NIST Interagency Report
NIST IR 8286r1 ipd

Integrating Cybersecurity and Enterprise Risk Management (ERM)

Initial Public Draft

Stephen Quinn
Julie Chua
Nahla Ivy
R. K. Gardner
Karen Scarfone
Matthew C. Smith
Greg Witte

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8286r1.ipd

NATIONAL INSTITUTE OF
STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

NIST Interagency Report
NIST IR 8286r1 ipd

Integrating Cybersecurity and Enterprise Risk Management (ERM)

Initial Public Draft

Stephen Quinn
Computer Security Division
Information Technology Laboratory

Julie Chua
Office of Information Security
Office of the Chief Information Officer
U.S. Department of Health and Human Services

Nahla Ivy
Enterprise Risk Management Office
Office of Financial Resource Management

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

Karen Scarfone
Scarfone Cybersecurity
Clifton, VA

Matthew C. Smith
Seemless Transition LLC
Seattle, WA

Greg Witte
Huntington Ingalls Industries
Annapolis Junction, MD

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8286r1.ipd

February 2025

U.S. Department of Commerce
Howard Lutnick, Secretary of Commerce

National Institute of Standards and Technology
Craig Burkhardt, Acting Under Secretary of Commerce for Standards and Technology and Acting NIST Director

Certain equipment, instruments, software, or materials, commercial or non-commercial, are identified in this paper in order to specify the experimental procedure adequately. Such identification does not imply recommendation or endorsement of any product or service by NIST, nor does it imply that the materials or equipment identified 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.

NIST Technical Series Policies

NIST Technical Series Publication Identifier Syntax

How to Cite this NIST Technical Series Publication
Quinn SD, Chua J, Ivy N, Gardner RK, Scarfone K, Smith MC, Witte GA (2025) Integrating Cybersecurity and Enterprise Risk Management (ERM). (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency Report (IR) NIST IR 8286r1 ipd. https://doi.org/10.6028/NIST.IR.8286r1.ipd

Author ORCID iDs
Stephen D. Quinn: 0000-0003-1436-684X
Nahla Ivy: 0000-0003-4741-422X
Karen Scarfone: 0000-0001-6334-9486
Matthew C. Smith: 0000-0003-1004-7171
Gregory A. Witte: 0000-0002-5425-1097

Public Comment Period
February 26, 2025 – April 14, 2025

Submit Comments
nistir8286@nist.gov

National Institute of Standards and Technology
Attn: Applied Cybersecurity Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 2000) Gaithersburg, MD 20899-2000

Additional Information
Additional information about this publication is available at https://csrc.nist.gov/pubs/ir/8286/r1/ipd, including related content, potential updates, and document history.

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

Abstract

The increasing frequency, creativity, and severity of cybersecurity attacks means that all enterprises should ensure that cybersecurity risk is receiving 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. This document focuses on the use of risk registers to set out cybersecurity risk and explains the value of rolling up measures of risk that are usually addressed at lower system and organizational levels to the broader enterprise level.

Keywords

cybersecurity risk management (CSRM); cybersecurity risk measurement; cybersecurity risk profile; cybersecurity risk register (CSRR); enterprise risk management (ERM); enterprise risk profile; enterprise risk register (ERR); risk appetite; risk tolerance.

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.

Audience

The primary audience for this publication includes both federal and non-federal cybersecurity professionals at all levels who understand cybersecurity but may be unfamiliar with the details of enterprise risk management (ERM).

The secondary audience includes both federal and non-federal corporate officers, high-level executives, ERM officers and staff members, and others who understand ERM but may be unfamiliar with the details of cybersecurity.

All readers are expected to gain an improved understanding of how cybersecurity risk management (CSRM) and ERM complement and relate to each other as well as the benefits of integrating their use.

Document Conventions

The term "step" or "steps" is used in multiple frameworks and documents. If the term "step" is referring to anything other than the meaning from the ERM Playbook in Fig. 2, it will be preceded by a document or framework to differentiate its context (e.g., "NIST Cybersecurity Framework Step 1: *Prioritize and Scope*").

For the purposes of this document, the terms "cybersecurity" and "information security" are used interchangeably. While information security is generally considered to encompass the cybersecurity domain, the term "cybersecurity" has expanded in conventional usage to be equivalent to information security. Likewise, the terms "cybersecurity risk management" (CSRM) and "information security risk management" (ISRM) are used interchangeably based on the same reasoning.

Note to Reviewers

NIST is revising the IR 8286 series of documents to align them with the NIST Cybersecurity Framework (CSF) 2.0. Some of these documents only require errata updates, while others such as this one are undergoing a more substantial revision with a public comment period. Reviewers are encouraged to comment on the following topics:

- Alignment of IR 8286 with the CSF 2.0
- Alignment of IR 8286 with current ERM and CSRM practices
- Other topics of ERM and CSRM

Trademark Information

All registered trademarks and trademarks belong to their respective organizations.

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

Table of Contents

List of Tables

List of Figures

Acknowledgments

The authors wish to thank all of the individuals, organizations, and enterprises that contributed to the creation of the original version of this document. This includes Donna Dodson, Naomi Lefkovitz, Amy Mahn, Rodney Petersen, Victoria Yan Pillitteri, Ron Ross, Adam Sedgewick, and Kevin Stine of NIST; Larry Feldman, Heather Mills, and Daniel Topper of Huntington Ingalls Industries; and Mat Heyman of Impresa Management Solutions. Organizations and individuals who provided feedback on the public comment drafts include Aon; the Association of Local Government Auditors; Christopher White of Booz Allen Hamilton; Consortium for Information and Software Quality; P. Bevill, G. Celestin, M. Creary, E. Flaim, K. Francis, C. Gordon, K. Isaac, C. Livingston, M. Merritt, M. Nighswander, K. Pannah, J. Prutow, and N. Rohloff of the Cyber-ERM Community of Interest; FAIR Institute; Forescout Technologies; Adam Bobrow of Foresight Resilience Strategies; the IT Risk Management Team of the Internal Revenue Service; Larry Clinton of the Internet Security Alliance; Gerald Beuchelt and Christine Wachter of LogMeIn; Mosaic 451; Alex Krutov of Navigation Advisors; Ismael Garcia of the Nuclear Regulatory Commission; Kelly Hood and Tom Conkle of Optic Cyber Solutions; John Kimmins of Palindrome; Profitabil-IT; Dick Brooks of Reliable Energy Analytics; Jack Freund of RiskLens; Marshall Toburen of RSA Security; Paul Rohmeyer of Stevens Institute of Technology; The Open Group; Rob Arnold of Threat Sketch; Ashley P. Moore and Nnake Nweke of the U.S. Agency for Global Media; the U.S. Air Force; the U.S. Department of Defense; the U.S. Department of Education; the U.S. Department of Energy; the U.S. Department of Health and Human Services; the U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency; the U.S. Navy; Simon Burson; Norman Marks; Ellen Swanson; and Douglas Webster.

Executive Summary

For federal agencies, the Office of Management and Budget (OMB) Circular A-11 defines *risk* as "the effect of uncertainty on objectives" [1]. The effect of uncertainty on *enterprise* mission and business objectives may then be considered an "enterprise risk" that must be similarly managed. An *enterprise* is an organization that exists at the top level of a hierarchy with unique risk management responsibilities. Managing risks at that level is known as enterprise risk management (ERM) and calls for understanding the core risks that an enterprise faces, determining how best to address those risks, and ensuring that the necessary actions are taken. In the Federal Government, ERM is considered "an effective agency-wide approach to addressing the full spectrum of the organization's significant risks by understanding the combined impact of risks as an interrelated portfolio rather than addressing risks only within silos" [1].

Cybersecurity risk is an important type of risk for any enterprise. Other risks include but are not limited to financial, legal, legislative, operational, privacy, reputational, safety, strategic, and supply chain risks [2]. As part of an ERM program, senior leaders (e.g., corporate officers, government senior executive staff) often have fiduciary and reporting responsibilities that other organizational stakeholders do not, so they have a unique responsibility to holistically manage the combined set of risks, including cybersecurity risk. The individual organizations that comprise every enterprise are experiencing an increase in the frequency, creativity, and severity of cybersecurity attacks. All organizations and enterprises, regardless of size or type, should ensure that cybersecurity risks receive appropriate attention as they carry out their ERM functions. Since enterprises are at various degrees of maturity regarding the implementation of risk management, this document offers NIST's cybersecurity risk management (CSRM) expertise to help organizations improve the cybersecurity risk information they provide as inputs to their enterprise's ERM programs.

Many resources document ERM frameworks and processes, such as well-known frameworks from the Committee of Sponsoring Organizations (COSO), Office of Management and Budget (OMB) circulars, and the International Organization for Standardization (ISO). They generally include similar approaches: identify context, identify risks, analyze risks, estimate risk importance, determine and execute risk response, and identify and respond to changes over time. A critical risk document used to track and communicate risk information for all of these steps throughout the enterprise is called a *risk register* [1].[1] The risk register provides a formal communication vehicle for sharing and coordinating cybersecurity risk activities as an input to ERM decision-makers. For example, *cybersecurity risk registers* are key aspects of managing and communicating about those particular risks.[2]

At higher levels in the enterprise structure, those cybersecurity and other risk registers are aggregated, normalized, and prioritized into *risk profiles*. A risk profile is defined by OMB Circular A-123 as "a prioritized inventory of the most significant risks identified and assessed

[1] OMB Circular A-11 defines a risk register as "a repository of risk information including the data understood about risks over time" [1].

[2] Organizations creating a risk management program for the first time should not wait until the risk register is completed before addressing obvious issues. However, over time, it should become the ordinary means of communicating risk information.

through the risk assessment process versus a complete inventory of risks" [3]. While it is critical that enterprises address potential negative impacts on mission and business objectives, it is equally critical (and required for federal agencies) that enterprises plan for success. OMB states in Circular A-123 that "the [Enterprise Risk] profile must identify sources of uncertainty, both positive (opportunities) and negative (threats)." Enterprise-level decision-makers use the risk profile to choose which enterprise risks to address, allocate resources, and delegate responsibilities to appropriate risk owners. ERM programs should define terminology, formats, criteria, and other guidance for risk inputs from lower levels of the enterprise.

Cybersecurity risk inputs to ERM programs should be documented and tracked in written cybersecurity risk registers[3] that comply with the ERM program guidance. However, many enterprises do not communicate their cybersecurity risk guidance or risk responses in consistent, repeatable ways. Methods such as quantifying cybersecurity risk in dollars and aggregating cybersecurity risks are often ad hoc and are sometimes not performed with the same rigor as methods for quantifying other types of risk within the enterprise.

In addition to widely using cybersecurity risk registers, improving the risk measurement and analysis methods used in CSRM will boost the quality of the risk information provided to ERM. In turn, this practice promotes better management of cybersecurity at the enterprise level and correlates directly with the enterprise's objectives.

CSRM and ERM are concurrent cycles with many points of commonality and integration. NIST framework documents, specifically the Cybersecurity Framework (CSF) 2.0 and Special Publication (SP) 800-221A, provide methods for performing CSRM and integrating the results. The concepts detailed in this IR 8286 series are directly incorporated into both the CSF 2.0 (CSRM) and SP 800-221A (integrating with ERM) frameworks. Improving the measurement and communications methods used (e.g., using cybersecurity risk registers) can improve the quality of risk information, promote enterprise-wide CSRM, and support enterprise-level decision-making in language that is already understood by senior executives. Improved communications will also help executives and corporate officers understand the challenges that cybersecurity professionals face when providing the information that they are accustomed to receiving for other types of risk.

[3] Formats include risk register data displayed on dashboards, GRC tools, and file formats for communicating risk register data, such as the spreadsheet (CSV) and JSON formats.

1. Introduction

The terms *organization* and *enterprise* are often used interchangeably.[4] However, for the purposes of this document, an *organization* is defined as an entity of any size, complexity, or position within a larger organizational structure (e.g., a federal agency or company) [5]. An *enterprise* is an organization by this definition, but its primary functions subsist at the top level of the hierarchy, where individual senior leaders have unique risk management responsibilities. Most CSRM responsibilities tend to be carried out by individual organizations within an enterprise. In contrast, the responsibility for tracking key *enterprise* risks and their impacts on objectives is held by top-level corporate officers and board members who have fiduciary and reporting duties that are not performed anywhere else in the enterprise.

Figure 1 depicts a notional enterprise with subordinate organizations, illustrating that one of those subordinate organizations is itself an enterprise.

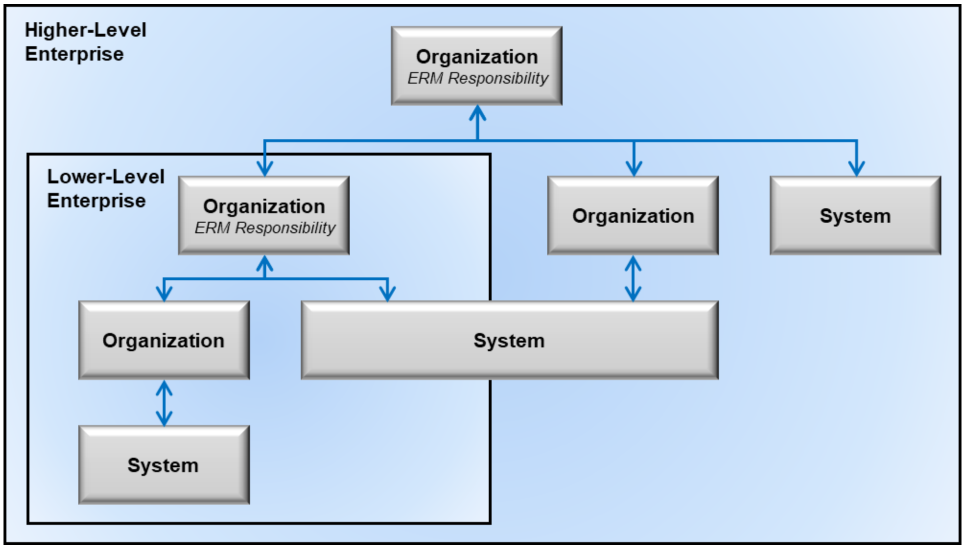


Fig. 1. Enterprise hierarchy for cybersecurity risk management

Both government and industry are represented in this depiction. Consider the example of the Department of Commerce as a higher-level enterprise with bureaus (e.g., Census Bureau, National Oceanic and Atmospheric Administration [NOAA], NIST) as lower-level enterprises and subordinates (e.g., NOAA's National Weather Service, NIST laboratories) representing organizations. In industry, consider mergers and acquisitions in which an enterprise acquires another company that itself was an enterprise and then subordinates it within the higher-level enterprise's conglomeration of organizations and systems.[5] Each enterprise is supported by various *systems* that are defined as "a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information" [5].

[4] For example, 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 discussed in this publication have more complex compositions.

[5] 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

This document is intended to help improve communications (including risk information sharing) between and among cybersecurity professionals, high-level executives, and corporate officers at multiple levels. The goal is to assist personnel and system owners in these enterprises and their subordinate organizations to better identify, assess, and manage cybersecurity risks in the context of their broader mission and business objectives.[6] This document will help cybersecurity professionals understand what executives and corporate officers need to carry out ERM, including what data to collect, what analyses to perform, and how to consolidate and condition this discipline-specific risk information so that it provides useful inputs for ERM programs. This document will also help high-level executives and corporate officers understand the challenges that cybersecurity professionals face in providing them with relevant information. Because enterprise stakeholders are accustomed to receiving reports regarding many types of risk, guidance on cybersecurity that is consistent with these other risk categories will support well-crafted and actionable risk appetite and risk tolerance decisions and statements.

Government and private industry CSRM and ERM programs are similar but often involve different oversight and reporting requirements, such as Congressional testimony versus a regulatory filing. For this reason, the Committee of Sponsoring Organizations (COSO) is often cited due to its dual role in providing guidance to both public and private organizations regarding ERM and the fact that OMB adopted much of its language when developing Circular A-123 [3].

This document bridges existing private industry risk management processes with federal cybersecurity risk requirements derived from OMB Circular A-130 [6]. It also introduces concepts that are further developed in subsequent documents in the IR 8286 series, such as communicating risk, consistently identifying threats and risks, estimating likelihood and impact, calculating risk exposure, establishing and using risk reserves, monitoring risk, reporting risk, and integrating with ERM programs. Furthermore, this document provides guidance for linking the CSF [7] (specifically, its new Govern Function), the Information and Communications Technology Risk Outcomes Framework (SP 800-221A) [8], and ERM processes. These concurrent risk management processes inform and are informed by each other to create a vertically and horizontally integrated risk management process that connects the boardroom to the server room.

This document references some materials that are specifically intended for use by federal agencies and will be highlighted as such, but the concepts and approaches are intended to be useful for all enterprises.

[6] Figure 1 depicts the correlation of cybersecurity professionals (system), high-level executives without fiduciary reporting requirements (organization), and corporate officers with fiduciary reporting requirements (enterprise), respectively.

An informative reference[7] links the contents of this document with CSF v1.1 and SP 800-221A as part of the National Online Informative References (OLIR) Program.[8] An updated OLIR will link SP 800-221A to CSF 2.0.

1.2. Document Structure

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

- Section 2 provides an overview of ERM and CSRM and highlights high-level gaps between current practices.
- Section 3 discusses detailed cybersecurity risk considerations throughout the ERM process and the use of the risk register to document cybersecurity risk as ERM input.
- Section 4 considers a portfolio view of risk at the enterprise level based on normalizing and aggregating risk registers into an enterprise risk register (ERR) and then applying prioritization to it to generate an enterprise risk profile (ERP) in support of senior executive decision-making.
- The References section provides links to external sites and publications that offer additional information.
- Appendix A lists the acronyms used in the document.
- Appendix B provides a glossary of the terminology used in this document.
- Appendix C lists Federal Government sources for identifying risks, as defined in *Playbook: Enterprise Risk Management for the U.S. Federal Government* [2].
- Appendix D provides a notional enterprise risk register.
- Appendix E provides a change log for this document.

[7] See https://csrc.nist.gov/projects/olir/informative-reference-catalog/details?referenceId=78 - /.

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

2. Gaps in Managing Cybersecurity Risk as an ERM Input

OMB Circular A-11 defines *risk* as “the effect of uncertainty on objectives” [1]. The effect of uncertainty on *enterprise* mission and business objectives may then be considered an “enterprise risk” that must be similarly managed. The process of managing risks at the enterprise level is known as ERM and calls for:

- Identifying and understanding the core risks facing an enterprise,
- Determining how best to address those risks, and
- Ensuring that the necessary actions are taken.

This publication focuses on recognizing and incorporating *cybersecurity risk*[9] within the ERM and complements other NIST documents by informing and extending existing guidance to respond to risks to an enterprise’s data, information, and technology assets. Integration draws on CSRM and the basics of ERM, which informs and is informed by various risks at subordinate levels. Comparing the results of CSRM activities with those required for effective input to ERM enables enterprise stakeholders to identify opportunities to close gaps.

2.1. Overview of ERM

ERM requires identifying and understanding the various types of risks that an enterprise faces, determining the probability that these risks will occur, and estimating their potential impacts. OMB considers ERM to be “an effective agency-wide approach to addressing the full spectrum of the organization’s significant risks by understanding the combined impact of risks as an interrelated portfolio, rather than addressing risks only within silos” [1].

Cybersecurity risk is one portion of the spectrum of an enterprise’s core risks. Appendix A of *Playbook: Enterprise Risk Management for the U.S. Federal Government* [2] defines numerous risk types, including compliance, cybersecurity (“cyber information security”), financial, legal, legislative, operational, reputational, and strategic. This list can easily be expanded to other risk disciplines, such as safety, privacy, and supply chains that ultimately anchor in ERM. In ERM, enterprises holistically manage the combined set of enterprise risks.[10]

The COSO 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” [10]. Public and private enterprises have a common primary purpose for ERM: to safeguard the enterprise’s mission, finances (e.g., net revenue, capital, and free cash flow), and reputation (e.g., stakeholder trust) in the face of natural, accidental, and adversarial threats.

[9]

[10] Per [4], “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.”

This is accomplished by considering enterprise risks in relation to achieving strategic and operational objectives as typically outlined in an organizational strategic plan. OMB Circular A-123 requires ERM risk profiles to include four kinds of objectives: strategic, operations (operational effectiveness and efficiency), reporting (reporting reliability), and compliance (compliance with applicable laws and regulations) [3]. While there may be some overlap of risk among the categories of objectives, understanding uncertainty as it affects these objectives will help inform effective and timely decision-making. In turn, context and categorization processes support risk guidance back to subordinate levels. Effective ERM balances achieving security objectives with optimizing limited resources.

This document draws on ERM principles regarding integration with culture, strategy, and performance. One such principle 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" [10]. OMB adapted this language for government use in Circular A-123 by similarly stating that risk appetite "is the broad-based amount of risk an organization is willing to accept in pursuit of its mission/vision" [3]. Risk appetite is established by the organization's most senior-level leadership (enterprise) and serves as the guidepost for decisions, such as setting strategy and selecting objectives.

Another important ERM concept is *risk tolerance* — the organization or stakeholders' readiness to bear the remaining risk *after responding to or considering the risk* in order to achieve its objectives (while recognizing that such tolerance can be influenced by legal or regulatory requirements) [10].[11] OMB again adapted the COSO language by stating that risk tolerance "is the acceptable level of variance in performance relative to the achievement of objectives" [3].

While risk tolerance can be defined at the enterprise level, OMB allows for organizational discretion, stating that risk tolerance is "generally established at the program, objective, or component level" [3], which can include the organization levels depicted in Fig. 1. Risk tolerance is always interpreted and applied by the receiving custodians of the risk management discipline (e.g., cybersecurity, legal, privacy) and usually interpreted at the organizational or system level.[12] For example, a statement of risk appetite might be: "Email service shall be available during the large majority of a 24-hour period." An associated risk tolerance statement for this defined appetite is narrower: "Email services shall not be interrupted for more than five minutes during core hours."

Senior enterprise executives provide risk guidance to the organizations within their purview, including advice on mission priority, risk appetite and tolerance, and capital and operating budgets to manage known risks. Risk appetite and tolerance statements are the usual means for communicating this guidance. Organizations then manage and monitor processes that properly balance the risks and resource allocation with the value created by information and technology. Measurements (e.g., from key risk indicators, or KRIs) demonstrate where risk tolerances have been exceeded or validate that the enterprise is operating within the defined

[11] 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].

[12] SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View* [11], uses the term "risk tolerance" to collectively refer to what Circular A-123 and this publication differentiate into two terms: "risk tolerance" and "risk appetite."

appetite. IR 8286A provides detailed examples of risk appetite and risk tolerance statements and how they are interrupted and applied with the associated risk defined, managed, and communicated back to executive management via the risk register [12]. ERM processes should aid senior enterprise executives by providing them with a portfolio view of key risks across the enterprise (see Sec. 4).[13]

2.1.1. Common Use of ERM

Public officials and corporate boards typically measure and weigh the impact and likelihood of each type of significant risk (e.g., market, operational, labor, geopolitical, cyber) to determine their individual and total impacts on the enterprise's mission, finances, and reputation. They then determine their risk appetite and resource allocations for each type of risk commensurate with likelihood and impact and balanced with all calculated enterprise risk exposures (i.e., the product of likelihood and impact). Public officials and board members also provide guidance to their corporate officers at the enterprise level and to high-level executives at the organizational level (see Fig. 1). This includes guidance on ceilings for capital expenditures (CapEx) and operating expenses (OpEx) and objectives for free cash flow. They then issue guidance to continue, accelerate, reduce, delay, or cancel significant enterprise initiatives while making decisions about prudent risk disclosures and balancing the competing objectives of a) properly informing stakeholders and overseers (including regulators) through required filings and statements at hearings with b) protecting sensitive information from competitors and adversaries.

2.1.2. ERM Framework Steps

This document uses the processes of the ERM Playbook for the U.S. Federal Government [2] to address cybersecurity risks. Figure 2 is taken from the ERM Playbook Appendix D and depicts an example of an ERM framework.

[13] This is defined by OMB as "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].

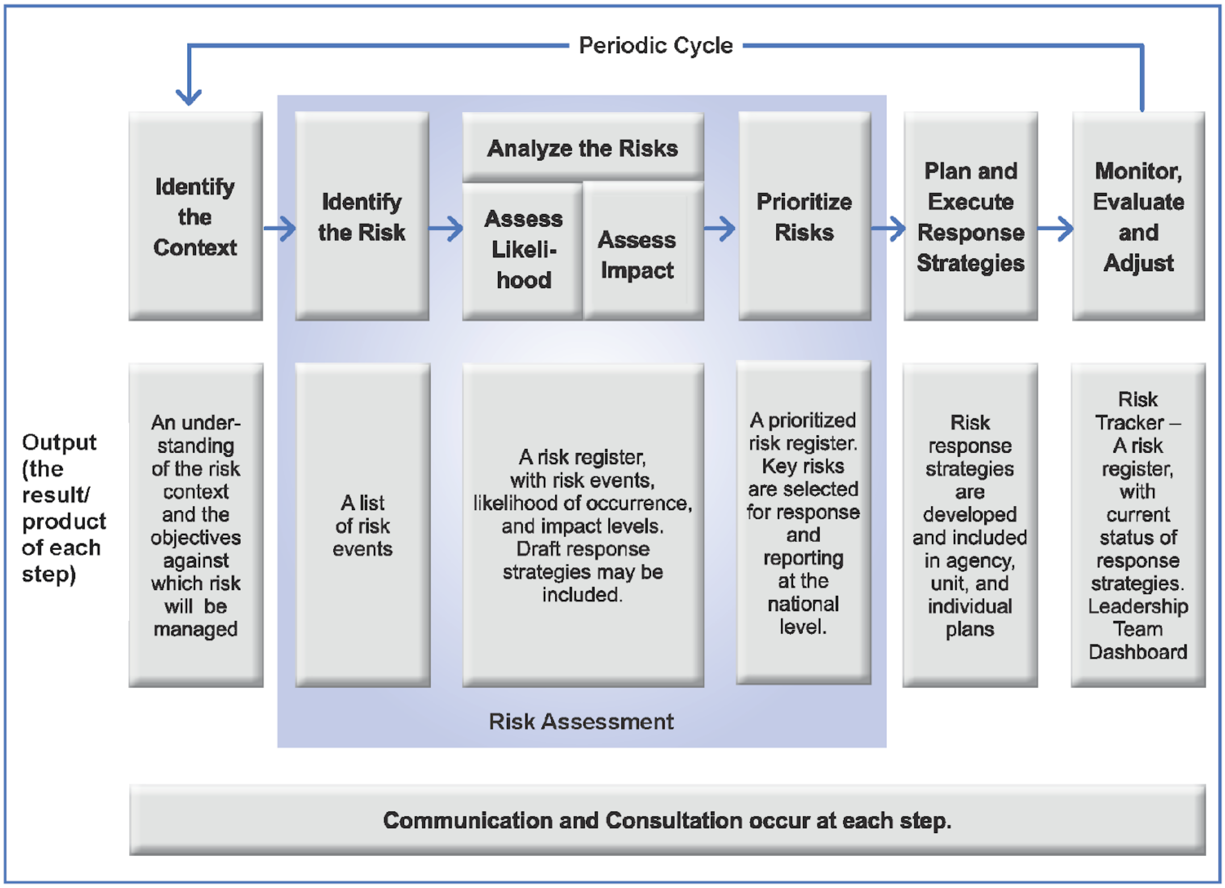

Periodic Cycle
Identify the Context
Identify the Risk
Analyze the Risks
Assess Likeli-hood
Assess Impact
Prioritize Risks
Plan and Execute Response Strategies
Monitor, Evaluate and Adjust
Output (the result/ product of each step)
An under-standing of the risk context and the objectives against which 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.

Fig. 2. Notional risk management life cycle

While the steps in Fig. 2 provide the basis for this document's structure, enterprises should use whatever ERM approach they favor with the assumption that it will contain the content of these steps in some way. SP 800-221A [8] provides a risk outcome framework that guides users on implementing these steps in their information and communications technology (ICT) and ERM activities.

Figure 2 depicts six steps that are discussed in further detail in Sec. 3:

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 (i.e., determining which events could enhance or impede objectives), including the risks of 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 the risks are prioritized based on their exposure.

5. **Plan and execute risk response strategies.** The appropriate response is determined for each risk, and the decisions are 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.

OMB Circular A-123 [3] recommends (and requires for federal users) that enterprise risks be recorded in a risk register comprised of discipline-specific risks (e.g., cybersecurity, legal, financial). OMB Circular A-11 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” [1]. Cybersecurity risk registers are a key aspect of managing cybersecurity risks within an enterprise, and organizations are strongly urged to adopt and integrate them into whatever risk management methodology they are currently using. Their use as a shared organizing method for cybersecurity risk ensures seamless communication with senior decision-makers.

Each register evolves and matures as other risk activities take place. Section 3 of this document contains more information on cybersecurity risk registers.

There are many publications with more information on ERM fundamentals, including:

- OMB Circular A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control* [3][14]
- *Enterprise Risk Management—Integrating with Strategy and Performance* [10]
- *Playbook: Enterprise Risk Management for the U.S. Federal Government* [2]

2.2. The Gap Between CSRM Output and ERM Input

Effectively balancing the benefits of technology with the potential risks and consequences of a threat event is more likely to result in effective CSRM that supports a comprehensive ERM approach. Attempting to avoid all cybersecurity risk might inadvertently stifle innovation, while applying technology without regard for cybersecurity, legal, regulatory, or compliance risks may lead to undesirable consequences.

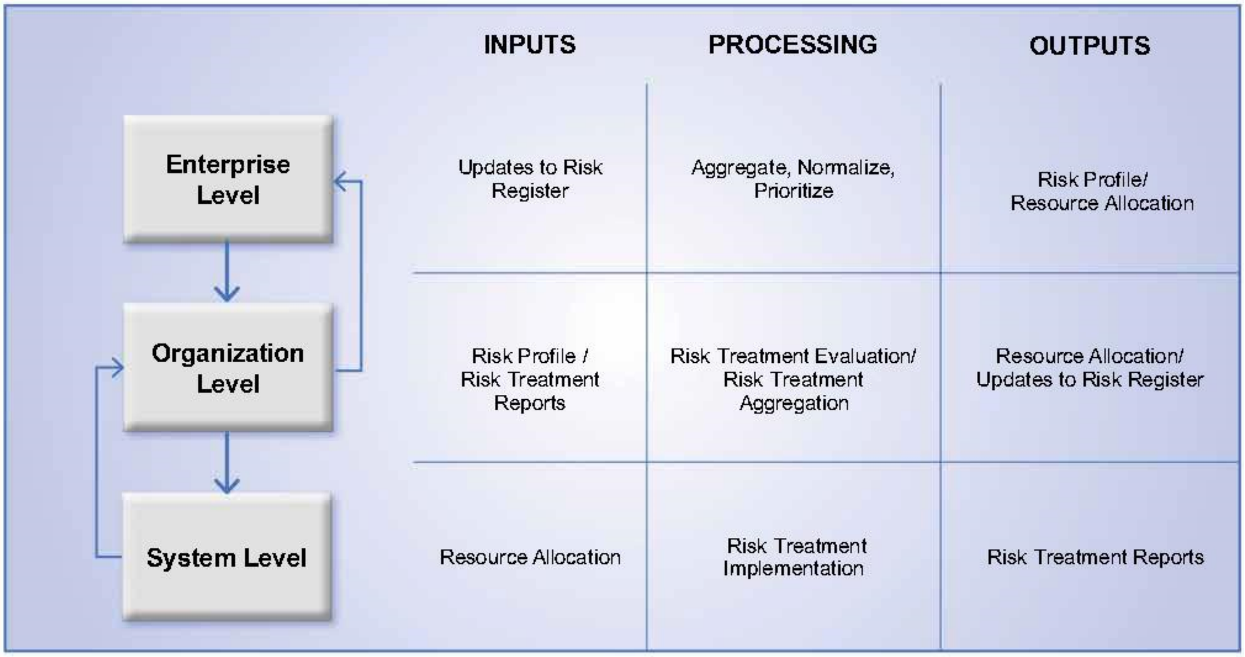
The separation between enterprise risk governance and cybersecurity risk governance can be emphasized by the introduction of complex, adaptive systems of systems. It is common for enterprises to handle these ever-growing systems as a single source of risk without understanding the interconnected nature of cybersecurity risks and the operational risks. Enterprises should engage in complex behavior analysis of their systems from an enterprise

[14] Per [4], “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.”

perspective to separate the knowable cybersecurity risks from the unknowable, emergent risks that could be realized. By reducing their risk footprint from aggregated and analyzed enterprise risks, enterprises can limit the impacts of a realized risk.

Enterprises, organizations, and practitioners should consider the influence of cybersecurity risks on achieving enterprise strategic, operations, reporting, and compliance objectives. Enterprise risk officers should clearly communicate these enterprise objectives so that cybersecurity practitioners can take actions and provide relevant risk inputs to ERM programs. Enterprise leaders should conduct an ongoing business impact analysis (BIA) of current assets that support those objectives. A cybersecurity risk assessment can then be conducted on critical assets to drive the enterprise's mission, as described in IR 8286D [13].

For ERM purposes, each high-value system[15] and organization should have a cybersecurity risk register that explicitly records and communicates risk decisions that consider the enterprise risk strategy. The contents of those registers should be aggregated, normalized, analyzed, and prioritized at higher levels to allow for the easy transfer of cybersecurity risk knowledge from CSRM to ERM. Figure 3 depicts the flow of information.



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

Fig. 3. Risk register information flow among system, organization, and enterprise levels

Improving the risk measurement and analysis methods used in CSRM[16] and widely using cybersecurity risk registers will enhance the quality of the risk information provided to ERM. This would also promote better management of cybersecurity risk at the enterprise level and improve enterprise-level decision-making.

[15] OMB Circular A-130 defines an *information system* as "a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information" [6].

[16] The NIST Cybersecurity Framework [7] describes CSRM progression through the four Tiers — Partial, Risk-Informed, Repeatable, and Adaptive — where risk management processes mature from ad hoc to formalized and agile.

According to IR 8170, *Approaches for Federal Agencies to Use the Cybersecurity Framework*, 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

Cybersecurity risk registers consistently capture, organize, and communicate risk-related information (e.g., risk assessments, evaluation decisions, responses, and monitoring activities) from the individual system level up through the organizational level and finally to the highest enterprise level. Considering those risks as *risk scenarios* presents detailed risk information in context. A complete risk scenario describes the source of uncertainty, any predisposing conditions, the resources affected, and the anticipated result. For cybersecurity risks, a scenario might include a threat source, a threat event, a vulnerability that the threat source might exploit, any enterprise assets that may be impacted by the threat, and the resulting harmful impact. For example, "Construction activity severs a critical fiber optic cable that was not protected in conduit, interrupting communications to the data center and resulting in the loss of availability of enterprise financial systems." Detailed information about the use of scenarios for risk identification and analysis will be described in a future NIST publication.

As introduced in previous sections, a key goal of CSRM is to help enterprise stakeholders optimize risk and resources to support enterprise business objectives. The information and technology being secured provide value to the enterprise by supporting one or more business needs. The CSRM process is intended to help ensure that the enterprise can realize that value while achieving stakeholders' expectations regarding the protection of confidentiality, integrity, and availability. Each of the following stages of CSRM as an ERM input should be based on the potential impact of a given risk scenario on the enterprise and mission and business objectives.

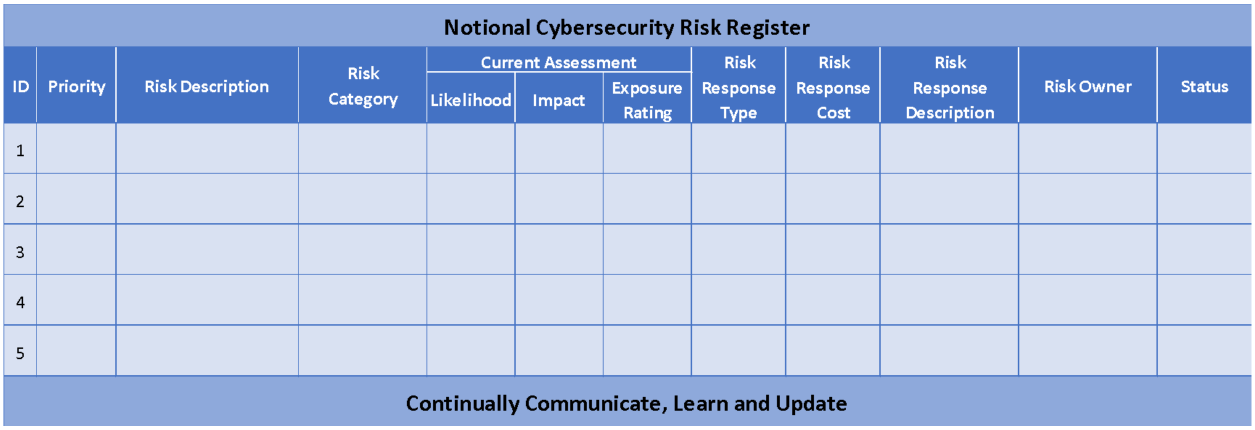
This section references two types of controls in support of ERM, each of which is essential and should not be confused with the other:

1. **Internal controls** are the overarching mechanisms used to achieve and monitor enterprise objectives. The COSO Internal Control – Integrated Framework defines internal control as "a process affected by an entity's board of directors, management and other personnel designed to provide reasonable assurance of the achievement of objectives" [14]. These internal controls are an important factor at the enterprise level. In fact, the title of OMB Circular A-123 is "Management's Responsibility for Enterprise Risk Management and Internal Control."

2. **Security controls** represent the "safeguards or countermeasures prescribed for an information system or an organization to protect the confidentiality, integrity, and availability of the system and its information" [6]. Security controls provide the management, administrative, and technical methods for responding to cybersecurity risks by deterring, detecting, preventing, or correcting threats and vulnerabilities.

Figure 4 shows a notional cybersecurity risk register template.[17]

[17] Depending on the organization's risk strategy, the risk register may contain many more (or fewer) fields that detail the risk metadata. That information may also be captured elsewhere but have a connected/linked path to the risk register content.



Notional Cybersecurity Risk Register

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

Continually Communicate, Learn and Update

Fig. 4. Notional cybersecurity risk register template

The remainder of Sec. 3 provides guidance and useful information for completing and using cybersecurity risk registers and integrating them with ERM. The notional template 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" [1].

The OMB examples from A-123 reference *inherent risk* that describes "conditions in the absence of risk management actions" [3]. There will likely be at least *some* elements that help mitigate risks, so this publication typically refers to *current risk* (rather than inherent risk) that represents a baseline risk posture.

Table 1 describes each of the elements in the notional cybersecurity risk register template.

Table 1. 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.
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 that could impact 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], as illustrated in Fig. 7). Consistent risk categorization is helpful for comparing risk registers during the risk aggregation step of ERM.
Current Assessment — Likelihood	Before any risk response, an estimation of the probability that this scenario will occur. On the first iteration of the risk cycle, this may also be considered the initial assessment, whereas subsequent cycles refer to this as inherent.
Current Assessment — Impact	Analysis of the potential benefits or consequences that might result from this scenario if no additional response is provided.

Register Element	Description
Current Assessment — Exposure Rating	A calculation of the probability of risk exposure based on the 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* (e.g., ISO 31000, SP 800-30r1).
Risk Response Type	The risk response (sometimes referred to as the risk treatment) for handling the identified risk. Values for risk response types are listed in Table 2 and Table 4 of this document.
Risk Response Cost	The estimated cost of applying the risk response.
Risk Response Description	A brief description of the risk response. For example, "Implement software management application XYZ to ensure that software platforms and applications are inventoried," or "Develop and implement a process to ensure the timely receipt of threat intelligence from [name of specific information sharing forums and sources]."
Risk Owner	The designated party responsible and accountable for ensuring that the risk is maintained in accordance with enterprise requirements. The risk owner may work with a designated risk manager who is responsible for managing and monitoring the selected risk response.
Status	A field for tracking the current condition of the risk and any subsequent activities.

This section discusses how risk registers are used within organizations as a method for communicating and tracking cybersecurity risks over time. Section 3.8 provides a notional example of activities at the enterprise level by which the prioritized organizational cybersecurity risk registers are correlated, aggregated, and normalized. The key risks are compiled into the enterprise risk profile (e.g., the Agency Risk Profile described in OMB Circular A-123 Section B1) [3].

The risk register model shown here illustrates a single point in time. The actual composition of the register will vary among enterprises and may contain more or fewer data points than those described in Table 1. For example, some organizations may wish to include both the current risk assessment (before risk response is applied) and the anticipated changes to risk that are expected to result based on the risk response. Regardless of which model is selected for use as a risk register, the enterprise should ensure that the model is used in a consistent and iterative way. As the risk professional progresses through the steps in Sec. 3, the risk register will be populated with relevant information. Once decisions have been made as part of a subsequent review of the risks, the agreed-upon risk response becomes the current state after mitigations are put in place, and the cycle begins anew.

While the risk register itself can be used to document and communicate summary information about current risks and responses, it may be necessary to supplement the register with a *risk detail record*, as detailed by the risk strategy. A risk detail record documents the considerations, assumptions, and results of risk management activities to keep the formal risk register a summary rather than a large, detailed report. It also enables the enterprise to record the personnel involved in those considerations, any actions to be taken, and schedules. This detailed risk record may be stored and maintained in a written record, as part of an organizational knowledge management system, or as a database entry in risk-specific software, such as a governance, risk, and compliance (GRC) application.

Regardless of the risk strategy chosen, there should be a connection between the data in the risk register and the risk detail report. The contents of a risk detail record may include:

- Information regarding the risk itself, such as a detailed risk scenario description and underlying threats, vulnerabilities, assets threatened, risk category, and risk assessment results
- The roles involved in risk decisions and management, such as the risk owner, risk manager, action owner for specific activities, stakeholders involved in risk response decisions, contractual agreements for supply chain/external partners
- Schedule considerations, such as the date on which the risk was first documented, the date of the last risk assessment, completion dates for mitigations, and the date of the next expected assessment
- Risk response decisions and follow-up, including detailed plans, status, and risk indicators

The examples above only illustrate the current risk assessment (i.e., likelihood, impact, and resulting exposure value). Organizations will need to determine which assessments should be reflected in the risk register. This report describes the risk register as an input into the risk management decision process, so only the current risk assessment results are depicted. If the register is to be updated after the risk response, the results of a post-response assessment could be reflected in the register as the *residual risk*. Organizations might even document the *target residual risk*, which is the desired risk state based on risk appetite/tolerance (see Sec. 3.2). Because the risk management process is cyclical, assessment results may be different in future iterations.

> SP 800-30r1, Appendix K [15], describes essential cybersecurity risk elements that might be recorded in a *cybersecurity risk assessment report (RAR).* An RAR and a cybersecurity risk register are complementary. The RAR provides a detailed record of the planning, execution, and evaluation of identified risks and can also be used to inform the risk register. The RAR could also be used as the *risk detail record* to document additional information, such as risk assumptions, constraints, and rationale.

3.1. Identify the Context

In the risk management life cycle shown in Fig. 2, the first step in managing cybersecurity risks is understanding *context* — the environment in which the organization operates and is influenced by the risks involved. As shown in Fig. 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:

1. **External context** involves the expectations of outside stakeholders that affect and are affected by the organization, such as customers, regulators, legislators, and business

partners. These stakeholders have objectives, perceptions, and expectations about how risk will be communicated, managed, and monitored.

2. **Internal context** relates to many of the factors within the organization and relevant cybersecurity considerations across the enterprise. This includes any internal factors that influence CSRM, such as the organization and enterprise's objectives, governance, culture, risk appetite, risk tolerances, policies, and practices.

Several NIST frameworks begin with determining these context factors. For example, the Risk Management Framework [16] includes a *Prepare* step to identify organizational strategy, management methods, and roles. Similarly, the CSF [7] Category Organizational Context within the Govern Function (GV.OC) states, "The circumstances — mission, stakeholder expectations, dependencies, and legal, regulatory, and contractual requirements — surrounding the organization's cybersecurity risk management decisions are understood." These context exercises identify organizational mission drivers and priorities used for subsequent assessment and planning.

3.1.1. Notional Risk Management Roles

An important element of the internal and external context is identifying the relevant work roles for each stage. Defining the types of stakeholders and recording the names of personnel in those roles who are involved at each stage will support risk communication and timely decision-making. The CSF Category titled Roles, Responsibilities, and Authorities in the Govern Function (GV.RR) states, "Cybersecurity roles, responsibilities, and authorities to foster accountability, performance assessment, and continuous improvement are established and communicated" [7]. It may be helpful to document responsibilities in the form of a RACI chart[18] that designates which roles are responsible, accountable, consulted, or informed about various activities.

Roles described in Sec. 3 and 4 of this publication include internal and external individuals and groups related to the Risk Executive Function,[19] such as:

- Cybersecurity Risk Officer — Manages the risk management process for a given information system (or set of systems). This individual may act as the risk owner for any particular risk in the register or as the risk manager designated by the risk owner who remains accountable for management and communication about the risk.
- Enterprise Risk Officer — A senior-level official accountable for managing and communicating risk across the enterprise. In some organizations, this may be the Chief Risk Officer (CRO) or another senior designee.

[18] A RACI chart provides a visual representation of those who are responsible (R), accountable (A), consulted (C), and informed (I).

[19] According to the ERM Playbook, the Senior Accountable Official for Risk Management (SAORM) is the head of the agency and is responsible for the oversight of information security, privacy risk management, and broader ERM processes. The Risk Executive function for each risk discipline oversees the management of risks within each discipline. The Risk Executive function for cybersecurity would be the Cybersecurity Risk Officer defined in this list. For enterprise-level ERM, it would be the Enterprise Risk Officer defined in this list in tandem with the ERM Council/Steering Committee or other governing body. A similar committee-style governance function also exists in the cybersecurity space in the form of the CIO and CISO councils.

- Other C-Suite Member — Chief Information Officer (CIO), Chief Information Security Officer (CISO), Chief Privacy Officer (CPO), Chief Financial Officer (CFO), or other similar roles.
- Senior Enterprise Leaders — Agency or corporate officials, such as those who represent various elements of the organization and assist with managing and communicating risk throughout the enterprise.
- Enterprise Risk Steering Committee (ERSC) — A group responsible for receiving risk management information from throughout the enterprise and considering the overarching impact.
- Auditor — Provides independent and formal verification regarding the achievement of enterprise objectives and the application of ERM processes.
- Other Internal Partners — Includes other enterprise stakeholders (e.g., legal affairs, human resources, business managers) with an interest in the risk management and risk decisions performed.
- External Stakeholders — Includes external parties with an interest in the management of the enterprise's risk to an acceptable level.
- External Partners — Personnel or organizations (e.g., service providers, vendors, organizations that collaborate under a formal agreement) external to the enterprise that participate in the management and communication of cybersecurity risk.

Throughout the risk management steps in Fig. 2, the use of cybersecurity risk registers helps record the progress of management processes. Risk registers also support multi-level stakeholder communications that are critical for enabling cybersecurity risk officers[20] and other practitioners to identify and propose ways to manage relevant cybersecurity risks.

External stakeholders and partners have key roles in identifying, managing, communicating, and monitoring cybersecurity risks. Enterprises increasingly function interdependently with external partners, such as material suppliers, communications and technology providers, cloud service providers, and managed service providers. NIST recommends using C-SCRM plans and activities to ensure that external partners are well-integrated.[21]

Risk monitoring also involves 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. This can help ensure cross-communication among other groups that support risk management, such as human resources, legal, auditing, and compliance management. As a primary compliance indicator, OMB Circular A-123 requires federal agencies to consider their management responsibilities for "the establishment of a government structure to effectively implement, direct and oversee implementation of the Circular and all the provisions of a robust process of risk management

[20] The cybersecurity risk officer has the expertise to identify relevant cybersecurity risks as opposed to an enterprise risk officer who would receive reports on such risks. The cybersecurity risk officer role is increasingly being recognized.
[21] For more information on C-SCRM, see https://csrc.nist.gov/Projects/cyber-supply-chain-risk-management.

and internal control" [3]. These governance structures formalize the relationships across all levels and operating units within a federal agency.

A significant risk to the effectiveness of cybersecurity controls and mitigation actions is the knowledge, training, and experience of the officers in charge of a risk or set of risks. Staff capability should be assessed, since it is a major contributor to upstream ERM risk management effectiveness.

3.1.2. Risk Management Strategy

As part of their governance responsibilities, senior leaders should establish clear and actionable risk management guidance based on the enterprise's mission and objectives. Senior leaders should clearly express guidance regarding risk appetite and risk tolerance, and those tolerance statements should have clear and measurable boundaries where possible to define. Key performance indicators and key risk indicators should be created to warn that these tolerance boundaries are being approached and reported accordingly. These and many other risk management strategies are discussed throughout the IR 8286 series.

To ensure that the enterprise is managing risks to achieve its mission and objectives in the face of cybersecurity risk, the CSF Govern Function states, "The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored" [7]. This statement creates a foundation for organizations implementing risk governance and cybersecurity risk management programs. The Subcategories within the CSF Govern Function provide outcome statements that are linked to informative references to guide an organization in achieving and prioritizing the outcomes of the other five Functions (i.e., Identify, Protect, Detect, Respond, and Recover). Govern activities are critical for incorporating cybersecurity into an organization's broader ERM strategy. The CSF Govern Function addresses an understanding of organizational context; the establishment of cybersecurity strategy and cybersecurity supply chain risk management; roles, responsibilities, and authorities; policy; and the oversight of cybersecurity strategy. By implementing the CSF Govern Function, enterprises link the context of its mission and stakeholder expectations to cybersecurity risk management activities.

Furthermore, the CSF Category, Risk Management Strategy, within the Govern Function states, "The organization's priorities, constraints, risk tolerance and appetite statements, and assumptions are established, communicated, and used to support operational risk decisions" [7]. These CSF Subcategories and their associated informative references are helpful to establish and maintain processes for enterprise risk context. Notably, the IR 8286 series provides details on how to implement these CSF Functions and their risk management Subcategories' outcome statements.

Enterprise leaders should continually review and adjust the risk strategy as the risk landscape evolves (e.g., due to technological and environmental changes). For example, an enterprise that is subject to outside regulation is likely to receive specific guidance regarding updated federal statutes and directives that must be considered when evaluating acceptable risk. Through this monitoring, enterprises can utilize the Govern Function to affect change in lower organizational levels. This risk management strategy allows an enterprise to effectively manage a division, business unit, or department with traceability to system-level actions.

Numerous NIST publications provide guidance regarding risk management strategy content and development. For example, SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View* [11], includes extensive information about setting and implementing strategy. It states that risk management "is carried out as a holistic, organization-wide activity that addresses risk from the strategic level to the tactical level, ensuring that risk-based decision making is integrated into every aspect of the organization." SP 800-39 further points out:

> The first component of risk management addresses how organizations *frame* risk or establish a risk context — that is, describing the environment in which risk-based decisions are made. The purpose of the risk framing component is to produce a risk management strategy that addresses how organizations intend to assess risk, respond to risk, and monitor risk — making explicit and transparent the risk perceptions that organizations routinely use in making both investment and operational decisions. [11]

This guidance is applied in SP 800-37r2 through several tasks within the Prepare step, including Task P-2, Risk Management Strategy [16].

A critical element of the enterprise risk strategy includes the consideration of supply chain risks. By understanding the cyber supply chain in which an organization participates, the organization can better mitigate disruptions to that supply chain (e.g., service outages, third-party vulnerabilities, data breaches). The relevant outcomes to achieving cyber supply chain security are described in the CSF's Supply Chain Risk Management (GV.SC) Category within the Govern Function:

> Cyber supply chain risk management processes are identified, established, managed, monitored, and improved by organizational stakeholders. [7]

Assumptions may occur at all levels of the organization, so it is important to determine internal and external stakeholders' expectations regarding risk communications and to use readily understandable and agreed upon terms and categories, such as strategic objectives, organizational priorities, decision-making processes, and risk reporting or tracking methodologies (e.g., regular risk management committee discussions and meetings).

> An effective ERM program defines and communicates enterprise risk appetite so that meaningful risk tolerance statements can be created, used, and monitored. Risk appetite also reflects strategic risk direction from leadership. As adopted from COSO, OMB Circular A-123 defines risk appetite as "the broad-based amount of risk an enterprise is willing to accept in pursuit of its mission/vision" [3]. With strategic risk direction communicated to the organizational and system levels of the enterprise, cybersecurity officers can apply the guideline when

establishing risk expectations at organizational and system levels. A risk management strategy should also include direction regarding the risk register, such as how entries should be categorized. The use of common risk categories supports the aggregation of various types of risk across the enterprise.

In providing risk strategy direction, it is critical that enterprise leaders also provide guidance regarding risk calculations. The CSF states, "Governance activities are critical for incorporating cybersecurity into an organization's broader enterprise risk management (ERM) strategy" [7]. Therefore, establishing a common scale for assessing levels of risk will support consistent risk estimation, measurement, and reporting. SP 800-221A identifies areas in which this type of outcome may be achieved in the Oversight Category of the Govern Function. It states, "Risk is identified and addressed by risk management programs according to the criteria and expectations of risk governance" [8]. The strategy may also include guidance regarding the mechanisms and frequency of risk reporting. By using the governance activities found in the Govern Function of SP 800-221A [8], enterprise leaders can establish clear metrics and assessment methodologies to provide mechanisms for reporting cybersecurity risk within the established enterprise risk management paradigm.

As cybersecurity risks are recorded, tracked, and reassessed throughout the cycle (as depicted in Fig. 2), this foundation ensures that various types of risk will be consistently communicated and managed to ensure adherence to risk guidance and expectations similarly established across other risk domains within the enterprise. The Federal ERM Practice Guidance suggests "establishing hierarchical decision-making processes that align risk decision-making vertically and horizontally across the organization" [17]. This action aligns the risk management strategy for all relevant stakeholders.

3.2. Identify the Risks

The second step in the risk management life cycle involves identifying a comprehensive set of risks and recording them in the risk register.[22] This includes events that could enhance or impede objectives, such as the risks involved in failing to pursue opportunities. For federal agencies, Circular A-123 [3] requires that the enterprise risk register consider both inherent and residual risks.[23] The COSO ERM Framework further describes these terms and differentiates between actual residual risk and target (desired) risk [10]:

- "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."

[22] Risk identification activities are described in SP 800-30r1, Step 2, Tasks 2-1 through 2-3 [15] and IR 8286A.

[23] While both Circular A-123 and some COSO documents reference inherent risk, this publication focuses on current 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 inputs:

1. Identification of the organization's mission-supporting assets and their valuation
2. Determination of potential threats that might jeopardize the confidentiality, integrity, and availability of those assets and potential information and technology opportunities that might benefit the organization
3. Consideration of the vulnerabilities of those assets
4. Evaluation of the potential consequences of risk scenarios

Risk practitioners often perform risk identification as both a top-down and bottom-up exercise. For example, after the organization has considered critical or mission-essential functions, it may consider various types of issues that could jeopardize those functions as an input to risk scenario development. Subsequently, as a detailed threat and vulnerability assessment occurs, assessors consider how those threats might affect various assets, conducting a bottom-up assessment. This bi-directional approach helps support holistic and comprehensive risk identification. The risk identification process is outlined below and discussed in detail in IR 8286A, Sec. 2.2 [12].

Risk managers should leverage the business impact analysis (BIA) register to consistently evaluate, record, and monitor the criticality and sensitivity of enterprise assets. The BIA's purpose is to correlate the system with the critical mission and business processes and services provided and characterize the consequences of a disruption based on that information. It also enables the ISCP Coordinator to characterize the system components, supported mission and business processes, and interdependencies. The BIA is a key step in implementing the CP controls in SP 800-53 and the contingency planning process overall. IR 8286D [13] details the BIA process and provides a BIA template for organizations to use in their ERM processes that integrates with the rest of the IR 8286 series documentation.

Within a BIA, organizations list high value assets (HVAs), especially those that are reported on the balance sheet in private industry. However, the value of an asset extends beyond its replacement cost. For example, an organization could calculate the direct costs of researching and developing a new product, but the long-term losses of the theft of that intellectual property could impact future revenue, share prices, enterprise reputation, and competitive advantage. Because of this potential impact, it is critical to gain senior stakeholders' guidance regarding the determination of which assets are critical or sensitive. Federal agencies will have additional guidance on how to categorize HVAs. The relative importance of each enterprise asset will be a necessary input for considering the impact portion of the risk analysis.

Following an HVA determination, the following steps inform the BIA:

1. Determine the risk appetite and tolerances for the relevant assets.
2. Perform a criticality and sensitivity analysis of relevant assets.
3. Communicate those analyses with other IR 8286 series processes.

4. Normalize and aggregate cybersecurity risk registers into enterprise cybersecurity risk registers.
5. Executives evaluate enterprise cybersecurity risk registers.
6. Communicate changes to risk appetite back down to managers to restart the process.

3.2.1. Inventory and Valuation of Assets

Since cybersecurity risk partly reflects the effect of uncertainty on digital components that support enterprise objectives, practitioners identify the assets that are necessary to achieve those objectives. SP 800-37r2 points out that risk could impact "organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals" [16]. Similarly, the CSF describes *assets* as "the data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes" [7]. A core concept in ERM is prioritizing attention and resources on assets that have the greatest impact on an enterprise's ability to achieve its mission and, in the case of federal agencies, on the public. This is one way in which cybersecurity risk is optimized; risks that affect the most valuable resources are ultimately assigned the largest risk exposure value based on the impact and likelihood metrics.

Keeping track of an organization's assets has always been a challenge. Personnel assets may not only include the internal workforce but also external service providers and third-party partners, as described in Sec. 3.1. Digital asset tracking problems have been exacerbated by the proliferation of mobile devices (e.g., smartphones, tablets), the Internet of Things (IoT), cloud computing, and bring-your-own-device (BYOD), as well as the convergence of IT and operational technology (OT) systems. It is increasingly difficult to know which computing devices the organization uses, where the organization's data is stored, or how and when it is transmitted, especially when devices and data are constantly changing. Incomplete or inaccurate information on technology assets means that it is not possible to fully quantify those assets or the impacts of cybersecurity risks.

While a BIA may be a good top-down approach, it also receives input and status from the bottom-up aggregation processes of the risk register to ensure that risks are adequately understood as the enterprise's technology landscape shifts. Organizations use cybersecurity risk assessments to categorize asset criticality and sensitivity (see Fig. 2 in IR 8286D [13]). These assessments will be used when updating the BIA register and providing feedback to the cybersecurity risk registers (CSRRs) in a bottom-up process (see Fig. 1 in IR 8286D [13]). By using both top-down and bottom-up analysis processes, the organization manages risk by mission-driven strategy and asset-informed data.

3.2.2. Determination of Potential Threats

Cybersecurity risk is not inherently good or bad. Rather, it represents the effects of uncertain circumstances, so risk managers should consider a broad array of potential positive and negative risks. The following sections primarily deal with negative risks. Additional information about balancing them with positive risks and opportunities is provided in Sec. 3.7.

A *negative risk* represents any circumstance or event with the potential to adversely impact organizational operations (i.e., a threat). The threat could arise from a malicious person with harmful intent or from an unintended or unavoidable situation (e.g., a natural disaster, technical failure, or human errors) that may trigger a vulnerability.[24] Numerous threat modeling techniques are available for analyzing cybersecurity-specific threats.[25] It may be helpful to consider both a top-down approach (i.e., reviewing critical or sensitive assets for what could potentially go wrong, regardless of threat source) and a bottom-up approach (i.e., considering the potential impact of a given set of threat or vulnerability scenarios).

IR 8286A, Sec. 2.2.2 [12] provides a detailed explanation of threat determination. Here are some examples:

- Threat enumerations: The Software Engineering Institute's (SEI) OCTAVE® uses a top-down approach to produce a catalog of potentially harmful outcomes based on the effects of various threat sources and their motives [18]. Other threat modeling techniques, such as MITRE's ATT&CK™ [19], provide a knowledge base of adversarial tactics and techniques based on real-world observations. There are numerous industry sources of cybersecurity-specific threat information, including commercial and non-profit organizations and public-sector sources, like the United States Computer Emergency Readiness Team (US-CERT), Information Sharing and Analysis Centers/Organizations (ISACs, ISAOs), and Automated Indicator Sharing (AIS) feeds.
- Gap analysis: Another source of threat information is a high-level risk assessment from the application of the CSF [7] using a gap analysis. Steps 3 and 4 of that framework describe the consideration of organizational practices and conditions (i.e., a current-state profile), the desired organizational practices (i.e., target-state profile), and a subsequent review of the risk implications of that current state toward the target state. The analysis can be open-ended by using the target state as an input to red-teaming exercises, or the analysis can target specific risks (e.g., phishing, distributed denial of service, ransomware).
- SWOT analysis: One commonly used method that may help organizations identify potential cybersecurity risk outcomes is a SWOT (strengths, weaknesses, opportunities, threats) analysis. Applying SWOT analysis helps users identify opportunities that arise from organizational strengths (e.g., a well-respected software development team) and threats (e.g., supply chain issues) that reflect an organizational weakness. The use of SWOT analysis helps describe and consider the context in Sec. 3.1, including internal factors (i.e., strengths and weaknesses internal to the organization), external factors (i.e., the opportunities and threats presented by the external environment), and ways in which these factors relate to each other.

When building a register of potential cybersecurity risks, the organization should consider risk events that have already occurred in similar organizations. For example, the U.S. Securities and Exchange Commission (SEC) has stated, "Given the frequency, magnitude and cost of

[24] SP 800-30r1 provides information about how to "Identify Threat Sources" and "Identify Threat Events" [15].

[25] This section is intended to introduce the topic of cybersecurity threats in the context of the enterprise. IR 8286A further decomposes cybersecurity threats and threat modeling with practical and actionable guidance related to populating the cybersecurity risk register.

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]" [20].

While it is critical for enterprises to address potential negative impacts on mission and business objectives, it is equally critical — and required for federal agencies — to plan for success. OMB states in Circular A-123 that "the profile must identify sources of uncertainty, both positive (opportunities) and negative (threats)" [3]. However, the notion of "planning for success" by identifying and realizing positive risks (opportunities) is a relatively new concept in CSRM that is influencing other risk management disciplines. The CSF [7] contains a Subcategory[26] and implementation examples and informative references[27] for this concept. Both positive and negative risks currently follow the same processes from identification to analysis to inclusion on the enterprise risk profile. Whatever means are used to determine potential threats, it is important to consider them in terms of both the *threat actors* (i.e., the instigators of risks with the capability to do harm) acting on the threat sources and the *threat events* caused by their actions.

Combinations of multiple risks should also be considered. 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 that affects 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 Sec. 3.3.

During the threat modeling process, practitioners should identify and mitigate instances of cognitive bias. Some common issues of bias include:

- **Overconfidence** — The tendency for stakeholders to be overly optimistic about risk scenarios (e.g., unreasonably low likelihood of a threat event, overstated benefits of an opportunity, exaggerated estimation of the ability to handle a threat)
- **Groupthink** — Rendering decisions as a group about potential threat sources and threat events in a way that discourages creativity or individual responsibility
- **Following trends** — Blindly following the latest trend without a detailed analysis of the specific threats facing the organization
- **Availability bias** — The tendency to focus on issues (e.g., threats) that come readily to mind because one has heard about or read about them, perhaps in ways that do not accurately represent the actual likelihood of a threat event occurring and resulting in adverse impact

[26] GV.RM-07: Strategic opportunities (i.e., positive risks) are characterized and included in organizational cybersecurity risk discussions.
[27] Direct Informative Reference Download is available at https://csrc.nist.gov/extensions/nudp/services/json/csf/download?olirids=all.

3.2.3. Determination of Exploitable and Susceptible Conditions

The next key input to risk identification is understanding the potential conditions that enable a threat event to occur.[28] It is important to consider all types of vulnerabilities in all assets, including people, facilities, and information. For the purposes of this document, a *vulnerability* is 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 (e.g., a wooden structure being flammable). The presence of a vulnerability does not cause harm in and of 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. Identifying negative risks includes understanding the potential threats and vulnerabilities to organizational assets, which can then be used to develop scenarios that describe potential risks.

Automated scanners can quickly identify certain common weaknesses, such as software flaws, missing patches, misconfigurations, or the presence of malware. However, cybersecurity weaknesses are not limited to the hardware and software of an enterprise. The SP 800-53 controls highlight the breadth of potential threats that are germane to cybersecurity, such as those that result from a lack of risk planning associated with continuity of operations (COOP), training, monitoring physical access, power considerations, and supply chain considerations.

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 that are 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 additional information. An effective example of an identified risk in the first scenario might be (as expressed in cause-and-effect terminology), “If a hurricane causes a storm surge, it could flood the data center and damage multiple critical file servers.”

Cybersecurity risks that cause unexpected or unreliable behavior in a system do not always result in the complete failure of an information system to fulfill its duty in support of business objectives. Many elements of a security plan are implemented to support redundancy and resilience so that a highly likely threat event might result in manageable consequences. Resilient enterprise systems may be able to continue operating in the face of adverse circumstances.

By combining the results of Sec. 3.2.1 through 3.2.4, a practitioner can create a set of risk scenarios (described at the beginning of Sec. 3) in the risk description column of the cybersecurity risk register, including the source of uncertainty, predisposing conditions, affected resources, and anticipated result. With this information recorded, risk analysis can proceed as described in the next step.

[28] SP 800-30r1 provides information about how to “Identify Vulnerabilities and Predisposing Conditions” [15].

3.3. Analyze the Risks

In step 3 of the risk management life cycle, 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

Some enterprises use informal risk analysis techniques. However, relying solely on an informal risk analysis may impair effective CSRM decisions in a modern enterprise. A broad array of risk analysis methodologies are available to enable more accurate estimation, including SP 800-30 [15], International Electrotechnical Commission (IEC) 31010:2019 [21], and The Open Group's Open FAIR standards [22].

The following are methods for risk analysis:

- *Qualitative analysis* is based on the assignment of a descriptor, such as low, medium, or high. The scale can be formed or adjusted to suit the circumstances, and different descriptions may be used for different risks. Qualitative analysis is helpful as an initial assessment or when considering intangible aspects of risk.

  To improve the quality of qualitative analysis, values and data can be leveraged from external sources, such as industry benchmarks or standards, metrics from similar previous risk scenarios, or findings from inspections and assessments.

- *Quantitative analysis* involves numerical values that are assigned to both impact and likelihood. These values are based on statistical probabilities and a monetized 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 of financial, technical, or human impacts.

  SP 800-30r1 describes a semi-quantitative assessment that employs "a set of methods, principles, or rules for assessing risk that uses bins, scales, or representative numbers whose values and meanings are not maintained in other contexts" [15]. This model helps translate risk analysis into qualitative terms that support risk communications for decision-makers as well as relative comparisons (e.g., within a particular scale or bin).

Each of these analysis types has advantages and disadvantages, so the type performed should be consistent with the context associated with the risk. When selecting the most appropriate type of risk analysis at the system or organization level, practitioners should consider both consistency with ERM at the enterprise level and the accuracy of measuring cybersecurity risks. The methods to be selected and under what circumstances depend on many organizational factors and might be included in the risk management discussions described in Sec. 3.1. While qualitative methods are commonly used, the practitioner may benefit from considering a quantitative methodology with a more data-driven approach to estimating likelihood and the impacts of consequences. This may help to better prioritize risks or prepare more accurate risk exposure forecasts. However, changing the risk assessment methodology may require time and resources for development and training. A detailed consideration of risk analysis techniques, including worked examples, is provided in the IR 8286 series, and meaningful metrics are discussed in SP 800-55v1[29].

3.3.2. Techniques for Estimating Likelihood and Impact of Consequences

One of the primary goals of CSRM is to identify potential risks that are most likely to have a significant impact, which requires an accurate analysis of risk with regard to the enterprise's risk appetite and system or organizational risk tolerance. IEC 31010 is an international standard that describes and provides guidance on 17 risk assessment techniques that can be used to analyze controls, dependencies, and interactions; understand consequence and likelihood; and measure overall risk [21]. Understanding the likelihood of threat events will also require experimentation, investigation into previous risk events, and research into the risk experiences of similar organizations. IR 8286A, Sec. 2.3.2 [12] provides more details and actionable guidance.

The likelihood and impact elements of a risk can be categorized into subfactors.[30] For example, consider a risk scenario in which a critical business server becomes unavailable to 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. Additionally, the availability of another server with a fault-tolerant connection could mean that the loss of the initial server has little consequence. Timing can also impact risk analysis. If the financial server supports an important payroll function, the impact of a loss occurring shortly before payday may be significantly higher than if it were to occur after paychecks had already been distributed. Impact may vary greatly depending on whether the server is used to archive legacy records or perform urgent stock trades. There are many considerations that go into estimating exposure and the events that can trigger them. Any subfactors that an organization considers should be clearly delineated and defined to ensure consistency in their use.

The calculation of multiple or cascading impacts is an important consideration, and each permutation should be individually included in the cybersecurity risk register. Secondary loss events should be captured with primary loss events to represent the total impact and cost of a risk scenario. The omission of secondary losses in the assessment of a risk scenario would underestimate the total impact, thereby misinforming risk response selection and prioritization. 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 the loss of customers from frustration with unavailable services or penalties resulting from the failure to meet contractual service levels.

[29] https://doi.org/10.6028/NIST.SP.800-55v1

[30] Determining the likelihood and potential adverse impacts of threat events is described in Step 2, Tasks 2-4 and 2-5 of SP 800-30r1 [15].

> Examples of techniques for estimating the probability that a risk event will occur include:
>
> - **Bayesian Analysis** — A model that helps inform a statistical understanding of probability as more evidence or information becomes available
> - **Monte-Carlo** — A simulation model that draws on random sample values from a given set of inputs, performs calculations to determine results, and iteratively repeats 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

Both tangible (e.g., direct financial losses) and less tangible impacts (e.g., reputational damage and impairment of mission) should be considered when evaluating the potential consequences of risk events. 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 states 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.

Practitioners document and track the potential consequences of each cybersecurity risk that would significantly impact enterprise objectives, such as causing material reputational damage or significant financial losses to the enterprise. Documenting and tracking these consequences at the organization or system level provides cybersecurity risk inputs to the ERM program (see Sec. 3.8).

The estimation of the likelihood and impact of a risk event should account for 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. [2]

The estimated likelihood and impact of each risk are recorded in the appropriate columns in the cybersecurity risk register. After risk responses are determined, the analysis should be revised to reflect the mitigation of likelihood and impact for each risk response. The residual risk (i.e., the remaining risk after applying risk responses) should then be recorded in the risk register's Residual Risk column. To simplify the process of normalizing cybersecurity risk registers when developing an enterprise risk register (see Sec. 3.8), a consistent time frame should be used for estimating the likelihood of each risk. Likewise, the level of impact helps to normalize the risk during the aggregation and prioritization process.

3.4. Prioritize Risks

After identifying and analyzing applicable risks and recording them in the cybersecurity risk register, the priorities of those risks should be determined and indicated based on the likelihood that a threat event will occur and result in an adverse impact.[31] IR 8286B [23] covers this topic in greater detail.

A cybersecurity risk can adversely affect organizational objectives. Based on the analysis conducted using the processes described in Sec. 3.3, such effects could range from negligible to severe, so exposure determination is important. Additionally, since organizations have limited resources, it is helpful to sort the risks within the register in order of importance to prioritize risk response. In the cybersecurity risk register (CSRR) template in Fig. 4, this result helps complete the Priority column.[32]

When completing the Priority column of the CSRR, consider the following:

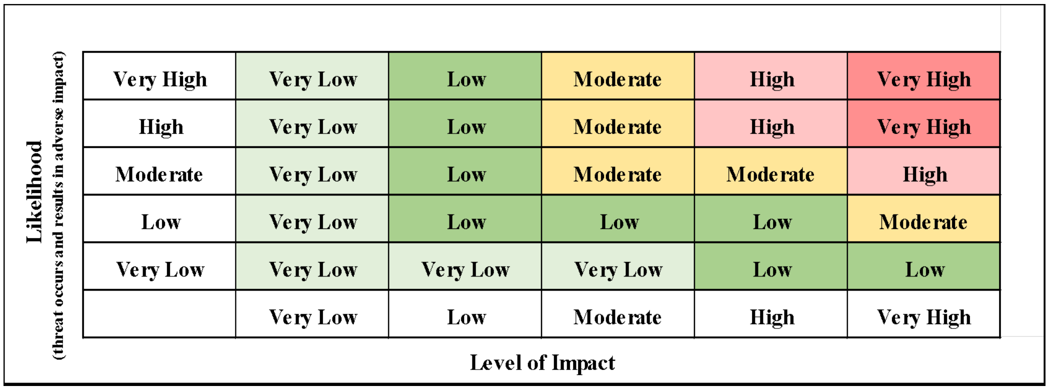
- How to combine the calculations of likelihood and impact to determine exposure[33]
- How to determine and measure the potential benefits of pursuing a particular risk response
- When to seek additional guidance on how to evaluate risk exposure levels (e.g., while evaluating exposures that are germane to risk tolerance statements)

Practitioners use both qualitative and quantitative models to calculate and communicate about exposure. Figure 5 (derived from Table I-2 of SP 800-30 [15]) demonstrates the use of qualitative descriptors for likelihood and impact as well as how these might be used to determine an overall exposure value.

[31] Risk identification activities are described in SP 800-30r1, Task 2-6 "Determine Risk" [15] and IR 8286B [23], Sec. 2.2.

[32] While risks in the CSRR are assigned a priority to help rank their relative importance, this prioritization is distinct from (but may help inform) the enterprise-level prioritization performed by senior leaders to create the enterprise risk profile.

[33] The formula for calculating risk exposure is the total loss if the risk occurs multiplied by the probability that the risk will happen. Loss is calculated through a traditional BIA used in conjunction with the risk register model to inform the senior level decision-making process. See SP 800-34 for additional information.



Likelihood
(threat occurs and results in adverse impact)

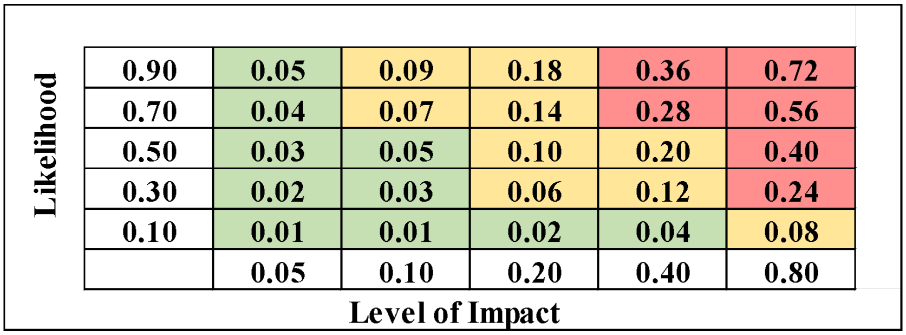
Very High	Very Low	Low	Moderate	High	Very High
High	Very Low	Low	Moderate	High	Very High
Moderate	Very Low	Low	Moderate	Moderate	High
Low	Very Low	Low	Low	Low	Moderate
Very Low	Very Low	Very Low	Very Low	Low	Low
	Very Low	Low	Moderate	High	Very High

Level of Impact

Fig. 5. Likelihood and impact matrix derived [15]

Each risk is evaluated based on its likelihood and impact as determined during risk analysis. The thresholds for ranges of exposure can be established and published as part of the enterprise governance model and used by stakeholders to prioritize each risk in the register.

Figure 6 depicts a quantitative example.



Likelihood

0.90	0.05	0.09	0.18	0.36	0.72
0.70	0.04	0.07	0.14	0.28	0.56
0.50	0.03	0.05	0.10	0.20	0.40
0.30	0.02	0.03	0.06	0.12	0.24
0.10	0.01	0.01	0.02	0.04	0.08
	0.05	0.10	0.20	0.40	0.80

Level of Impact

Fig. 6. Example of a quantitative risk matrix

In this illustration, the enterprise has provided guidance that any risk above 0.20 (based on probability x impact) represents a high risk, and risks rated between 0.08 and 0.2 are designated as moderate.

While the risk exposure determination will strongly influence prioritization, other factors may also influence those decisions, such as enterprise context or stakeholder priorities. Stakeholders might also use the risk management strategy or other directive to define a minimum level of exposure to include on the risk register. While cybersecurity risks should not be arbitrarily omitted from the register, there are likely to be many that represent such a low exposure that they need not be included. Guidance for this threshold should be applied consistently throughout the enterprise. For cybersecurity risks that *are* included and prioritized in the CSRR, an evaluation should be performed to identify appropriate risk responses.

3.5. Plan and Execute Risk Response Strategies

The fifth step of the risk management life cycle is to determine the appropriate response to each risk. While this section summarizes risk response strategies, Sec. 2.3 of IR 8286B [23] covers the topic in greater detail.

The goal of effective risk management is to identify ways to keep risk aligned with the risk appetite or tolerance as cost-effectively as possible. In this stage, the practitioner will determine whether the exposure associated with each risk in the register is within acceptable levels based on the potential consequences. If not, that practitioner can identify and select cost-effective risk response options to achieve cybersecurity objectives.

Planning and executing risk responses is an iterative activity and should be based on the risk strategy guidance described in Sec. 3.1.2. As the risk oversight authorities monitor the success of those responses, they will provide financial and mission guidance 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 Sec. 3.6. Risk responses themselves may introduce new risks. For example, adding multi-factor authentication to a business system to reduce an access control risk may introduce a new risk of decreased productivity when users have difficulty using the new technology.

While there is some variance among the terms used by risk management frameworks, there are four types of actions available (illustrated in Table 2) for responding to negative cybersecurity risks: *accept*, *transfer*, *mitigate*, and *avoid*.

Table 2. Response types for negative cybersecurity risks

Type	Description
Accept	Accept cybersecurity risks within risk tolerance levels. No additional risk response action is needed except for monitoring.
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 the loss of customer trust.
Mitigate	Apply actions (e.g., security controls discussed in Sec. 3.5.1) that reduce the threats, vulnerabilities, and impacts of a given risk to an acceptable level. Responses could include those that help prevent a loss (i.e., reducing the probability of occurrence or the likelihood that a threat event materializes or succeeds) or that help limit such a loss by decreasing the damage and liability.
Avoid	Apply responses to ensure that 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.

Risk response will often involve creating a *risk reserve* to avoid or mitigate an identified negative risk or to realize 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 that the opportunity is realized or that the threat is avoided. For example, the technical skill of subject-matter experts to recover after a cybersecurity attack may not be available with current staffing resources. A risk reserve can also be used with the *accept* response type to address this (e.g., 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 general, people, processes, and technology combine to provide risk management controls that can be applied to achieve an acceptable level of risk. Examples of controls include:

- **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 poor authentication practices (e.g., weak or reused passwords) that could lead to the disclosure of sensitive customer financial information and to employees of the software provider gaining unauthorized access and tampering with the financial data. The organization can apply several deterrent controls and document the applied control identifiers and any applicable notes in the Risk Register Comments column, including warning banners and the threat of prosecution for any threat actors who 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 can install 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 should be encrypted so that it protects its data if the file system is exfiltrated.

In many cases, mitigation to bring exposure to negative cybersecurity risks within risk tolerance levels is accomplished using security controls. For example, if the Risk Executive Function declares that the organization must avoid risks with likelihood and impact values of High/High for all costs over $500,000, the Risk Response Type column of the risk register (see Fig. 4) can be updated with a response type from Table 2. The Risk Response Description column can be populated with the CSF Subcategory outcomes and SP 800-53 control descriptions that address negative risks, as illustrated in Fig. 7. While including a particular informative reference (e.g., security controls or CSF Categories and Subcategories) may be helpful in guiding and describing a risk response, additional information is likely to be required.

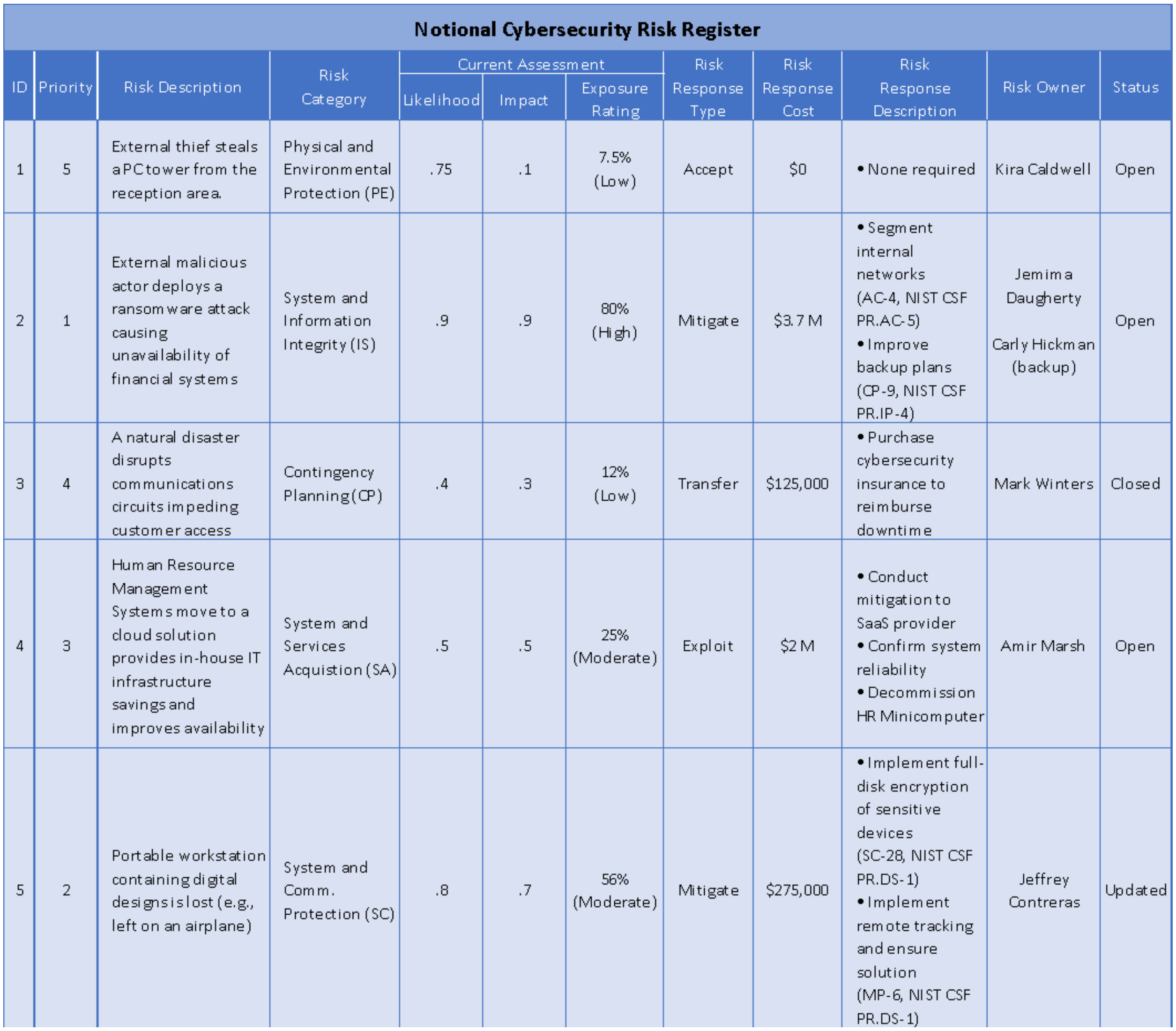
SP 800-53 provides a comprehensive catalog of technical and non-technical (i.e., administrative) controls that act as "safeguards or countermeasures prescribed for an information system or an organization to protect the confidentiality, integrity, and availability of the system and its information." 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 manage privacy risks" [5].

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. SP 800-53A, *Assessing Security and Privacy Controls in Information Systems and Organizations*, provides detailed criteria for examining the application of controls and processes, testing control effectiveness, and conducting interviews to confirm that the mitigation techniques are likely to achieve their intended result [24].

3.5.2. Responding to Residual Risk

Section 3.2 briefly introduced the concept of residual risk, which is what remains after a risk response (e.g., those listed in Table 2) has been applied. The residual risk can be calculated using the same methods for calculating current risk, as discussed in Sec. 3.3. If the residual risk is beyond the acceptable level of risk, then the risk owner should evaluate whether the risk can be brought to an acceptable level (e.g., by applying additional security controls). If a risk response exceeds the benefit of the activity at risk, the risk owner may wish to explore ways to avoid the risk altogether.

The risk register provides an important mechanism for recording and communicating risk decisions. Figure 7 provides a completed notional cybersecurity risk register.



Notional Cybersecurity Risk Register

ID	Priority	Risk Description	Risk Category	Current Assessment			Risk Response Type	Risk Response Cost	Risk Response Description	Risk Owner	Status
				Likelihood	Impact	Exposure Rating					
1	5	External thief steals a PC tower from the reception area.	Physical and Environmental Protection (PE)	.75	.1	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 (IS)	.9	.9	80% (High)	Mitigate	$3.7 M	• 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)	.4	.3	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 Acquistion (SA)	.5	.5	25% (Moderate)	Exploit	$2 M	• Conduct mitigation 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 Comm. Protection (SC)	.8	.7	56% (Moderate)	Mitigate	$275,000	• Implement full-disk encryption of sensitive devices (SC-28, NIST CSF PR.DS-1) • Implement remote tracking and ensure solution (MP-6, NIST CSF PR.DS-1)	Jeffrey Contreras	Updated

Fig. 7. Excerpt from a notional cybersecurity risk register

A key factor in achieving effectiveness is using a cost-benefit analysis (CBA). IEC 31010 states that a CBA "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" [21]. Through this analysis, the practitioner can consider the exposure factor cost (i.e., the likely cost of exposure based on the likelihood and impact of a residual risk, as recorded in the risk register) compared to the potential cost of the risk response for that residual risk. For example, consider Risk #5 from Fig. 7. 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 opportunities. The labor and software to apply full-disk encryption and remote tracking on laptops with sensitive data would cost $275,000, so the benefit is worth the cost of the countermeasures.

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

Circular A-123 states, "Residual risk is the exposure remaining from an inherent risk after action has been taken to manage it, using the same assessment standards as the inherent assessment" [3].

Enterprise risk officers document residual risks on the enterprise risk profile and analyze those risks against applicable enterprise risk appetite and tolerance levels set by senior leadership. They then determine whether any additional risk response plans or actions are needed. Enterprise risk officers must communicate these proposed plans and actions to the enterprise's senior management to make the final decisions and then communicate those decisions appropriately and in a timely way to risk owners at lower levels, such as organization or system levels.

Federal agencies are required to develop a risk register-like report called *a plan of actions and milestones* (POA&M) for each system. The document is an output of the *Assess* step described in SP 800-37r2 and documents planned risk mitigation actions, including those that cannot be immediately implemented (e.g., due to operational requirements or resource unavailability). A POA&M "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 action and milestones are informed by the risk management strategy developed as part of the risk executive (function)…" [16]

3.5.3. When a Risk Event Passes Without Triggering the Event

Risk responses will often be adjusted as opportunities and threats evolve. This is similar to the project management concept of the "cone of uncertainty" in that understanding about an identified risk will grow over time. For changes in identified risk, one mitigation technique is the use of risk reserves, as introduced in Sec. 3.5. For this risk response, it is important that the risk owners collaborate with the acquisition or procurement teams and budget owners. With appropriate budget planning, risk reserves can be released for other predetermined funding requirements after the risk has been reduced to an acceptable level or the time for the risk to occur has passed.

While many industry-based enterprises can return unused funds to shareholders or pay down corporate debt, unused reserves are more difficult for government agencies to use without preplanning. Most government procurement cycles are rigidly based on the government fiscal year. Identified opportunities can be "planned for" in government procurement cycles as "optional" tasking or purchases. For example, unused funds could be used to accelerate the IT refresh cycle to address cybersecurity risks (e.g., CPU vulnerabilities that resulted in performance losses when patched). If the current fiscal year only allows for the purchase of half of the required materials, an option can be included at the time of the base contract award for the other half of the materials but not funded at the time of the based contract award. When the practitioner liberates the risk reserve after the chance of the negative risk occurring has passed, the funding can be used to exercise the already awarded option that lacked the initial funding when the base contract was awarded. Exercising an option in government contracting is trivial (often 30 days or less) when compared to the long lead time for initial contract procurements. See the "Integrate and Align Cybersecurity and Acquisition Processes" section of IR 8170 [4] for more information on preplanning for government agencies.

The CSF states that a Target Profile "considers anticipated changes to the organization's cybersecurity posture, such as new requirements, new technology adoption, and threat intelligence trends" [7]. If an organization used the CSF to create a list of products or services for addressing identified risks, the risk reserve can be used to acquire these predetermined risk mitigation solutions. Once a product or service is purchased, the Target Profile can also be used to track and address residual cybersecurity risk using the risk register.

3.6. Monitor, Evaluate, and Adjust

Step 6 in Fig. 2 (Monitor, Evaluate, and Adjust) focuses on managing cybersecurity risks to support mission and business objectives. IR 8286C [25], Sec. 5 provides greater detail on the subject.

By protecting the value provided by enterprise information and technology, CSRM requires the continual balancing of benefits, resources, and risk considerations. As an input to ERM, CSRM requires a dynamic and collaborative process to maintain that balance by continually monitoring risk parameters, evaluating their relevance to organizational objectives, and responding accordingly when necessary (e.g., by adjusting controls). The risk register provides a formal communication vehicle for sharing and collaborating on cybersecurity risk activities as an input to ERM decision-makers.

Ongoing dialogue is needed among all relevant stakeholders, including the initial agreement and understanding of internal/external context and the discussion, determination, and implementation of risk responses. While such discussions often occur within a given business unit or subordinate organization, the enterprise will benefit from broader, frequent, and transparent communication regarding risk options, decisions, changes, and adjustments to improve the quality of information used in enterprise-level decisions. The evolving cybersecurity risk registers and profiles provide a formal method for communicating institutional knowledge and decisions regarding cybersecurity risks and their contributions to ERM.

3.6.1. Continuous Risk Monitoring

Because cybersecurity risks and their impacts on other risks frequently change, enterprise risk conditions should be continually monitored to ensure that they remain within acceptable levels.[34] 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. Proactive activities, including the examples listed in Table 3, support that kind of culture.

Table 3. Examples of proactive risk management 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 effectively managing 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	Foster an environment in which employees and partners may openly and proactively report potential risk situations without fear of reprisal.

Each risk in the register is assigned a risk owner, as described in Table 1. The risk owner is accountable for applying the priority (described in Sec. 3.4) to select and assign appropriate risk responses while considering business objectives and performance targets. ERM leadership (e.g., the Risk Executive Function described in SP 800-39) should ensure that accountability. There may be a distinction between responsibility and accountability for risk ownership. For example, in a federal agency, responsibility for information system risks might be assigned to a System Owner, but accountability might be assigned to an Authorizing Official. It is not the intent of this report to prescribe an approach but to remind the reader that enterprise risk strategy should clearly describe the roles that will be responsible and accountable for risk decisions at each organizational level.

ERM programs, policies, and processes should specify the frequency and methods for monitoring, evaluating the effectiveness of, and adjusting risk responses. They should also define the approved governance bodies to discuss, approve, and communicate the most significant risks and their plans.

If the risk response for a given risk (or set of risks) requires a funding or schedule consideration, specific monitoring and measurement milestones can be included in the associated risk response plan. The risk owner can then identify performance measures or trends (e.g., deliverable artifacts or software development achievements) that represent milestones in addressing the risk. Achieving those milestones may trigger the release or repurposing of 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

[34] Continuous monitoring is described in detail in several NIST publications including SP 800-30, SP 800-37, SP 800-39, SP 800-137, IR 8286C, and the IR 8011 series. These and other publications are available at https://csrc.nist.gov.

be beneficial for the monitoring process to identify that a given risk is unlikely to occur, allowing the risk owner sufficient time to reallocate those reserves before other funding deadlines.

Based on ongoing cost-benefit analysis, the enterprise should continually monitor the risk register, including those risks that were accepted as residual risk. By continually refreshing the risk register and risk profile artifacts described in this report, monitoring and adjustment will be straightforward. It is important to communicate and benefit from the lessons learned from previous practice and actual risk events. By examining adverse events and losses from the past and reviewing missed opportunities (including those missed due to a risk-averse mindset), an enterprise can improve its risk management model and organizational outcomes.

Many organizations employ automated processes and software to support continuous risk monitoring. NIST and its National Cybersecurity Center of Excellence (NCCoE) have developed extensive guidance regarding the technical mechanisms that are available to perform and assess information security continuous monitoring (ISCM) [26]. For ISCM to provide meaningful input into ERM processes, the ISCM must be designed and operated in light of the ERM strategy described above. In this way, the risk dashboard and associated reports provide a visual representation of the information in the risk register. Examples of systems that use such a dashboard include the Department of Homeland Security (DHS) Continuous Diagnostics and Mitigation (CDM) system and the Department of Defense (DoD) Enterprise Mission Assurance Support Service (eMASS).

3.6.2. Key Risk Indicators and Key Performance Indicators

Risk tolerance is addressed through the application of various risk responses, including security controls. Even when risks are identified and marked as accepted, they need to be measured to ensure that they remain within established risk tolerance parameters. Measuring the performance of those controls through key performance indicators (KPIs), especially metrics that represent key risk indicators (KRIs), enables the oversight and management of risk tolerance. Section 5 of IR 8286C [25] provides greater detail.

KRIs should be defined with regard to the given risk exposures that have been identified in the previous sections. Executives should ensure that risk appetite statements focus on ensuring the success of mission and business objectives. For example, if a federal agency has a strategic objective to ensure the protection of user data, the agency’s risk appetite statement might be, “Ensure that only authorized parties have access to federal systems.” Therefore, a corresponding risk tolerance statement might be, “We will issue unique user accounts, and our computer systems will audit both positive and negative logon events.” The agency can deploy an audit control to determine whether a breach occurred. However, that audit control looks backward and does not support a plan to thwart the attack. The agency could employ KRIs that provide a leading metric (e.g., detection of increasing external reconnaissance scanning activity) that might indicate an impending attack [28]. Other indicators might be to data-mine captured network data for information that might indicate that an adversary is preparing to move its payload into the enterprise to exfiltrate data. Similarly, an organization might assess download times, network traffic surges, account auditing, or statistical deviations from normal user behavior. This second set of indicators is actionable because they provide leading metrics to proactively address risks in contrast to audit-based findings.

Cybersecurity KRIs can be *positive*, such as the number of critical business systems that include strong authentication protections. They also can be *negative*, such as the number of severe customer disruptions in the last 90 days. Additional measures may include compliance measures, performance targets for positive risk, and objectives for balancing risk and reward.

Based on the monitoring and reporting of KRIs and KPIs, 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 a periodic review of risk appetite, tolerance, KPIs, and KRIs.

3.6.3. Continuous Improvement

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

The Plan-Do-Check-Act (i.e., The Deming Cycle) is a well-known model for achieving the ongoing effectiveness of any process, and it applies well to CSRM. Earlier in Sec. 3, this report described methods for the Plan and Do elements — essentially, planning based on enterprise direction and carrying out activities to achieve an acceptable level of cybersecurity risk. Section 3.6.1 describes the Check element, where the practitioner 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, the identification of threats and opportunities, the analysis of resulting exposure, and the implementation of responses — and that the risk register is the vehicle for all of those communications. Each of these activities provides a chance for feedback and documenting lessons learned to drive subsequent improvement. Practitioners can adjust risk management processes for emerging and evolving threats and opportunities 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).

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

3.7. Considerations of Positive Risks as an Input to ERM

Planning for success is equally as important as avoiding disasters. As mentioned in Sec. 3.2.2, OMB states in Circular A-123 that regarding the inclusion of opportunities (positive risks) as a function of the ERM profile, "the profile must identify sources of uncertainty, both positive (opportunities) and negative (threats)" [3].

In the CSRM discipline, a significant portion of risk information is collected and reported with regard to weaknesses and threats that could result in negative consequences. However, positive risks (opportunities) also inform decisions by senior leaders for setting the risk appetite and tolerance of the enterprise. For example, conducting a SWOT analysis that considers strengths *and* weaknesses as well as threats *and* opportunities may be a useful exercise.

Consider, for example, an organization that is evaluating moving a major financial system from an in-house data center to a commercial hosting provider. If the organization maintains vast amounts of land and warehouses, the move could be considered a strength of the organization, and they might increase revenue by offering space to a commercial vendor to host both their own and other organizations' data centers. The Federal Government has realized many opportunities of this nature, including consolidating payroll functions under the National Finance Center (NFC) and consolidating reporting requirements in the Department of Justice Cyber Security Assessment and Management (CSAM) application.

Section 3.2.2 describes the need to treat threat actors and threat sources as inputs into an estimation of risk. If the enterprise chooses to include positive risk scenarios in the register, then the process should similarly consider *sources of opportunity* that might provide benefits. A consideration of both threats and opportunities may enable discussions regarding the benefits and risks of a particular endeavor. Alternatively, the organization could manage an *opportunity risk register* separately from the traditional threat-based risk register, since positive risks (i.e., opportunities) often have to be assessed on a slightly different scale.

In addition to the threat modeling examples above, 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 agencies like 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 asks 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 to determine other inputs, such as those described in Sec. 3.2.3 and Sec. 3.2.4.

With regard to positive risk response, consider the previous example of an organization that has identified the positive risk of increasing revenue by providing physical space for a commercial vendor to offer an outsourcing service. 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 colocation. The Risk Response Type column of the risk register should also be updated using a response type from Table 5, the comment field updated to contain information that is pertinent to the opportunity, and the residual risk uncertainty of not realizing the opportunity calculated, as discussed in Sec. 3.5.2.

With these controls and methods in place and assessed as effective, the remaining risks can be analyzed to determine the residual impact, likelihood, and exposure, as described in Sec. 3.3. 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.

Where positive risks are to be considered and included in risk registers, there are four generally used response types, as shown in Table 4.

Table 4. Response types for positive cybersecurity risks

Type	Description
Realize	Eliminate uncertainty to make sure the opportunity is actualized (sometimes referenced as “exploit”).
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).

As with negative risks, positive entries in the cybersecurity risk registers may be normalized and aggregated into the enterprise-level risk register.

3.8. Creating and Maintaining an Enterprise-Level Cybersecurity Risk Register

A key outcome of the risk identification and communications elements is the ability to create an enterprise cybersecurity risk register as input to the broader enterprise risk register (Sec. 3.9). As described throughout Sec. 3, applying a consistent risk register with agreed-upon criteria and categories enables various data points to be normalized, aggregated, and sorted into an enterprise view. While this section highlights the aggregation, normalization, analysis, and prioritization of CSRRs, Sec. 2 of IR 8286C [25] provides greater detail on the topic. This document presents the CSRR as a table and in automated formats (i.e., JSON formats), since many organizations maintain formal and automated applications that provide detailed tracking and reporting (e.g., a GRC product).

A component of ERM is information and communications technology risk management (ICTRM), which is a category of technological risks that may face an enterprise (e.g., cybersecurity, privacy, and supply chain). ERM and ICTRM have several points of integration. First, enterprise governance activities for ERM direct the strategy and methods for ICTRM and other risk management disciplines to use. Based on this guidance, each discipline within each organization uses risk registers to document its risks. In the case of ICTRM, risks are derived from system-level assessments. Next, these risk registers are aggregated, normalized, analyzed, and used to create enterprise-level risk registers for each discipline. These, in turn, become part of a broader enterprise risk register that encompasses all disciplines. Therefore, ICT risks are managed in parallel and then brought together for evaluation in the ERR. SP 800-221A [8] provides greater detail on the ICTRM process.

As shown in Fig. 1, risk registers from all ICT risks — including cybersecurity — are composed and maintained at the enterprise (including higher-level and lower-level enterprises), organizational (including suborganizations and business units), and system levels.[35] Each level of the enterprise has a unique set of cybersecurity risks that must be included when considering enterprise risk. Integrating the contents of lower level CSRRs into higher level registers allows for the effective transfer of risk information from CSRM to ERM in formats and terms that are familiar to senior leaders. Figure 8 illustrates this flow of information.

[35] OMB Circular A-130 defines an *information system* as “a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information” [6].

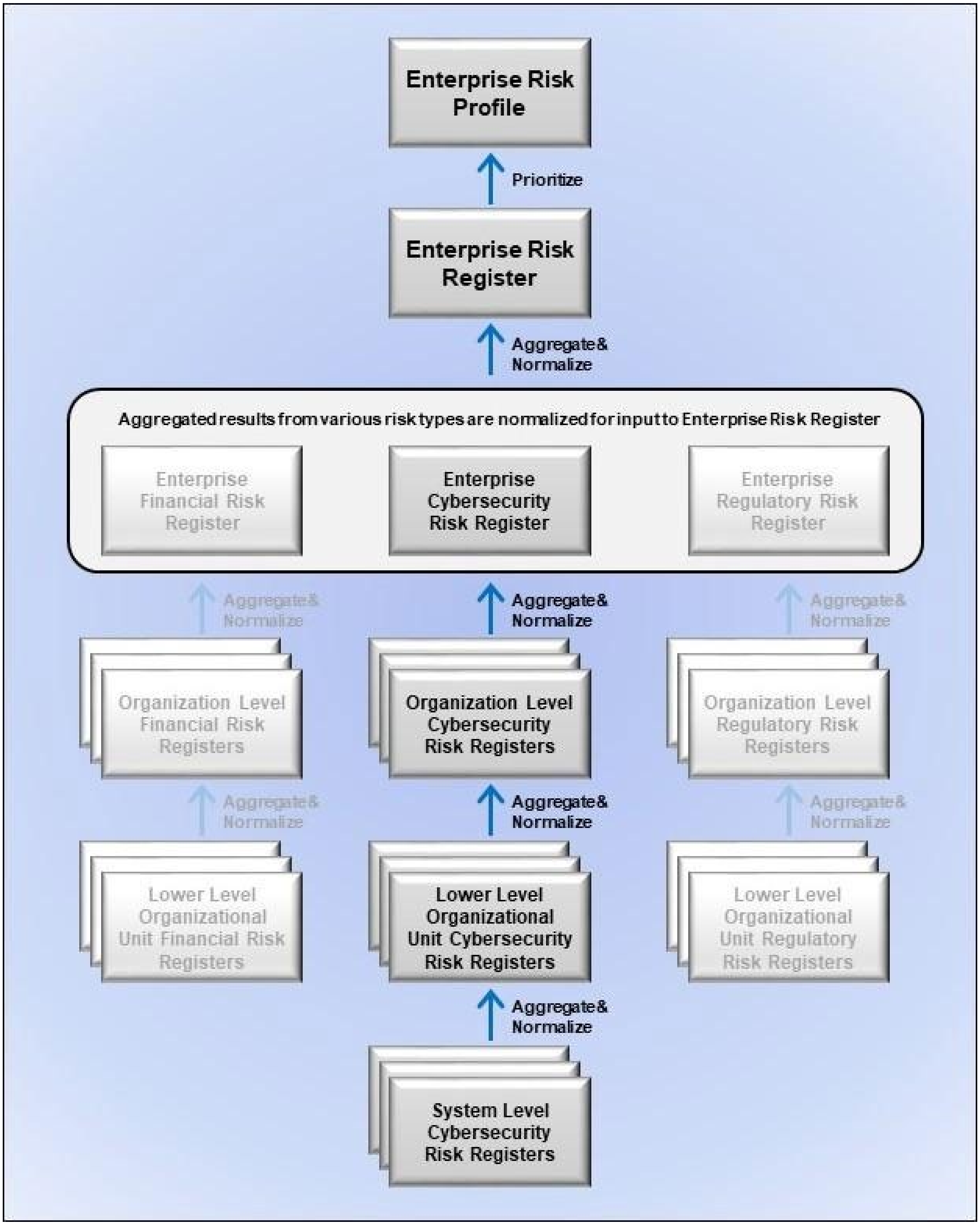

Enterprise Risk Profile
Prioritize
Enterprise Risk Register
Aggregate& Normalize
Aggregated results from various risk types are normalized for input to Enterprise Risk Register
Enterprise Financial Risk Register
Enterprise Cybersecurity Risk Register
Enterprise Regulatory Risk Register
Aggregate& Normalize
Aggregate& Normalize
Aggregate& Normalize
Organization Level Financial Risk Registers
Organization Level Cybersecurity Risk Registers
Organization Level Regulatory Risk Registers
Aggregate& Normalize
Aggregate& Normalize
Aggregate& Normalize
Lower Level Organizational Unit Financial Risk Registers
Lower Level Organizational Unit Cybersecurity Risk Registers
Lower Level Organizational Unit Regulatory Risk Registers
Aggregate& Normalize
System Level Cybersecurity Risk Registers

Fig. 8. Integration of CSRRs into enterprise risk profile

As the risk registers from each system and organization are completed, they are provided to the designated risk officers at the relevant level (i.e., system or organization) and shared with senior management to conduct the following actions:

1. Aggregate risks in similar categories into a concise view. This process can be time-intensive if executed manually using spreadsheets. Using automation is recommended for efficiency and to reduce errors due to manual processing (see IR 8286C [25]).
2. Normalize risks to ensure that definitions and values as recorded by various enterprise entities are consistent (see IR 8286C [25]).
3. Analyze risks to determine their relevance at the current risk register level (see IR 8286C [25]).
4. Prioritize risks based on whether they need to be promoted to the next level (see IR 8286C [25] and IR 8286B [23]).
5. Optimize risks to meet risk tolerance and operational targets (see IR 8286B [23]).

Enterprise risk officers collect all risk inputs — including the CSRRs — and analyze potential risk events, consequences, and impacts at the enterprise level to create the ERR. The aggregated and prioritized ERR is the ERP that enables key executive stakeholders to stay aware of critical risks, including those that are related to cybersecurity. For some organizations, this information will need to be provided to senior managers who have a fiduciary duty to remain aware of and help manage risks (discussed in Sec. 4). In this way, enterprise leaders will have the necessary information and opportunity to consider cybersecurity exposure as factors for budgets or corporate balance sheet reporting. Section 3 of IR 8286C provides greater detail on the integration of cybersecurity risk into the ERR/ERP.

Private-sector and public-sector enterprises will benefit from the use of this risk register integration process, and OMB A-123 mandates the creation of an ERP for federal agencies.[36]

> The primary purpose of a risk profile is to provide analysis of the risks an [enterprise] 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]

This prioritization is supported by one of COSO’s key principles: “The organization prioritizes risks as a basis for selecting responses to risks” [10]. Prioritization helps managers evaluate the costs and benefits of allocating resources to mitigate one risk compared to another.

As part of the risk guidance, enterprise leaders will designate ERM process participants and the responsibilities of each role. That guidance should declare the role responsible for creating and maintaining the enterprise risk register, the frequency with which the register will be updated,

[36] Special treatment and communication flow that are germane to the enterprise-level treatment of risk prioritization are discussed in Sec. 4 of this document.

and how the risks within the register will be communicated to various stakeholders. This report will consider that role to be assigned to the enterprise risk officer, although the responsibility could fall upon any designated party, as described in Sec. 3.1.1.

The creation and maintenance of the enterprise risk register also supports a periodic review of the enterprise risk guidance, including risk definitions, context, and risk appetite criteria. It provides an opportunity to review and validate enterprise definitions for risks, risk categories, and risk assessment scales. If any changes or updates to the risk context or guidance need to occur, the enterprise risk officer (or equivalent) likely has sufficient seniority to ensure appropriate updates to those enterprise processes. Cybersecurity executives should consider any positive cybersecurity risks that are present in the rolled-up report and add other opportunities as inputs to the enterprise risk register.

3.9. Cybersecurity Risk Data Conditioned for Enterprise Risk Roll-Up

To support the subsequent aggregation of various risk registers, enterprise risk guidance should identify the enterprise objectives to which various types of cybersecurity risk should be aligned. Section 4 of this report describes an enterprise risk profile that reflects risks that may impact four discrete enterprise objectives: strategic, operations, reporting, and compliance [1]. These same four objectives were key factors in the original COSO ERM framework and are often used as guideposts for enterprise risk reporting. Clear direction from senior leaders about how to align various types of cybersecurity risk with enterprise objectives will help enable subsequent aggregation, normalization, and prioritization.

Objective categories include:

- **Strategic:** Risks related to the implementation of a new service offering; cybersecurity issues that might impact an upcoming federal agency merger or private-sector acquisition
- **Operations:** Cybersecurity issues regarding existing operational systems, such as a ransomware attack that disables a manufacturing line; business continuity/disaster recovery issues
- **Reporting:** Cybersecurity risks regarding the availability, integrity, and confidentiality of accounting or other financial management systems
- **Compliance:** Cybersecurity risks, where a negative event might result in a failure to meet a contractual service agreement or in a regulatory penalty or fine

If the cybersecurity risk register employed SP 800-53 families as its organizing principle for categories, a predetermined mapping between the family and one of the four enterprise objectives could streamline the process. Direction may be needed regarding how to account for risks that cross multiple boundaries and how each organizational level should perform an aggregation of subordinate risk registers.

Appendix D provides a notional enterprise risk register that combines both federal agency and critical infrastructure risks to illustrate the integration of various cybersecurity risks alongside other key enterprise risks. Table 5 provides an excerpt from the larger Appendix D table to illustrate a notional example of each of the enterprise risk register's fields.

Table 5. Excerpt from a notional enterprise risk register

Register Element	Notional Example
ID (Risk Identifier)	1
Priority	5
Risk Description	Retiring staff lead to personnel shortages
Risk Category	Operational Risk
Current Assessment — Financial Impact	OpEx M CapEx L
Current Assessment — Reputation Impact	L
Current Assessment — Mission Impact	M
Current Assessment — Likelihood	M
Current Assessment — Exposure Rating	M
Risk Response	• Improve hiring diversity • Improve employee benefits packages per recent survey and discussions
Risk Owner	Dwayne Rhodes (Human Resources Department)
Status	Open

Table 6 describes each of the elements in the example enterprise risk register.

Table 6. Descriptions of the notional 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). 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.
Risk Category	An organizing construct that helps to evaluate similar types of risk at the enterprise level and to consolidate and normalize information from subordinate risk registers. Organizations draw from many available taxonomies of risk categories; these examples use the taxonomy described in the U.S. Government Federal ERM Playbook [2].
Current Assessment — Financial Impact	An analysis of the potential financial benefits or consequences resulting from this scenario, including cost considerations from the CSRRs. While this element could be quantitative, it is often qualitative (e.g., high, moderate, low) at the enterprise level. Financial considerations may be expressed as (1) capital expenditures (CapEx) that represent a longer-term business expense (e.g., property, facilities, equipment) and (2) operating expenses (OpEx) that support day-to-day operations.
Current Assessment — Reputation Impact	An 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.
Current Assessment — Mission Impact	An analysis of the potential benefits or consequences that the scenario might have on the ability of the enterprise to successfully achieve mission objectives.

Register Element	Description
Current Assessment — Likelihood	An estimation of the probability, before any risk response, that this scenario will occur. This considers the effectiveness of current key controls.
Current 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	The designated party responsible and accountable for ensuring that the risk is maintained in accordance with enterprise requirements. The risk owner may work with a designated risk manager who is responsible for managing and monitoring the selected risk response.
Status	A field for tracking the current condition of this risk and any next steps.

There is value in both a single point of reference (i.e., the register) and detailed risk information (i.e., the risk detail report). The risk register provides an easily consumed summary for understanding the risk landscape, while the detailed version provides additional information. The risk detail report also enables additional information, such as historical information, detailed risk analysis data, and information about individual and organizational accountability.

Additional information to include in an enterprise risk detail report might include:

- Detailed risk information (e.g., full risk statement, detailed scenario description, KRIs, enterprise status for this particular risk)
- Information regarding various risk roles (e.g., risk owner, risk manager, risk approver) and affected stakeholders
- Historical timeline information (e.g., last update date, next expected review)
- Risk analysis information, including an aggregate understanding of threats, vulnerabilities, resources affected, and impact
- Detailed risk response information (e.g., responses implemented, status and results of previous responses, additional responses planned)

The enterprise risk register provides input for those performing enterprise risk oversight, such as an executive risk committee. The register acts as an informative gauge that can be used to stay aware of various risks, including those related to cybersecurity. By tracking the status of each risk, including their exposure values, enterprise stakeholders can identify the most relevant risks (e.g., a top 10 list that may be used to further inform enterprise risk decisions). Summary reports about the highest priority risks may be used to inform stakeholders (e.g., for federal departments and agencies, those in an oversight role, such as Congress, OMB, or GAO) about existing risks, risk responses, and planned activities.

Since it is difficult to compare dissimilar risk exposures (e.g., employee retention, disaster recovery), risks are often translated into financial impact and may be further broken down into direct costs (i.e., the impact of a given risk on the capital budget and operating expenses), the financial cost of reputational damage, and the direct financial implications of impact on the enterprise mission. Careful planning as to how dissimilar risks will be evaluated is recommended to streamline the roll-up processes. The relative financial impact of each type of risk can provide further input into risk management prioritization and monitoring decisions for enterprise risk managers. Reputation exposure can be similarly determined in the enterprise risk register (e.g., by the CRO) by combining high-impact attacks, the enterprise sector, and consequences with a histogram (trend) analysis of stakeholder sentiment for each stakeholder type. This last action of prioritization creates the enterprise risk profile, as discussed in Sec. 4.

4. Cybersecurity Risk Management as Part of a Portfolio View

The objective of ERM deliberations and related decisions is to provide timely 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. Likewise, federal ERM best practices and guidelines are similar to those of commercial practices.

Federal agencies regularly report the risk status and progress of agency information security programs, such as through management reports to DHS, OMB, and Congress. Similarly, U.S. publicly traded companies typically disclose information security to the SEC in Section 1.A. Risk Factors of Form 10-Q/K filings. At this level of reporting, information security would be considered an enterprise risk statement. Information security can be dissected into intermediate risk statements, such as Electronic information security and physical information security. Each of these intermediate risk statements can be further broken down into individual risk register statements as detail is required.

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. ERM officials then prioritize the risks on the enterprise risk register in the context of achieving the enterprise objectives (i.e., strategic, operations, reporting, and compliance) to develop an enterprise risk profile (described in Sec. 4.1). NIST often references a strategic view at the enterprise level, supported by business units that implement that strategy and are in turn supported by information and systems that enable the tactical implementation of enterprise objectives. That view is illustrated by the Information and Decision Flows diagram from the CSF [7] shown in Fig. 9.[37]

[37] Adopting and using cybersecurity risk registers is the quickest way for an enterprise to progress from Cybersecurity Framework Tier 1: Partial to Tier 4: Adaptive.

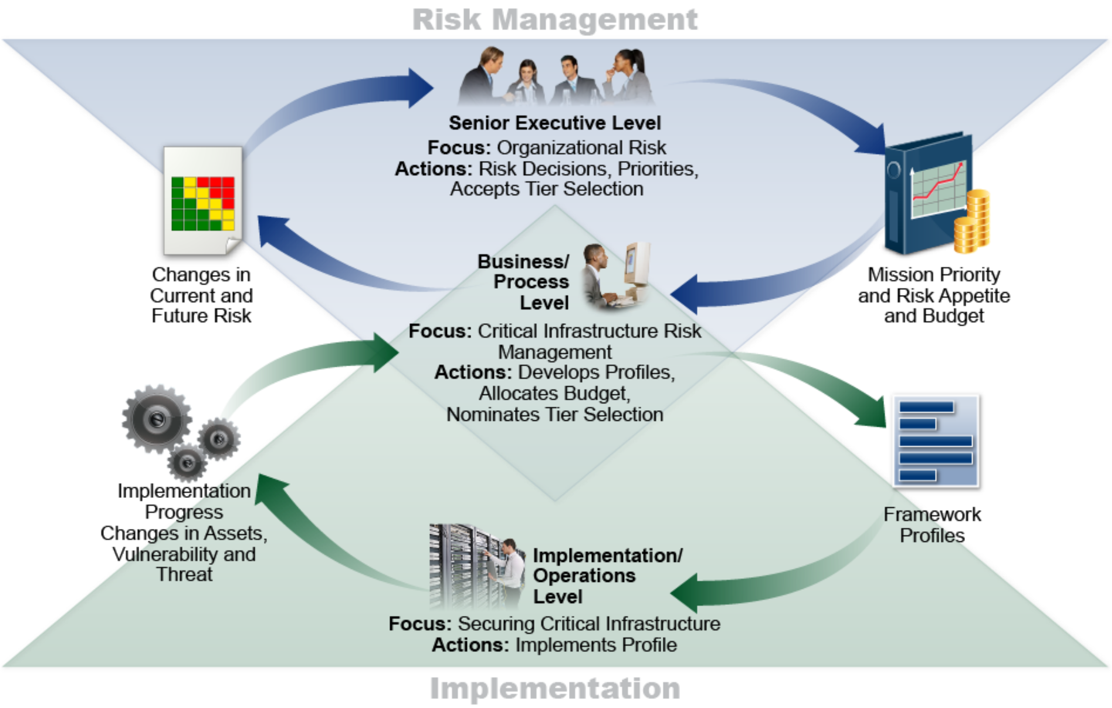

Risk Management
Senior Executive Level
Focus: Organizational Risk
Actions: Risk Decisions, Priorities, Accepts Tier Selection
Changes in Current and Future Risk
Mission Priority and Risk Appetite and Budget
Business/ Process Level
Focus: Critical Infrastructure Risk Management
Actions: Develops Profiles, 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

Fig. 9. Notional information and decision flows diagram from the CSF

Cybersecurity risk inputs are not intended to address all of the risks that may affect enterprise objectives. However, considering cybersecurity risks with regard to the enterprise's objectives supports decisions by enterprise leadership. Normalizing and aggregating the risk register supports a holistic understanding of risk response and provides a way to inform enterprise risk managers about the portfolio view of various risks throughout the enterprise.

4.1. Applying the Enterprise Risk Register and Developing the Enterprise Risk Profile

As risk information is transmitted up from lower levels of the organization, each level's risk register contains pertinent information to create a prioritized risk profile for the level immediately above it. Subordinate organizations' impacts may be different, similar, conflicting, overlapping, or unavailable and must be properly combined by financial and mission analysis at the level immediately above the reporting organization. While the impacts of cybersecurity risk on various assets may be determined at lower levels, the overall cash flow and capital implications of all of the risks can only be normalized, aggregated, and recorded in the enterprise risk register by enterprise fiduciaries (e.g., CFOs). Similarly, enterprise mission impacts must be aggregated and expressed by the senior executives who are most directly accountable to stakeholders.

The enterprise risk register informs the enterprise risk profile once the risks are prioritized at the highest level of the risk management function in the enterprise, as depicted in Table 7.

Table 7. Illustrative example of a risk profile (derived from [3])

	STRATEGIC OBJECTIVE – Improve Program Outcomes	**OPERATIONS OBJECTIVE – Manage the Risk of Fraud in Federal Operations**	**REPORTING OBJECTIVE – Provide Reliable External Financial Reporting**	**COMPLIANCE OBJECTIVE – Comply With the Improper Payments Legislation**
Risk	Agency X may fail to achieve program targets due to a lack of capacity at program partners	Contract and grant fraud	Agency X identified material weaknesses in internal control	Program X is highly susceptible to significant improper payments
Current Impact	High	High	High	High
Current Likeli-hood	High	Medium	High	High
Current Risk Response	REDUCTION: Agency X has developed a program to provide program partners with technical assistance	REDUCTION: Agency X has developed procedures to ensure that contract performance is monitored and that proper checks and balances are in place	REDUCTION: Agency X has developed corrective actions to provide program partners with technical assistance	REDUCTION: Agency X has developed corrective actions to ensure that improper payment rates are monitored and reduced
Residual Impact	High	High	High	High
Residual Likeli-hood	Medium	Medium	Medium	Medium
Proposed Risk Response	Agency X will monitor the capacity of program partners through quarterly reporting from partners	Agency X will provide training on fraud awareness, identification, prevention, and reporting	Agency X will monitor corrective actions in consultation with OMB to maintain audit opinion	Agency X will develop budget proposals to strengthen program integrity
Owner	Primary – Program Office	Primary – Contracting or Grants Officer	Primary – Chief Financial Officer	Primary – Program Office
Proposed Risk Response Category	Primary – Strategic Review	Primary – Internal Control Assessment	Primary – Internal Control Assessment	Primary – Internal Control Assessment and Strategic Review

The enterprise risk profile is a subset of carefully selected risks from the larger enterprise risk register.[38] It reflects assessments of mission, financial, and reputation exposures that are organized according to the four enterprise objectives. They may be full-value exposures or modified (and so noted) by the likelihood assessments of enterprise leaders. At the top enterprise level, ERM officials have the prerogative to add their own judgment of likelihood and impact as part of the normalization process, along with other members of the enterprise risk

[38] For the purposes of this example, "REDUCTION" is interpreted as the IR 8286 "mitigate" risk response type.

executive function. While the ERM process helps drive the 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 likelihood and impact estimations and reserves based on the changing risk landscape. Enterprise risk profiles should also reflect comparable occurrence incidents and trends for the subject enterprise and peer organizations.

The enterprise risk profile supports the governance and management of risk in several ways:

- **Financial impact** — Various risk scenarios are converted into actual capital and operational expenses, enabling executive leaders to conduct a fiscally responsible cost-benefit analysis that considers the recommended strategies for risk response. These presentations are equivalent to the financial disclosures in Form 10-Q and Form 10-K filings to the U.S. SEC by commercial public companies each quarter and for Form 8-K filings as risk incidents occur.
- **Reputation impact** — While subordinate risk registers describe risk scenarios, including those that may impact reputation, executive leaders record the evaluation of consequences on the *enterprise's* reputation. This also supports the consideration of other downstream impacts that are likely to result from damage to reputation, such as financial losses or credit risk.
- **Mission impact** — Executive leaders record the evaluation of consequences on the overall ability for the enterprise to conduct its mission and achieve strategic objectives (e.g., share value/market cap and share volatility tables for commercial public).

These high-level impact considerations are then used in conjunction with other enterprise risk responses to determine tolerances, allocations, and disclosures that are commensurate with risk exposure.

4.2. Translating the Risk Profile to Inform Leadership Decisions

The qualitative data presented in Fig. 8 must be distilled into actionable information for senior leadership decision-making (e.g., during industry boardroom deliberations and its federal analog). Table 8 provides a notional enterprise risk profile supplement that reflects a portfolio evaluation of various organizational risk profiles.

Table 8. Notional enterprise risk portfolio view for a private corporation

Financial Risk Profile						
	Current Period			**Previous Period**		
	Net Revenue	Capital	Free Cash Flow	Net Revenue	Capital	Free Cash Flow
Enterprise						
Dept A						
Dept B						
…						

Dept N						
Reputation Risk Profile						
	Current Period			**Previous Period**		
	Public	Regulators	Partners	Public	Regulators	Partners
Enterprise						
Dept A						
Dept B						
…						
Dept N						
Mission Risk Profile						
	Current Period			**Previous Period**		
Enterprise						
Dept A						
Dept B						
…						
Dept N						

4.3. Information and Decision Flows in Support of ERM

As stated in Sec. 2.1, enterprise senior leaders provide risk strategy and guidance to the organizations within their purview, including advice regarding mission priority, risk appetite and tolerance guidance, and capital and operating expenses to manage known risks. 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. Prioritized risk profile information is developed at each level, normalized, and summarized for enterprise consideration. Risk registers that reflect successes, challenges, opportunities, and increased risks enable enterprise-level managers to 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. Individual cybersecurity risks are managed and tracked within each organization and will likely be handled differently in each. Each organization's 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. They might then help those at lower levels of the enterprise to maintain the current course of action, or they may suggest different or additional steps to reduce risk. In some cases, enterprise leaders might determine that the overall risk is significantly less than the enterprise risk appetite and decide to motivate organizational risk officers to accept greater risk in targeted areas in order to enhance that organization's value.

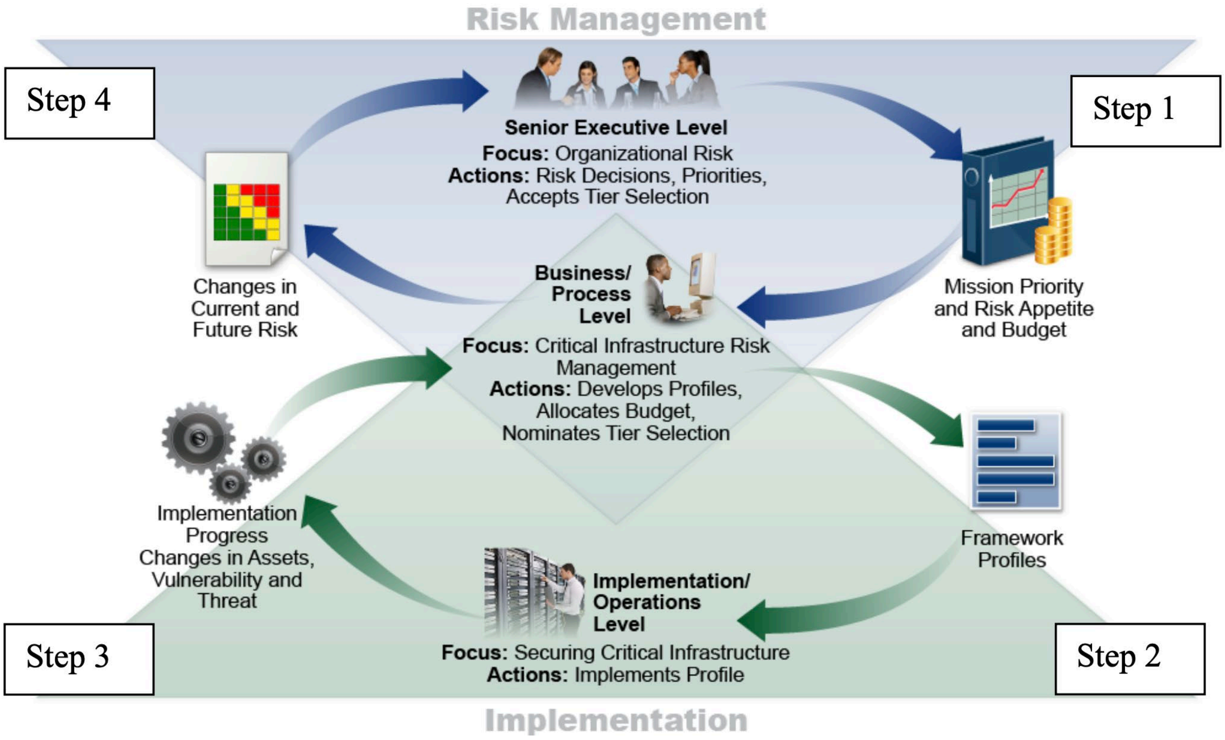

Risk Management
Step 4
Step 1
Senior Executive Level
Focus: Organizational Risk
Actions: Risk Decisions, Priorities, Accepts Tier Selection
Changes in Current and Future Risk
Mission Priority and Risk Appetite and Budget
Business/ Process Level
Focus: Critical Infrastructure Risk Management
Actions: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

Fig. 10. Notional information and decision flows diagram with numbered steps

The following process considers the information and decision flows depicted in Fig. 10.

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

  The result is mission and financial guidance for 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 in expenses).

- In **Step 2, Cybersecurity Activity 1**, organizational managers receive this guidance and perform a similar analysis for any subordinate organizations. They may utilize the CSF [7] to frame, assess, manage, respond to, and report on 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 CSRM outcomes. Implementation and operation staff then apply those principles to their systems through the NIST Risk Management Framework (RMF) or other mechanisms [16].

- In **Step 3, Cybersecurity Activity 2**, as risk is managed at the system level in accordance with organizational direction, risk acceptance, and monitoring, results are provided to organizational stakeholders. The risk determinations, decisions, and status are reported through the organizational risk register and adjusted as necessary (see Sec. 3.6).
- In **Step 4, Translating Cybersecurity to ERM**, high-level executives without fiduciary reporting requirements (organization) and corporate officers with fiduciary reporting requirements (enterprise) act upon risk registers, aggregate the information, normalize results, analyze the results, prioritize the results for executive leadership, optimize the results for risk appetite, and inform decisions. The risk categories facilitate normalization and reporting. Through this process of aggregating, normalizing, analyzing, and prioritizing risk register information, the enterprise risk officers and risk committees can:
    - Understanding actual and potential risks from threats and system failures
    - Normalize risk management across the enterprise (e.g., 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)
    - Provide enterprise executives with information to measure and understand potential exposure
    - Inform operational risk mitigation activities and relate them to enterprise mission and budgetary guidance to prioritize and optimize 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, including the exposure determination process and result, recent trends of enterprise improvement, peer trends, and contingency strategies to inform periodic and incident-driven disclosures

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

This cycle allows cybersecurity risks to be discussed in terms that are relevant for each target audience. Detailed operational discussions may occur in Steps 2 and 3, and more abstracted information may be used for executives and the Board in Steps 1 and 4.

While the steps above describe the 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. OMB Circular A-123 states that "agencies must complete their initial risk profiles in coordination with the agency Strategic Reviews," and "no less than annually, all agencies must prepare a complete risk profile and include required risk components and elements required by this guidance" [3].

The steps discussed above generate risk reports. Regarding federal agencies, IR 8170 [4] states:

> 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 the 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. Conclusion

Cybersecurity events can have consequences that significantly impact an enterprise's finances, reputation, and mission. From a financial perspective, the compromise of the integrity of financial statements (e.g., income statement, balance sheet, cash flow), assurance statements,[39] and risk narratives in quarterly reports can cause an enterprise to deliver inaccurate information to shareholders. In a modern digital economy, reputation and attention-driven business become inextricably linked to mission impact. Cybersecurity risks can also impact enterprise objectives that are established or influenced by different stakeholders (e.g., Congress, regulators, taxpayers, shareholders, clients, public, partners). Recognizing 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 are collected, analyzed, and aligned with enterprise strategic objectives. This collective understanding helps enterprise leaders stay aware of and assess substantial cybersecurity risk changes, review risk and

[39] Risk assessments directly inform annual assurance statements regarding the effectiveness of management controls (including system controls) in both the public and private sector 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 [3].

performance results, and continually pursue improvement within the broader ERM to help the organization achieve its stated mission.

References

[1] 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://bidenwhitehouse.archives.gov/wp-content/uploads/2018/06/a11.pdf

[2] 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

[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://bidenwhitehouse.archives.gov/wp-content/uploads/legacy_drupal_files/omb/memoranda/2016/m-16-17.pdf

[4] Barrett M, Marron J, Pillitteri VY, 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 Report (IR) NIST IR 8170. Includes updates as of August 17, 2021. https://doi.org/10.6028/NIST.IR.8170-upd

[5] Joint Task Force (2020) Security and Privacy Controls for Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-53r5. Includes updates as of December 10, 2020. https://doi.org/10.6028/NIST.SP.800-53r5

[6] Office of Management and Budget (2016) OMB Circular No. A-130, Managing Information as a Strategic Resource. (The White House, Washington, DC), OMB Circular No. A-130, July 28, 2016. Available at https://bidenwhitehouse.archives.gov/wp-content/uploads/legacy_drupal_files/omb/circulars/A130/a130revised.pdf

[7] National Institute of Standards and Technology (2024) The NIST Cybersecurity Framework (CSF) 2.0. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Cybersecurity White Paper (CSWP) NIST CSWP 29. https://doi.org/10.6028/NIST.CSWP.29

[8] Quinn S, Ivy N, Chua J, Scarfone K, Barrett M, Feldman L, Topper D, Witte G, Gardner RK (2023) Information and Communications Technology (ICT) Risk Outcomes: Integrating ICT Risk Management Programs with the Enterprise Risk Portfolio. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-221A. https://doi.org/10.6028/NIST.SP.800-221A

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

[10] 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/_files/ugd/3059fc_61ea5985b03c4293960642fdce408eaa.pdf

[11] 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) NIST SP 800-39. https://doi.org/10.6028/NIST.SP.800-39

[12] Quinn SD, Ivy N, Barrett M, Feldman L, Witte GA, Gardner RK (2025) Identifying and Estimating Cybersecurity Risk for Enterprise Risk Management. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency Report (IR) NIST IR 8286Ar1 ipd. https://doi.org/10.6028/NIST.IR.8286Ar1.ipd

[13] Quinn SD, Ivy N, Chua J, Barrett M, Feldman L, Topper D, Witte GA, Gardner RK (2025) Using Business Impact Analysis to Inform Risk Prioritization and Response. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency Report (IR) NIST IR 8286D-upd1. https://doi.org/10.6028/NIST.IR.8286D-upd1

[14] Committee of Sponsoring Organizations (COSO) of the Treadway Commission (2013) Internal Control—Integrated Framework, Executive Summary. Available at https://www.coso.org/_files/ugd/3059fc_1df7d5dd38074006bce8fdf621a942cf.pdf

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

[16] 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) NIST SP 800-37r2. https://doi.org/10.6028/NIST.SP.800-37r2

[17] Association for Federal Enterprise Risk Management (2021) Federal ERM Areas of Practice Guidance — 2021. Available at https://www.aferm.org/wp-content/uploads/2022/02/AFERM-Federal-ERM-Areas-of-Practice-Guidance.pdf

[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. Available at https://resources.sei.cmu.edu/asset_files/TechnicalReport/2007_005_001_14885.pdf

[19] The MITRE Corporation (2025) ATT&CK. Available at https://attack.mitre.org

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

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

[22] The Open Group (2025) Open FAIR Body of Knowledge, Version 2.0. Available at https://publications.opengroup.org/t230

[23] Quinn SD, Ivy N, Barrett M, Witte GA, Gardner RK (2025) Prioritizing Cybersecurity Risk for Enterprise Risk Management. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency Report (IR) NIST IR 8286B-upd1. https://doi.org/10.6028/NIST.IR.8286B-upd1

[24] Joint Task Force (2022) Assessing Security and Privacy Controls in Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-53Ar5. https://doi.org/10.6028/NIST.SP.800-53Ar5

[25] Quinn SD, Ivy N, Barrett M, Gardner RK, Smith MC, Witte GA (2025) Staging Cybersecurity Risks for Enterprise Risk Management and Governance Oversight. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency Report (IR) NIST IR 8286Cr1 ipd. https://doi.org/10.6028/NIST.IR.8286Cr1.ipd

[26] Dempsey KL, Chawla NS, Johnson LA, Johnston R, Jones AC, Orebaugh AD, Scholl MA, Stine KM (2011) Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-137. https://doi.org/10.6028/NIST.SP.800-137

[27] 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) NIST SP 800-60v1r1. https://doi.org/10.6028/NIST.SP.800-60v1r1

[28] Nelson A, Rekhi S, Souppaya M, Scarfone K (2024) Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile for more information. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-61r3 ipd. https://doi.org/10.6028/NIST.SP.800-61r3.ipd

Appendix A. List of Symbols, Abbreviations, and Acronyms

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

AFR
Agency Financial Report

AIS
Automated Indicator Sharing

BIA
Business Impact Analysis

BYOD
Bring-Your-Own-Device

CapEx
Capital Expenditures

CBA
Cost-Benefit Analysis

CDM
Continuous Diagnostics and Mitigation

CFO
Chief Financial Officer

CIO
Chief Information Officer

CISO
Chief Information Security Officer

COOP
Continuity of Operations

COSO
Committee of Sponsoring Organizations

CPO
Chief Privacy Officer

CRO
Chief Risk Officer

CSAM
Cyber Security Assessment and Management

CSF
Cybersecurity Framework

C-SCRM
Cyber Supply Chain Risk Management

CSRM
Cybersecurity Risk Management

CSRR
Cybersecurity Risk Register

DHS
Department of Homeland Security

DoD
Department of Defense

eMASS
Enterprise Mission Assurance Support Service

ERM
Enterprise Risk Management

ERP
Enterprise Risk Profile

ERR
Enterprise Risk Register

ERSC
Enterprise Risk Steering Committee

GAO
U.S. Government Accountability Office

GRC
Governance, Risk, Compliance

HVA
High Value Asset

ICT
Information and Communications Technology

ICTRM
Information and Communications Technology Risk Management

IEC
International Electrotechnical Commission

IG
Inspector General

IoT
Internet of Things

IR
Internal or Interagency Report

ISAC
Information Sharing and Analysis Center

ISAO
Information Sharing and Analysis Organization

ISCM
Information Security Continuous Monitoring

ISO
International Organization for Standardization

KPI
Key Performance Indicator

KRI
Key Risk Indicator

NCCoE
National Cybersecurity Center of Excellence

NFC
National Finance Center

NOAA
National Oceanic and Atmospheric Administration

OCTAVE
Operationally Critical Threat, Asset, and Vulnerability Evaluation

OLIR
National Online Informative References Program

OMB
Office of Management and Budget

OpEx
Operating Expenses

OT
Operational Technology

POA&M
Plan of Actions and Milestones

RAR
Risk Assessment Report

RMC
Risk Management Council or Committee

RMF
Risk Management Framework

SAORM
Senior Accountable Official for Risk Management

SEC
U.S. Securities and Exchange Commission

SEI
Software Engineering Institute

SP
Special Publication

SWOT
Strengths, Weaknesses, Opportunities, Threats

US-CERT
United States Computer Emergency Readiness Team

Appendix B. Glossary

actual residual risk
The risk remaining after management has taken action to alter its severity. [10]

aggregation
The consolidation of similar or related information.

assets
The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes. [7]

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

cybersecurity risk
The effect of uncertainty on or within information and technology. 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. [9][27]

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
The effect of uncertainty on the enterprise's mission and objectives.

enterprise risk management
An effective agency-wide approach to addressing the full spectrum of the organization's significant risks by understanding the combined impact of risks as an interrelated portfolio rather than addressing risks only within silos. [1]

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. [10]

enterprise risk register
A risk register at the enterprise level that contains normalized and aggregated inputs from subordinate organizations' risk registers and profiles.

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

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

inherent risk
The risk to an entity in the absence of any direct or focused actions by management to alter its severity. [10]

internal control
An overarching mechanism that an enterprise uses to achieve and monitor enterprise objectives.

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 a larger organizational structure (e.g., a federal agency or a company). [5]

plan of actions and milestones
A document for a system that "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." [16]

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 in which numerical values are assigned to both impact and likelihood based on statistical probabilities and the monetarized valuation of loss or gain.

residual risk
The risk that remains after risk responses have been documented and performed.

risk
The effect of uncertainty on objectives. [1]

risk appetite
The types and amount of risk, on a broad level, [an organization] is willing to accept in its pursuit of value. [10]

The broad-based amount an enterprise is willing to accept in pursuit of its mission/vision. [3]

risk detail report
A report of detailed risk scenario information that supports the contents of a risk register entry, including risk history information, risk analysis data, and information about individual and organizational accountability.

risk profile
A prioritized inventory of the most significant risks identified and assessed through the risk assessment process versus a complete inventory of risks. [3]

risk register
A repository of risk information, including the data understood about risks over time. [1]

risk reserve
A type of management reserve in which funding or labor hours are set aside and employed if a risk is triggered to ensure that the opportunity is realized or that the 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 realized, shared, enhanced, or accepted.

risk tolerance
The organization's or stakeholder's readiness to bear the remaining risk after risk response in order to achieve its objectives, with the consideration that such tolerance can be influenced by legal or regulatory requirements. [9]

security control
The safeguards or countermeasures that are prescribed for an information system or organization to protect the confidentiality, integrity, and availability of the system and its information.

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

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

target residual risk
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. [10]

threat
Any circumstance or event with the potential to adversely impact organizational operations (a negative risk).

threat actor
A risk instigator with the capability to do harm.

threat source
A malicious person with harmful intent or an unintended or unavoidable situation (e.g., natural disaster, technical failure, human error) that may trigger a vulnerability.

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 in *Playbook: Enterprise Risk Management for the U.S. Federal Government* [2]. These sources are intended to supplement risk management programs and do not by themselves constitute the foundation of a risk management program.

- Agency reports and self-assessments
    - Previous year Federal Managers and Financial Integrity Act (FMFIA) reports and OMB Circular A-123, Appendix A [3] self-assessments and related assurance statements
        - Entity-level control interviews and evidence documentation
        - Assessments of agency processes and thousands of documented controls
        - Documented control deficiencies, including their level of significance (i.e., simple, significant, or material weakness)
        - 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 Reviews, quarterly performance reviews, Risk Management Council (RMC), etc.
- Inspector General (IG) and Government Accountability Office (GAO)
    - IG Management Challenges documented annually in the agency's Annual Financial Report (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

Appendix D. Notional Enterprise Risk Register

Table 9 provides a notional enterprise risk register that combines both federal agency and critical infrastructure risks to illustrate the integration of various cybersecurity risks with key enterprise risks. This table directly supports the discussion in Sec. 3.9 of this report.

Table 9. Notional enterprise risk register

ID	Priority	Risk Description	Risk Category	Current Financial Impact	Current Reputation Impact	Current Mission Impact	Current Likelihood	Current Exposure Rating	Risk Response	Risk Owner	Status
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	Dwayne Rhodes (Human Resources Department)	Open
2	6	A strategic opportunity to hire a globally recognized technologist leads to establishing a new satellite communications initiative[40]	Operational Risk	OpEx M CapEx L	H	M	M	M	• Allocate funds for compensation package • Initiate strategic recruiting plan	Dwayne Rhodes (Human Resources Department)	Open
3	1	A social engineering attack on the enterprise workforce leads to a breach or loss	Operational 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 the IT Risk Council	Carly Franklin (CISO)	Open

[40] This is an example response to an opportunity (positive risk).

ID	Priority	Risk Description	Risk Category	Current Financial Impact	Current Reputation Impact	Current Mission Impact	Current Likelihood	Current Exposure Rating	Risk Response	Risk Owner	Status
4	3	A security event at a third-party partner results in data loss or system outage	Operational Risk	OpEx L CapEx L	H	H	M	M	• Chief Financial Officer and Chief Executive Officer agree on plans for potential secondary financial impacts 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 department • Implement 3rd Party Partner Assessment for Tier 1 providers per CIO and CISO recommendations	Ernest Woods (Procurement)	Open
5	7	A sales reduction due to tariffs leads to reduced revenue	Financial Risk	OpEx M CapEx L	L	L	L	L	• Increase marketing in target areas • Ensure competitive pricing in target markets	Elaine Kim (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	Elaine Kim (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 and Development (IRAD) funding by 10 % to spur and expand internal innovation • Update technical training to include design thinking methodologies	Sharika Grigsby (VP, Product Development)	Open

ID	Priority	Risk Description	Risk Category	Current Financial Impact	Current Reputation Impact	Current Mission Impact	Current Likelihood	Current Exposure Rating	Risk Response	Risk Owner	Status
									• Implement customer surveys in target areas to ensure adequate product coverage		
8	2	Company intellectual property data is disclosed through employee error or a malicious act	Operational Risk	OpEx M CapEx M	H	H	M	M	• Review and improve employee background screening controls • Update corporate security training to reinforce the need for diligence • Implement data loss prevention tools per CISO recommendation	Carly Franklin (CISO)	Closed
9	10	A flaw in product quality leads to reputational damage and reduced sales	Strategic Risk	OpEx M CapEx M	H	H	L	L	• Update the continuous improvement process • Implement the Baldrige Excellence Framework • Update external provider quality standards	Sharika Grigsby (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 and maintain a centralized register of compliance requirements • Update employee training based on an updated understanding of corporate requirements • Review BIA templates to ensure that information and technology requirements include regulatory and contractual obligation criteria	Mark Braxton (Legal Dept.)	Open

Appendix E. Change Log

In February 2025, the following changes were made to this report:

- All — Made minor editorial changes throughout the report to implement the current NIST IR template.
- All — Updated all Cybersecurity Framework (CSF) references and excerpts throughout the report from version 1.1 to version 2.0.
- Executive Summary and Sec. 1.1 — Added content on how SP 800-221A relates to the IR 8286 series.
- Section 2.1.2 — Removed Table 1 (similarities among selected ERM and risk management documents) and its corresponding text.
- Section 2 — Removed the original Sec. 2.2 (“Shortcomings of Typical Approaches to Cybersecurity Risk Management”). Moved content of the original Sec. 2.3.1 (“Insufficient Asset Information”) to Sec. 3.2.1 (“Inventory and Valuation of Assets”).
- Section 2.2 — Added a paragraph on complex systems of systems that is partially based on the original Sec. 2.2.4 (“Increasing System and Ecosystem Complexity”). Added a recommendation to perform a BIA and a pointer to IR 8286D for more information. Expanded the list of risk management activities during which cybersecurity risk registers should be used.
- Section 3.1.2 — Made significant content revisions throughout (“Risk Management Strategy”).
- Section 3.2 — Added content on using the BIA register and a pointer to IR 8286D for more information.
- Section 3.2.1 — Made significant content revisions throughout (“Inventory and Valuation of Assets”).
- Section 3.3.2 — Added a pointer to IR 8286A for additional information on estimating the likelihood and impact of consequences.
- Section 3.4 — Added a pointer to IR 8286B for additional information on techniques for prioritizing risks.
- Section 3.5 — Added a pointer to IR 8286B for additional information on risk response strategies.
- Section 3.6 — Added a pointer to IR 8286C for additional information on risk monitoring, evaluation, and adjustment.
- Section 3.6.2 — Expanded content to include key performance indicators and point to IR 8286C for more information.

- Section 3.8 — Added pointers to IR 8286C for additional information on cybersecurity risk register aggregation, normalization, analysis, and prioritization and on integrating cybersecurity risk into the ERR/ERP. Added content on information and communications technology risk management (ICTRM) and a pointer to SP 800-221A for more information. Added a list of actions for designated risk officers and senior management to perform on risk registers.
- Section 3.9 — Moved the large table with the notional enterprise risk register to a new Appendix D. Added a new small table with an excerpt from the large table.
- Section 4.1 — Transposed and adjusted the content of the table with the illustrative example of a risk profile to improve its readability and accessibility.
- Section 4.4 — Updated the conclusion.
- References — Updated references to reflect current versions and URLs. Renumbered references to indicate their current order within the document.