for cybersecurity CapEx and OpEx, and objectives for free cash flow. Direction regarding risk appetite will vary by enterprise. As with risk analysis, risk appetite may be communicated using qualitative, quantitative, and semi-qualitative methods. It could be expressed as "low appetite" or "high appetite" for various risk categories, or expressed numerically, such as through a target percentage, a range of permissible downtime or financial losses, or a ceiling (e.g., up to $1,000,000 expense.)

- In **step 2**, organizational managers receive this guidance and perform similar analysis for any subordinate organizations. They then conduct cybersecurity risk management activities as described in Section 3. One process that these managers may apply is the NIST Cybersecurity Framework itself. [16] Based on five Functions—Identify, Protect, Detect, Respond, and Recover—that organize basic cybersecurity activities, that model can assist managers with framing, assessing, managing, responding to, and reporting risks within the business unit and in support of enterprise objectives. The organization can use one or more Target State Profiles (the organizing principles for control selection) that express desired cybersecurity risk management outcomes. Implementation and operation staff then apply those principles to their systems through the Risk Management Framework (RMF) or other mechanisms. [13]

- In **step 3**, as risk is managed at the system level in accordance with organizational direction, risk acceptance and monitoring results are provided to the organization stakeholders. The risk determinations, decisions, and status are reported through the organizational risk register and adjusted as necessary (see Section 3.6).

- In **step 4**, high-level executives without fiduciary reporting requirements (organization) and corporate officers with fiduciary reporting requirements (enterprise) respectively act upon risk registers, aggregating the information and normalizing results. The risk categories facilitate normalization and reporting. Through this process of collating, aggregating, normalizing, and deconflicting risk register information, the enterprise risk officers are able to:

  - Report understanding of actual and potential risks from threats and system failures to enterprise information and technology

  - Normalize risk management across the enterprise. For example, if different exposure scales were used in two business units, a "high risk exposure" in one may represent a "moderate risk exposure" under the same conditions in another. Organizations may consider using the same enterprise-level risk lexicon and criteria for consistent messaging as they report risks upwards through the enterprise.

  - Provide enterprise executives with information to measure potential exposure on mission, finances, and reputation

  - Inform operational risk mitigation activities, to relate these to enterprise mission and budgetary guidance to prioritize and implement appropriate responses

  - Produce enterprise-level risk disclosures for required filings and hearings, or for formal reports as required (e.g., after a significant incident)
  - Maintain a risk profile for use in disclosures, to include exposure determination process and result, recent trends of enterprise improvement, peer trends, and contingency strategies to inform periodic and incident-driven disclosures

Information gained and adjustments to priority, risk appetite, and budget are then provided through the next iteration of Step 1.

While the steps above describe aggregation of risk registers and risk profiles at the enterprise level, similar activities occur throughout the organization. System risk registers may be prioritized into system risk profiles, which may then be aggregated into risk registers at the next level, such as department or organization. As these are prioritized, they become organizational risk profiles that support an aggregated portfolio risk register.

The steps discussed above generate risk reports. From NISTIR 8170, regarding federal agencies: “Reports often need to be distributed to a variety of audiences, including business process personnel who manage risk as part of their daily responsibilities; senior executives who approve and are responsible for agency operations and investment strategies based on risk, other internal units; and external organizations. This means that reports need to be clear, understandable, and vary significantly in both transparency and detail, depending on the recipient and report requirement. Furthermore, reporting timelines need to match expectations of the receiving parties in order to minimize the time between the measurement of risk and delivery of the report. A standardized reporting format can assist agencies in meeting multiple cybersecurity reporting needs.” [4]

4.3 Conclusion

Cybersecurity events can have consequences that compromise the integrity of financial statements (Income Statement, Balance Sheet, Cash Flow), assurance statements[14], and risk narratives in quarterly reports. They certainly impact reputation among different stakeholders (shareholders, clients, public, partners). Board and Enterprise risk officers’ recognition and attention to these and other enterprise vulnerabilities may become a demonstration of “Duty of Care” as the last line of protection for legal and regulatory risk.

Through the mission-based portfolio approach outlined in this section, senior executives can ensure that individual cybersecurity risks at the system level may be collected and analyzed for their alignment with and impact on enterprise strategic objectives. This collective understanding helps enterprise leaders to stay aware of and assess substantial cybersecurity risk changes, review risk and performance results, and continually pursue improvement within the broader ERM.

[14] Risk assessments directly inform annual assurance statements regarding the effectiveness of management controls (including system controls) both in public and private sector. This is because they apply the same best practices and standards for risk management and internal controls. Per OMB Circular A-123 for government, assurance statements are directly informed by risk analysis in a broad array of areas, including financial and non-financial.

References

[1] Chief Financial Officers Council (CFOC) and Performance Improvement Council (PIC) (2016) Playbook: Enterprise Risk Management for the U.S. Federal Government. Available at https://cfo.gov/wp-content/uploads/2016/07/FINAL-ERM-Playbook.pdf

[2] Office of Management and Budget (2019) Preparation, Submission, and Execution of the Budget. (The White House, Washington, DC), OMB Circular No. A-11, December 18, 2019. Available at https://www.whitehouse.gov/wp-content/uploads/2018/06/a11.pdf

[3] Office of Management and Budget (2016) OMB Circular No. A-123, Management's Responsibility for Enterprise Risk Management and Internal Control. (The White House, Washington, DC), OMB Memorandum M-16-17, July 15, 2016. Available at https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2016/m-16-17.pdf

[4] Marron J, Pillitteri V, Boyens J, Quinn S, Witte G, Feldman L (2020) Approaches for Federal Agencies to Use the Cybersecurity Framework. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8170. https://doi.org/10.6028/NIST.IR.8170

[5] Joint Task Force Transformation Initiative (2013) Security and Privacy Controls for Federal Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53, Rev. 4, Includes updates as of January 22, 2015. https://doi.org/10.6028/NIST.SP.800-53r4

[6] International Organization for Standardization (ISO) (2015) Quality management systems — Fundamentals and vocabulary. ISO 9000:2015. https://www.iso.org/standard/45481.html

[7] International Organization for Standardization (ISO) (2009) Risk management – Vocabulary. ISO Guide 73:2009. https://www.iso.org/standard/44651.html

[8] Stine KM, Kissel RL, Barker WC, Fahlsing J, Gulick J (2008) Guide for Mapping Types of Information and Information Systems to Security Categories. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-60, Vol. 1, Rev. 1. https://doi.org/10.6028/NIST.SP.800-60v1r1

[9] Committee of Sponsoring Organizations (COSO) of the Treadway Commission (2017) Enterprise Risk Management—Integrating with Strategy and Performance, Executive Summary. Available at https://www.coso.org/Documents/2017-COSO-ERM-Integrating-with-Strategy-and-Performance-Executive-Summary.pdf

[10] International Organization for Standardization (ISO) (2018) Risk management—Guidelines. ISO 31000:2018. https://www.iso.org/standard/65694.html

[11] U.S. Government Accountability Office (GAO) (2014) Standards for Internal Control in the Federal Government. https://www.gao.gov/assets/670/665712.pdf

[12] Joint Task Force Transformation Initiative (2012) Guide for Conducting Risk Assessments. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-30, Rev. 1. https://doi.org/10.6028/NIST.SP.800-30r1

[13] Joint Task Force (2018) Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-37, Rev. 2. https://doi.org/10.6028/NIST.SP.800-37r2

[14] Joint Task Force Transformation Initiative (2011) Managing Information Security Risk: Organization, Mission, and Information System View. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-39. https://doi.org/10.6028/NIST.SP.800-39

[15] Forum of Incident Response and Security Teams (FIRST) (2019) Common Vulnerability Scoring System version 3.1 Specification Document, Revision 1. https://www.first.org/cvss/v3-1/cvss-v31-specification_r1.pdf

[16] National Institute of Standards and Technology (2018) Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. (National Institute of Standards and Technology, Gaithersburg, MD). https://doi.org/10.6028/NIST.CSWP.04162018

[17] National Institute of Standards and Technology (2020) NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management, Version 1.0. (National Institute of Standards and Technology, Gaithersburg, MD). https://www.nist.gov/privacy-framework/privacy-framework

[18] Software Engineering Institute (2007) Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process. (Software Engineering Institute, Pittsburgh, PA), Technical Report CMU/SEI-2007-TR-012. https://resources.sei.cmu.edu/asset_files/TechnicalReport/2007_005_001_14885.pdf

[19] Shostack A (2007) STRIDE chart. (Microsoft, Redmond, WA), September 11, 2007. Available at https://www.microsoft.com/security/blog/2007/09/11/stride-chart/

[20] Microsoft (2018) Threat modeling for drivers. (Microsoft, Redmond, WA), June 26, 2018. Available at https://docs.microsoft.com/en-us/windows-hardware/drivers/driversecurity/threat-modeling-for-drivers

[21] The MITRE Corporation (2019) ATT&CK. Available at https://attack.mitre.org

[22] U.S. Securities and Exchange Commission (SEC) (2018) Commission Statement and Guidance on Public Company Cybersecurity Disclosures. https://www.sec.gov/rules/interp/2018/33-10459.pdf

[23] International Electrotechnical Commission (IEC) (2019) Risk management – Risk assessment techniques. IEC 31010:2019. https://www.iso.org/standard/72140.html

[24] FAIR Institute (2020) What Is FAIR? Available at https://www.fairinstitute.org/what-is-fair

[25] Joint Task Force Transformation Initiative (2014) Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53A, Rev. 4, Includes updates as of December 18, 2014. https://doi.org/10.6028/NIST.SP.800-53Ar4

[26] Basel Committee on Banking Supervision (2006) Basel II: International Convergence of Capital Measurement and Capital Standards: A Revised Framework – Comprehensive Version. (The Bank for International Settlements [BIS]). https://www.bis.org/publ/bcbs128.htm

Appendix A—Acronyms and Abbreviations

Selected acronyms and abbreviations used in this paper are defined below.

AFR	Agency Financial Report
BIS	The Bank for International Settlements
CapEx	Capital Expenditures
CBA	Cost/Benefit Analysis
CFO	Chief Financial Officer
CFOC	Chief Financial Officers Council
CISO	Chief Information Security Officer
COSO	Committee of Sponsoring Organizations
CRO	Chief Risk Officer
ERM	Enterprise Risk Management
FAIR	Factor Analysis of Information Risk
FIRST	Forum of Incident Response and Security Teams
FOIA	Freedom of Information Act
GAO	U.S. Government Accountability Office
IEC	International Electrotechnical Commission
IoT	Internet of Things
ISO	International Organization for Standardization
IT	Information Technology
ITL	Information Technology Laboratory
KRI	Key Risk Indicator
NICE	National Initiative for Cybersecurity Education
NIST	National Institute of Standards and Technology
NISTIR	National Institute of Standards and Technology Interagency or Internal Report
OCTAVE	Operationally Critical Threat, Asset, and Vulnerability Evaluation
OLIR	Online Informative References
OMB	Office of Management and Budget
OpEx	Operating Expenses
PBX	Private Branch Exchange

PIC	Performance Improvement Council
RAR	Risk Assessment Report
RMC	Risk Management Council or Committee
RMF	Risk Management Framework
SaaS	Software-as-a-Service
SEC	U.S. Securities and Exchange Commission
SP	Special Publication
SWOT	Strengths, Weaknesses, Opportunities, Threats
US-CERT	United States Computer Emergency Readiness Team

Appendix B—Glossary

Aggregation
The consolidation of similar or related information.

Assets
"The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes." [16]

Context
The environment in which the enterprise operates and is influenced by the risks involved.

Cybersecurity Risk
An effect of uncertainty on or within a digital context. Cybersecurity risks arise from the loss of confidentiality, integrity, or availability of information, data, or information (or control) systems and reflect the potential adverse impacts to organizational operations (i.e., mission, functions, image, or reputation) and assets, individuals, other organizations, and the Nation. (Definition based on ISO Guide 73 [7] and NIST SP 800-60 Vol. 1 Rev. 1 [8])

Enterprise
A top-level organization with unique risk management responsibilities based on its position in the hierarchy and the roles and responsibilities of its officers.

Enterprise Risk Management
The "culture, capabilities, and practices that organizations integrate with strategy-setting and apply when they carry out that strategy, with a purpose of managing risk in creating, preserving, and realizing value." [9]

Understanding all the types of risk an enterprise faces, determining how to address that risk, and ensuring the necessary actions are taken.

Exposure
The combination of likelihood and impact levels for a risk.

Normalization
The conversion of information into consistent representations and categorizations.

Opportunity
A condition that may result in a beneficial outcome.

Organization
An entity of any size, complexity, or positioning within an organizational structure (e.g., a federal agency or, as appropriate, any of its operational elements). [5]

A "person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its objectives." [6]

Qualitative Risk Analysis
A method for risk analysis that is based on the assignment of a descriptor such as low, medium, or high.

Quantitative Risk Analysis

A method for risk analysis where numerical values are assigned to both impact and likelihood based on statistical probabilities and monetarized valuation of loss.

Risk Appetite

“The types and amount of risk, on a broad level, [an organization] is willing to accept in its pursuit of value.” [9]

Risk Profile

The result of aggregating, normalizing, and prioritizing risk registers at higher levels of an enterprise.

Risk Register

“A repository of risk information including the data understood about risks over time.” [2]

Risk Reserve

A types of management reserve where funding or labor hours are set aside and employed if a risk is triggered to ensure the successful opportunity is realized or negative threat is avoided.

Risk Response

A way to keep risk within tolerable levels. Negative risks can be accepted, transferred, mitigated, or avoided. Positive risks can be exploited, shared, enhanced, or accepted.

Risk Tolerance

The organization’s or stakeholder’s readiness to bear the risk after risk response in order to achieve its objectives, with the consideration that such tolerance can be influenced by legal or regulatory requirements. [7]

Semi-Qualitative Risk Analysis

A method for risk analysis with qualitative categories assigned numeric values to allow for the calculation of numeric results.

System

“A discrete set of information resources organized expressly for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.” [5]

Threat

Anything that can act against an asset in a manner that can result in harm.

Vulnerability

A condition that enables a threat event to occur.

Appendix C—Federal Government Sources for Identifying Risks

This appendix lists federal government sources for identifying risks as defined on page 28 of *Playbook: Enterprise Risk Management for the U.S. Federal Government* [1].

- "Agency Reports and Self-Assessments
    - Previous year Federal Managers and Financial Integrity Act reports and A-123, Appendix A self-assessments and related assurance statements. Specifically, this may include:
        - Entity-level control interviews and evidence documentation;
        - Assessment of agency processes and thousands of documented controls;
        - Documentation of control deficiencies, including the level of significance of those deficiencies (simple, significant, or material weakness); and
        - Corrective actions associated with the deficiencies and tracked to either remediation or risk acceptance.
    - Financial Management Risks documented in the agency's Annual Report.
    - Project management risks documented in the agency's investment and project management processes.
    - Anything raised during Strategic Objectives Annual Review, quarterly performance reviews, RMC, etc.
- Inspector General (IG) and Government Accountability Office (GAO)
    - IG Management Challenges documented annually in the agency's AFR.
    - IG audits and the outstanding corrective actions associated with those audits.
    - GAO audits and the outstanding corrective actions associated with those audits.
- Congress
    - Issues and risks identified during Congressional Hearings and Questions for the Record.
- Media
    - Issues and risks identified in the news media."

Note: RMC stands for Risk Management Council or Committee, and AFR stands for Agency Financial Report.