NIST Interagency Report
NIST IR 8286Cr1

Staging Cybersecurity Risks for Enterprise Risk Management and Governance Oversight

Stephen Quinn
Nahla Ivy
Matthew Barrett
R. K. Gardner
Matthew C. Smith
Greg Witte

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8286Cr1

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

NIST Interagency Report
NIST IR 8286Cr1

Staging Cybersecurity Risks for Enterprise Risk Management and Governance Oversight

Stephen Quinn
Computer Security Division
Information Technology Laboratory

Nahla Ivy
Enterprise Risk Management Office
Office of Financial Resource Management

Matthew Barrett
CyberESI Group, Inc.

R.K. Gardner
New World Technology Partners

Matthew C. Smith
Seemless Transition LLC

Greg Witte
Palydin LLC

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8286Cr1

December 2025

U.S. Department of Commerce
Howard Lutnick, Secretary

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.

Publication History
Approved by the NIST Editorial Review Board on 2025-11-26
Supersedes NIST IR 8286C-upd1 (September 2022, updated March 6, 2024)
https://doi.org/10.6028/NIST.IR.8286C-upd1

How to Cite this NIST Technical Series Publication:
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. https://doi.org/10.6028/NIST.IR.8286Cr1

Author ORCID iDs
Stephen D. Quinn: 0000-0003-1436-684X
Nahla Ivy: 0000-0003-4741-422X
Matthew Barrett: 0000-0002-7689-427X
Matthew C. Smith: 0000-0003-1004-7171
Gregory A. Witte: 0000-0002-5425-1097

Contact Information
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/c/r1/final, including related content, potential updates, and document history.

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

Abstract

This document is the third in a series that supplements NIST Interagency Report (IR) 8286, Integrating Cybersecurity and Enterprise Risk Management (ERM). This series provides additional details regarding enterprise application of cybersecurity risk information; the previous documents, IRs 8286A and 8286B, provide details regarding stakeholder risk direction and methods for assessing and managing cybersecurity risk in light of enterprise objectives. This report, IR 8286C, describes how information recorded in cybersecurity risk registers may be integrated as part of a holistic approach to ensuring that risks to information and technology are properly considered for the enterprise risk portfolio. This cohesive understanding supports an enterprise risk register and enterprise risk profile that, in turn, support the achievement of enterprise objectives.

Keywords

cyber risk management; cybersecurity risk management (CSRM); cybersecurity risk measurement; cybersecurity risk register (CSRR); enterprise risk management (ERM); enterprise risk profile (ERP); enterprise risk register (ERR); key performance indicator (KPI); key risk indicator (KRI); risk prioritization.

Reports on Computer Systems Technology

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

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 Readers

This document references government-mandated federal agency enterprise and cybersecurity risk requirements to demonstrate alignment with existing federal uses. Such references are included to provide guidance and to help bridge private and public ERM processes. However, these references must not be interpreted as mandates.

Concurrently, the following documents provide the high-level outcome statements to implement for the content contained within the IR 8286 series:

- The NIST Cybersecurity Framework (CSF) 2.0 [3]
- NIST Special Publication (SP) 800-221, *Enterprise Impact of Information and Communications Technology Risk: Governing and Managing ICT Risk Programs Within an Enterprise Risk Portfolio* [4]
- SP 800-221A, *Information and Communications Technology (ICT) Risk Outcomes: Integrating ICT Risk Management Programs with the Enterprise Risk Portfolio* [5]

Patent Disclosure Notice

NOTICE: ITL has requested that holders of patent claims whose use may be required for compliance with the guidance or requirements of this publication disclose such patent claims to ITL. However, holders of patents are not obligated to respond to ITL calls for patents and ITL has not undertaken a patent search in order to identify which, if any, patents may apply to this publication.

As of the date of publication and following call(s) for the identification of patent claims whose use may be required for compliance with the guidance or requirements of this publication, no such patent claims have been identified to ITL.

No representation is made or implied by ITL that licenses are not required to avoid patent infringement in the use of this publication.

Table of Contents

List of Tables

List of Figures

Acknowledgments

The authors thank everyone who has contributed to Revision 1 of this publication and provided feedback on its content, including the following: Daniel Eliot of NIST; Yasin Carkci (CTO/Cybersecurity Architect, Finance); Thomas Scott Crumbaugh (Emergency Preparedness & Response Operations (EPRO), Department of Health and Human Services (HHS)); Dr. Robert Mark (Managing Director, Black Diamond); Andrew Shea (President, CRFQ); Xiang Zheng Teo (Vice President of Advisory, Ensign InfoSecurity); The FAIR Institute - Standards Committee Members: Michael Coden (Cofounder and Associate Director, Cybersecurity at MIT Sloan); Pankaj Goyal (Director, Standards and Research, FAIR Institute); Alexander Holbrook (Principal, Boston Consulting Group (BCG)); Jack Jones (Author and Chairman Emeritus, FAIR Institute); Pierre Olodo (Senior Lead, Cyber Risk, Richemont); Mike Radigan (Senior Advisor, Cisco); Jan Reich (Data Protection & Risk Management, Novartis); Rob Moore (VP, Technology Risk Management, Mastercard); and Denny Wan (Chair, Reasonable Security Institute); FAIR Institute Management (Nick Sanna (President & Founder); Todd Tucker (Managing Director); Bernadette Dunn (Head of Education); Luke Bader (Director of Member Programs); and Other Contributing Members: (AJ Anand (Director, Transformation and Continuous Improvement, Global Security, ADP); Heather Dart (Senior Manager, Information Risk Management, Danaher Corporation); Dana Haubold (Cybersecurity Advisor, DH Cyber Security Consultancy); Glen Garmes (CISO, Old Republic International); Marko Hamel (Product Security & Risk Expert, SAP); Anthony Leatherwood (Director, Technology Risk and Cybersecurity, Plains All American); Vincent Milette (GRC Transformation Delivery Manager, Air Canada); Steve Reznik (Lead Security Analyst, TriNet); and Timothy Szerlong (Information Security Risk Management Consultant, Unum).

The authors also wish to thank all individuals, organizations, and enterprises that contributed to the creation of the original version of this document. This includes Lisa Carnahan, Amy Mahn, Matt Scholl, Isabel Van Wyk, Jim Foti, Daniel Eliot, and Kevin Stine of NIST; Larry Feldman and Daniel Topper of Huntington Ingalls Industries; Mat Heyman of Impresa Management Solutions; and Scott Crumbaugh of United States Center for Medicare & Medicaid Services. Organizations and individuals who provided feedback on the public comment drafts include Piyavauth Bhutrakarn, Julie Chua, Khairun Pannah, Charles Livingston, Rehana Mwalimu, Michael Young, and the United States Department of Health and Human Services as part of the Cyber-ERM Community of Interest; Joel Crook, Dr. Pat Goguen, Denis Maratos, Michael Whitley, and Andrew Resseguie of Consolidated Nuclear Security, LLC; Scott Bouboulis of CTIA; Jamie Ferguson and Lori Potter of Kaiser Permanente; Kelly Hood of Optic Cyber Solutions; Edward J. DeMarco, Jr. of the Risk Management Association; and Amy Hamilton of the U.S. Department of Energy.

Executive Summary

This NIST Interagency Report (IR) explores methods for integrating disparate cybersecurity risk management (CSRM) information from throughout the enterprise to create a composite enterprise risk profile to inform company executives' and agency officials' enterprise risk management (ERM) deliberations, decisions, and actions. It describes the inclusion of cybersecurity risks as part of financial, valuation, mission, operational and reputation exposure. Fig. 1 expands the enterprise risk cycle from previous reports to remind the reader that the input and sentiments of external stakeholders are a critical element of risk decisions.[1]

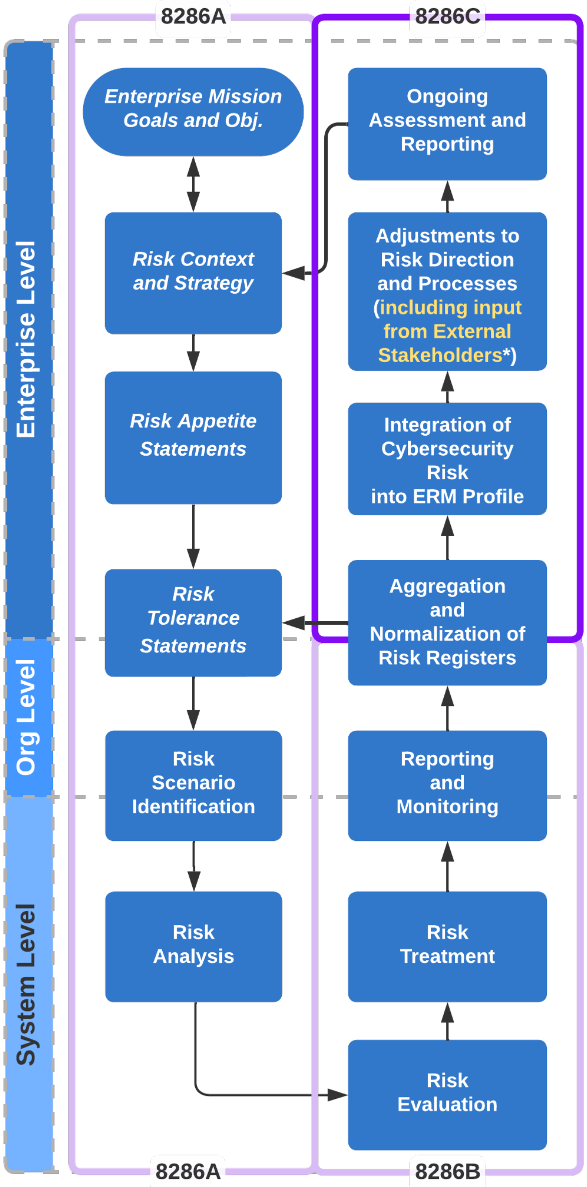

8286A
8286C
Enterprise Level
Org Level
System Level
Enterprise Mission Goals and Obj.
Risk Context and Strategy
Risk Appetite Statements
Risk Tolerance Statements
Risk Scenario Identification
Risk Analysis
Ongoing Assessment and Reporting
Adjustments to Risk Direction and Processes (including input from External Stakeholders*)
Integration of Cybersecurity Risk into ERM Profile
Aggregation and Normalization of Risk Registers
Reporting and Monitoring
Risk Treatment
Risk Evaluation
8286A
8286B

Fig. 1. IR 8286 [6] series publications describe CSRM/ERM integration

[1] Key external stakeholders include shareholders, strategic partners, regulators, constituents, allies, and legislators.

The importance of information and technology risks to the enterprise risk posture makes it critical to ensure broad visibility about risk-related activities to protect enterprise reputation, finances, and objectives. A comprehensive enterprise risk register (ERR) and enterprise risk profile (ERP) support communication and disclosure requirements. The integration of CSRM activities supports understanding of exposures related to corporate reporting (e.g., income statements, balance sheets, and cash flow) and similar requirements (e.g., reporting for appropriation and oversight authorities) for public-sector entities.

This document explores the methods for integrating disparate CSRM information from throughout the enterprise to create a composite understanding of the various cyber risks that may have an impact on the enterprise's objectives. The report continues the discussion where IR 8286B [7] concluded by focusing on the integration of data points to create a comprehensive view of opportunities and threats to the enterprise's information and technology. Notably, because cybersecurity risk is only one of dozens of risk types in the enterprise risk universe, that risk understanding will itself be integrated with similar aggregate observations of other collective risk points.

This document discusses how risk governance elements such as enterprise risk strategy, appetite, tolerance, and capacity direct risk performance. By monitoring the results of CSRM activities at each hierarchical level, senior leaders can adjust various governance components (e.g., policy, procedures, workforce skills) to achieve risk objectives. This report describes how the CSRM Monitor, Evaluate, and Adjust (MEA) process supports ERM and a repeatable and consistent use of terms, including how the context of various terms can vary depending on the enterprise's perspective. That understanding helps to ensure effective CSRM communication and coordination.

While ERM is a well-established field, there is an opportunity to expand and improve the body of knowledge regarding coordination among cybersecurity risk managers – particularly the integration of first and third party/supply chain risk management - and those managing risk at the most senior levels. This series is intended to introduce this integration while recognizing the need for additional research and collaboration. Further points of discussion include IR 8286D's focus on business impact analysis (BIA), which is a foundation of understanding exposure and opportunity [8]. NIST also continues to perform extensive research and publication development regarding metrics, a topic that will certainly support ERM/CSRM performance measurement, monitoring, and communication.

This document also describes the use of frameworks for ERM and governance oversight. Section 4 of this publication provides details regarding the NIST Cybersecurity Framework, or CSF, that is well-suited for this purpose. In particular, the GOVERN function of the NIST CSF provides a high-level framework that's consistent with this document series, enabling information gathering regarding organizational context (including risk criteria); risk strategy, policy, and roles; supply chain risk considerations; and oversight methods.

This document continues the discussion regarding the inclusion of CSRM priorities and results in support of an improved understanding about organization and enterprise impacts of cybersecurity risks on financial, reputation, operational and mission considerations.

1. Introduction

This document provides guidance that supplements NIST Interagency Report (IR) 8286, *Integrating Cybersecurity and Enterprise Risk Management (ERM)* [6]. IR 8286C is the third in a series of companion publications that provide guidance for implementing, monitoring, and maintaining an enterprise approach designed to integrate cybersecurity risk management (CSRM) into ERM.[2] Readers of this report will benefit from reviewing the foundation document, IR 8286, since many of the concepts described in this report are based on practices and definitions established in that IR. Each publication in the series, as illustrated in Fig. 2, provides detailed guidance to supplement topics from IR 8286.

Activities in dark blue boxes are described in this report and are identified below; those in other documents are shown in a lighter shade.

- IR 8286A details the context, scenario identification, and analysis of the likelihood and impacts of cybersecurity risk. It also includes methods to convey risk information, such as cybersecurity risk registers (CSRRs) and risk detail records [9].
- IR 8286B describes ways to apply risk analysis to help prioritize cybersecurity risk, evaluate and select appropriate risk responses, and communicate risk activities as part of an enterprise CSRM strategy [7].
- IR 8286C (this report) describes processes for aggregating information from CSRM activities throughout the enterprise. As that information is integrated and harmonized, organizational and enterprise leaders monitor the achievement of risk objectives, consider changes to risk strategy, and use the combined information to maintain awareness of risk factors and positive risks (opportunities).
- IR 8286D describes considerations for documenting and analyzing business impacts that result in a full or partial loss of the confidentiality, integrity, or availability of a mission-essential resource [8].

[2] For the purposes of this document, the terms “cybersecurity” and “information security” are used interchangeably.

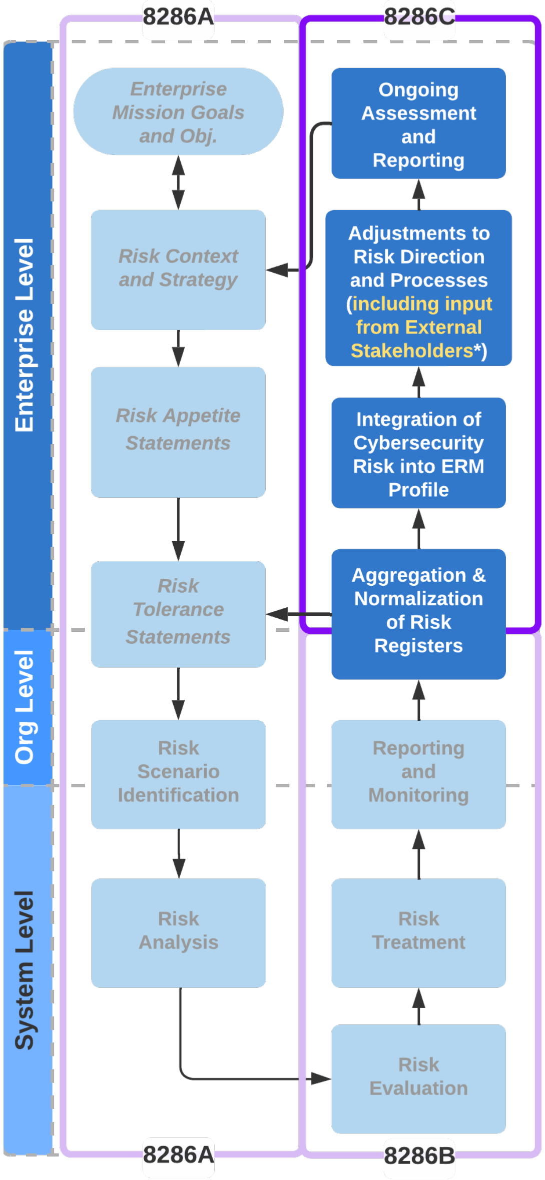

8286A
8286C
Enterprise Level
Org Level
System Level
Enterprise Mission Goals and Obj.
Risk Context and Strategy
Risk Appetite Statements
Risk Tolerance Statements
Risk Scenario Identification
Risk Analysis
Ongoing Assessment and Reporting
Adjustments to Risk Direction and Processes (including input from External Stakeholders*)
Integration of Cybersecurity Risk into ERM Profile
Aggregation & Normalization of Risk Registers
Reporting and Monitoring
Risk Treatment
Risk Evaluation
8286A
8286B

Fig. 2. IR 8286C activities as part of CSRM/ERM integration

The terms *organization* and *enterprise* are often used interchangeably. This report defines both an organization and an enterprise as an entity of any size, complexity, or positioning within a larger organization structure (e.g., a federal agency or company). It further defines the *enterprise level* as a unique type of organization, one in which individual senior leaders govern at the highest point in the hierarchy and have unique risk management responsibilities, such as fiduciary reporting and establishing risk strategy (e.g., risk appetite, methods). Notably, government and private industry CSRM and ERM programs have different oversight and reporting requirements (e.g., accountability to Congress versus accountability to shareholders), but the general needs and processes are similar.

1.1. Purpose and Scope

This document brings together elements from other documents in the series to help inform decisions by leaders throughout the enterprise. Those decisions include intentional steps to capitalize on opportunities and proactive steps to avoid harmful surprises that might derail those opportunities. Managers at all enterprise levels depend on senior leaders to define the mission and objectives for the enterprise, and those senior leaders depend on risk practitioners to take appropriate actions and report them in a consistent and timely manner. Managing cybersecurity risks (especially as part of ERM activities) can be highly beneficial. For example, in non-governmental entities, such management often has a positive impact on an enterprise's ability to obtain cybersecurity insurance coverage, possibly reducing premiums or raising the coverage threshold. Decisions and directives about risk acceptance and risk mitigation inform investment priorities and workforce allocation.

This IR series focuses heavily on the use of risk registers to record and share information within and among hierarchical levels. The goal of risk management is not simply to maintain lists of risks, but also to support effective decision-making at each of those levels. The CSRR is one of many tools to help managers and leaders continually monitor activities, evaluate available options (both to exploit opportunities and to mitigate potential harms), and adjust actions in such a way as to ensure mission success. This document describes the integration of the various CSRM activities, as described within the CSRRs, to contribute to a prioritized profile of the enterprise's risk. As with other risk elements, the maintenance of an enterprise risk profile (ERP) itself is not a goal but simply another tool for helping senior leaders and enterprise executives chart and maintain a course for achieving mission success.

In support of transforming lists of risks and actions into a prioritized ERP, this document describes four key ERM activities:

1. Aggregation, normalization, and analysis (including optimization) of CSRM data from throughout the enterprise to create a composite CSRM understanding;
2. Integration of data regarding key cyber risks that should be included in overarching enterprise-level risk artifacts, such as the enterprise risk register (ERR) and ERP;
3. Adjustments to risk direction (including risk limits and risk treatment options) within governance system components to optimize enterprise CSRM results; and
4. Monitoring and reporting at various hierarchical levels to maintain situational awareness regarding changes to the risk landscape and CSRM outcomes.

These activities are part of an ongoing cycle. As adjustments are made to the ERM direction and activities, the results are reported to keep stakeholders informed and to improve subsequent risk assessments. The cycle also helps to confirm or improve decisions regarding the value and categorization of important assets that enable mission-critical (and mission-essential) functions. This determination is important to support the business impact analysis (BIA) from a loss or degradation of such assets. Additional information about BIA and asset valuation is available in IR 8286D [8].

Because cybersecurity risk is only one of dozens of risk types affecting an enterprise, cybersecurity risk understanding is integrated with similar aggregate observations of other collective risk points. When this disparate data is collected and analyzed by those in an enterprise risk governance role, senior leaders can create or maintain a comprehensive ERR and ERP, enabling effective stakeholder communication regarding ERM effectiveness, changes to the entity's risk posture, and achievement of enterprise ERM strategy.

This publication discusses how risk governance elements such as enterprise risk strategy, appetite, tolerance, and capacity direct risk performance. By monitoring the results of CSRM activities at each hierarchical level, senior leaders can adjust various governance components (e.g., policy, procedures, skills, governance structures) to achieve risk objectives.

1.2. Document Structure

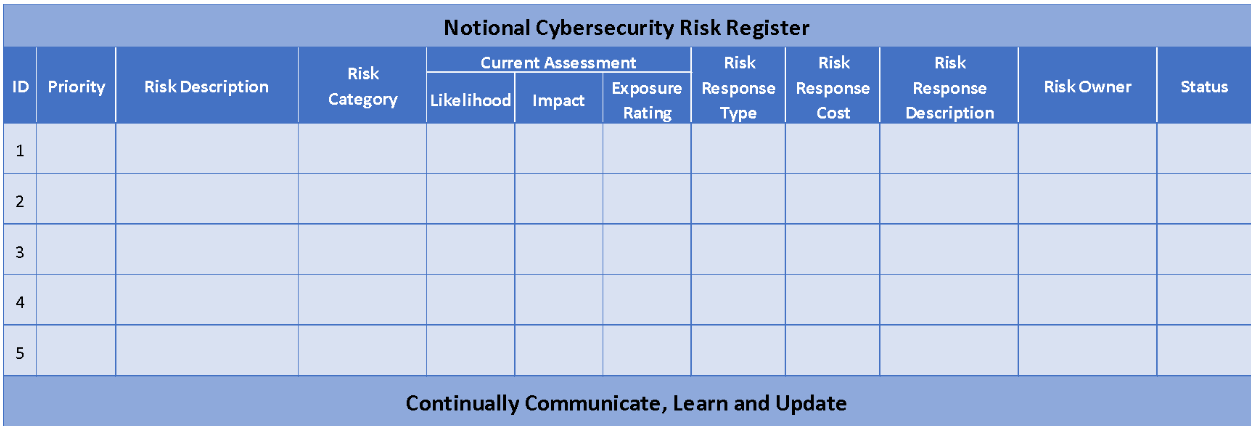
This publication provides recommendations for integrating CSRM information as documented in the CSRR and other communications artifacts, evaluating necessary adjustments based on the enterprise's risk strategy, and highlighting key risks that should be included in enterprise risk documentation. Each of the sections below provides information and recommendations for integrating CSRM data and helping to evaluate enterprise-level risks based on their potential to impact the enterprise mission and objectives.

The document is organized into the following major sections:

- Section 2 describes the aggregation of CSRM information from various sources.
- Section 3 describes methods for integrating cyber risk details into an enterprise-level cybersecurity risk register, providing awareness and reporting capabilities to inform stakeholders about key risks, and supporting updates to the ERR and ERP.
- Section 4 reviews the enterprise governance system and components for maintaining a comprehensive cybersecurity management program. It describes example methodologies that will help inform strategic adjustments and ongoing assessments.
- Section 5 describes processes for monitoring cybersecurity risk conditions, evaluating potential options for how to respond to changes, and adjusting the risk strategy or risk management activities.
- The References section provides links to external sites and publications referenced in this publication.
- Appendix A contains the acronyms and abbreviations used in this publication.
- Appendix B provides a change log for this document.

2. Aggregation, Normalization, and Analysis of Cybersecurity Risk Registers (CSRRs)

The IR 8286 series presents the value in using a consistent CSRR. The precise contents and format of the CSRR will vary by enterprise but generally follow the structure that has been illustrated throughout this series. Fig. 3 provides a notional example of a CSRR.[3]



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. 3. Notional cybersecurity risk register template

When providing CSRR input into ERRs and informing other ERM activities, there are three key phases to take to ensure the quality, efficacy, and efficiency of the data: aggregation, normalization, and analysis.

Fig. 4 depicts how a CSRR moves through each phase. An analyzed CSRR will include priority input from leadership as well as resourcing determinations for risk optimization. Analyzing CSRRs, and eventually ERRs and ERPs, is an iterative process which is informed by leadership, management, and practitioners. Risk priority assignments are present in CSRRs since they represent a bottom-up optic on criticality. However, senior leaders, based on their optic, often make changes as cybersecurity risks are considered alongside other information and communications technology (ICT) risk. Optimized budgets and resourcing will be determined by management in conjunction with enterprise leadership and system-level data.

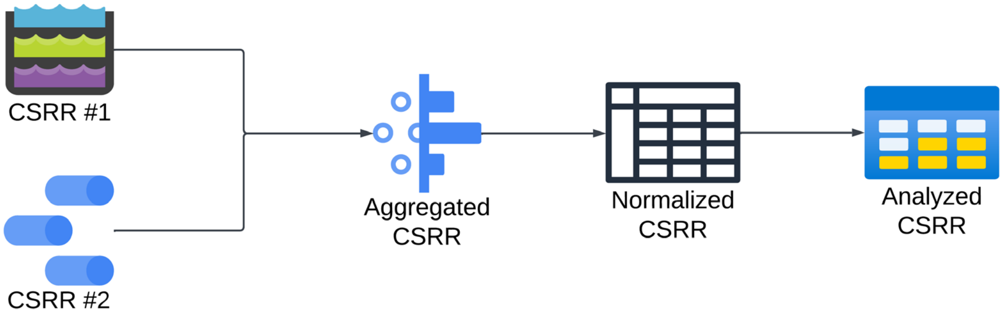


Fig. 4. Moving CSRRs through the aggregation, normalization, and analysis phases

[3] 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.

2.1. Aggregation of Cybersecurity Risk Information

The activities described in IRs 8286A and 8286B provide guidance to help complete the CSRR for a given system, using that form to record information about known risk scenarios, analysis of their impact, and actual or planned activities to respond to those risks. Section 2.5 of IR 8286B contains information about steps for conditioning information in the CSRRs to ease subsequent integration, the next activity in CSRM/ERM coordination. Some of these system-level risks, as recorded in CSRRs, represent operational risks that must be considered within operational risk management (ORM) processes (described in Sec. 3.2).

The purpose of the aggregation step is to take disparate sources of data and put them into a single source of data for a given organization level. The aggregation step can be managed through documents, spreadsheets, or other specialized tools. As an enterprise grows, the number of risk registers from the system level being aggregated through organization levels to the enterprise level increases. Therefore, the process of aggregation should scale with the enterprise. Enterprises should consider careful creation and integration of risk register templates up and down the enterprise levels. More complex enterprises should examine automated tools to reduce the errors associated with manual processes.

Aggregation activities are performed using the hierarchical levels described in IR 8286A, Fig. 3.[4] System-level CSRRs are combined with others from the same lower-level organization (e.g., business department, branch office, division). In a similar way, the now-combined CSRRs at the organization level (e.g., business unit, government bureau) and enterprise level are aggregated.

Centralizing risk registers in a single place necessitates a way to individually identify a risk from an associated subordinate risk register. This traceability is typically achieved by assigning a unique risk identifier (Risk_ID) to each row in the aggregated spreadsheet. The method for managing the Risk_ID is left to the practitioner, but a source ID (e.g., “System A” CSRR Risk_ID #1 might be tagged as aggregated Risk_ID A-1) is required to support the ability to trace a risk back to the original register. While every enterprise will be different, the important action is to collate all the risks into a summarized risk management knowledge base.

The nature of aggregated risk data in early adopters is that it will be “ragged” or non-normalized. There will be different columns or risk descriptors from each specialized risk register at the lower level of the enterprise. Thus, the enterprise will need to take the non-normalized data and curate it into a standard format. Organizations that implement sound risk management strategy from the top down will avoid these bottom-up inefficiencies. Taking the time to establish standardized guidance, practices, and templates as part of a comprehensive risk management strategy from enterprise leadership will ensure that not only are objectives clear, but also that the processes by which those objectives are efficiently monitored and evaluated are informing their respective management/risk owners.

[4] While integration might take place across many risk disciplines, this report series is focused on cybersecurity risk management and will only describe activities related to the CSRRs.

2.2. Normalization of Cybersecurity Risk Registers

Once data from lower-level CSRRs is aggregated and uniquely identified, it is critical to ensure that the risk data is conditioned to meet the level of the current CSRR. To ensure compliance, the current-level CSRR template must be clearly defined. A clearly defined CSRR template has unambiguous columns and, where possible, enumerated values which can occupy these columns.

If a template does not exist, all incoming CSRRs must be translated into a common format at a given CSRR level. Enterprises that establish a clear process for risk register consolidation or standardize on one format avoid these inefficiencies. This type of normalization activity, if necessary, is part of the information flow from CSRM into ERM. Process improvement and efficiency are gained through clear communication between enterprise levels. Transformation could entail many different techniques of data curation, such as the following:

- **Column renaming** – If a lower-level CSRR has a similar column name with the same information, a simple renaming is sufficient to normalize the data.
- **Default values** – If a lower-level CSRR does not have a given column which is present in the current-level CSRR, a default value could be assigned, such as “N/A,” “0,” “Null,” “None,” “defaultValue,” etc.
- **Value mapping** – If a lower-level CSRR has the same columns as the current-level CSRR but uses a different data enumeration or data scheme, a mapping between the two CSRRs could be useful. For example, if both CSRRs have a “priority” column, and the lower-level CSRR uses the enumeration [high, medium, low] and the current-level CSRR uses the enumeration [1, 2, 3], a mapping could be created. The mapping could look like [(high, 1), (medium, 2), (low, 3)].
- **Column expansion** – If a lower-level CSRR has fewer columns than the current-level CSRR but still has the relevant data, it may be necessary to copy some data into a different column. For example, if the lower-level CSRR has “exposure” as a column with likelihood and impact data within it, and the current-level CSRR has “likelihood” and “impact” columns, a cybersecurity risk manager could copy the relevant segments of the “exposure” data into the “likelihood” and “impact” columns.
- **Column omission** – If a lower-level CSRR has more columns than the current-level CSRR and the data is not relevant to the current-level CSRR, the columns could be dropped and not included in the next-level analysis.
- **Column collapse** – If a lower-level CSRR has more columns than the current-level CSRR and the data is relevant, it may be necessary to copy the data from multiple columns of the lower-level CSRR into a single column of the current-level CSRR. Computation or processing may be needed to achieve this outcome. For example, if “exposure” is in the current-level CSRR and “likelihood” and “impact” are in the lower-level CSRR, the product of “likelihood” and “impact” could be calculated. The result would then be input into the “exposure” column.

- Taxonomy and ontology alignment – ensuring a common taxonomy and ontology is used across risk domains. This includes alignment of the use of ordinal values or actual likelihood and impact expressions.

With all these transformation techniques, it is recommended that a process document be created to ensure uniform application of these techniques across the enterprise.
At a minimum, the normalization process at the higher level (e.g., for the enterprise CSRR) should use the same rating criteria (ordinal, categorical, etc.) to enable comparison and tracking. Good risk management strategy defines these as criteria in the ERP and subsequent ERR template as dictated by the objectives and risk categories (described in Sec. 3). This typically includes definitions for how negative (and positive) consequences and likelihoods are to be measured to enable comparing assessment results. Risk criteria may also describe how time factors, such as risk velocity, should be considered in determining risk severity.

As noted in this series, risk criteria may also consider the organization’s objectives and internal/external context. Criteria for risk escalation or risk elevation (as described in Sec. 2.4.3 of IR 8286B [7]) may also be considered as part of the equation for whether specific cybersecurity risks meet the minimum threshold for enterprise-level discussion. For example, enterprise leaders may note shared risks that represent a broad threat that should be addressed through centralized risk mitigation, or they may identify a reputational risk that demands immediate preventative action.

2.3. Analysis of Cybersecurity Risk Registers

As data points are brought together, there will likely be some risks that occur so infrequently (or are of low enough consequence) that they do not merit inclusion in the next-level CSRR. Integration decisions depend on the use of a common risk rating scheme that enables risk assessments to be translated and integrated at higher enterprise levels.

Additionally, there may be items that are classified as risks which are actually threats, vulnerabilities, methods, exploits and audit/assessment findings which should be removed once discussed with the CSRR owner(s).

During analysis, risk managers review the results from the various CSRRs to support consistent risk taxonomy, treatment and communication. Some examples of risk analysis are described in Table 1. A key element of analysis is the identification and resolution of cases where a similar risk scenario is treated differently by different enterprise participants. There may be no issue with such a difference since context and circumstances might be different, but the underlying cause should be understood, and the disparity should be recognized.

Table 1. Examples of cybersecurity risk analysis

Analysis Activity	Notional Examples
De-duplicate and combine identical or similar risks	• An external attacker deploys a remote access tool and exfiltrates plans for the company’s upcoming merger.

Analysis Activity	Notional Examples
	• External threat actors steal information about marketing plans through malicious code deployed in the sales department. • Malicious parties plant a web shell in an external site that enables them to access documents stored in the Legal Affairs shared document folder, resulting in the loss of critical corporate information.
Reprioritize according to ERM risk appetite and tolerance statements	• Since priorities have been established at the enterprise, organization, and system levels, it may be necessary to review their collective priority and recommend adjustments to a higher or lower priority.
Resolve CSRR disparities	One of two alternatives might be applied: • The combined risk description could be listed in the CSRR for each risk response selected by system owners at lower levels. If two system owners had mitigated the above exfiltration risk and one had chosen to accept it, the risk would appear in the combined CSRR twice, with each row indicating the number of times the relevant risk was selected. • The combined cybersecurity risk would be included once in the CSRR, with both responses included in the risk response type column.
Adjudicate key risks	• Those risks that warrant tracking and further communication in the enterprise-level CSRR (E-CSRR) are highlighted and reviewed by enterprise-level risk managers.

The categories of each cybersecurity risk in each register are likely to be limited and consistent, so that column provides a practical key for the initial sorting exercise. After all the risks at a given level are combined, aggregation is a straightforward activity but may require some manual adjustment. Various risk owners will likely use differing risk descriptions for the same scenario.

For example, consider that three similar risks relating to the exfiltration of sensitive documents, such as internal business documents, patient health records, and employee financial information, might be recorded from various lower-level organizations within the enterprise of the same business unit. The risk manager of that business unit would convert these cybersecurity risks into a single representative risk on the business unit's CSRR, which would include definition of the threat, the asset and the impact such as "External malicious party uses malicious code to exfiltrate sensitive business-related documents." In this case, the risk must describe the type of information that is at risk of theft, since the loss of internal business documents, patient healthcare records, and employee financial information might each have different likelihoods and impacts.

The criteria for delineating these factors will be determined by each enterprise. For example, if sufficiently detailed risk appetite and risk tolerance statements have been recorded, they might provide input into those risk criteria.

The activities described in this report are solely intended to support enterprise information gathering and reporting. Actions for an immediate response, escalation, and notification for any particular risk event should be handled through the enterprise's incident response processes. Similarly, raw risk information from each CSRR should be fully available for any manager's review. Aggregated summarization is a valuable reporting tool, but it should not impede the ability of managers to review specific risk decisions. The reader should also remember that, while aggregation methods and algorithms are helpful, these formulas and data are not intended to take the place of management experience and prudent judgement.

Aggregating the risk analysis from multiple CSRRs follows the same approach as that described in IR 8286A, Sec. 2.3, Detailed Risk Analysis. The method will vary by enterprise, but, for example, a three-point estimation could be used to complete the likelihood and impact columns on the combined register. Using the lowest observed value as the best case, the highest value as the worst case, and the mean value of the others as the most likely, the business unit risk manager could calculate these values. That manager could also apply their knowledge of the personnel and processes used to generate the CSRRs (e.g., a particularly detailed estimate might influence the understanding of the most likely value).

The analysis process results in risk data that is prioritized and risk optimized. Risk priority is detailed in Sec. 3 of this document and Sec. 2.2 of IR 8286B [7]. Risk optimization is detailed in Sec. 2.2.2 of IR 8286B [7]. Risk tolerances, priorities, resourcing, and budget are set by enterprise leadership to monitor risk exposure. The analysis process provides data from the organization and system levels to confirm or deny the appropriate level of exposure. The process of CSRR inputs into E-CSRR, ERR, and ERP provides the organization- and system-level data for making recommendations and informing enterprise strategy and direction.

2.4. Integrating CSRR Details

For some enterprises, aggregation of these risk analysis and risk response values may be both art and science. Some organizations have skilled practitioners with actuarial experience who can statistically aggregate multiple data points and draw a scientific conclusion about the likelihood and impact (and, therefore, exposure rating) of various risks. Other organizations will simply work to normalize a list of highs and lows, with risk managers using their best judgment to estimate the combined exposure. Because the process of analyzing and responding to risk factors is highly iterative, an enterprise might need to begin with qualitative risk values and identify opportunities to increasingly apply quantitative approaches as more information and history become available.

It may be helpful to recall that the exercises in IR 8286C are primarily communicative, sharing information after risk response has been implemented. The information provides valuable data that will guide enterprise-level risk decisions.

Completion of the remaining columns presents opportunities for enterprise determination as follows:

- For an aggregation of the risk response cost column, an organization-level risk manager may wish to record a statistically weighted average of the risk response costs in some cases. In other cases, the manager may wish to provide a total cost allocated across all subsidiary systems and organizations.

- The column for risk owner should indicate an organization-level representative who has the accountability and authority to manage that risk. Risk ownership is a key information point that must be carefully considered and applied. The party designated as the risk owner must be constantly knowledgeable about relevant risk conditions and must also have the accountability and authority to manage the risk. In a commercial enterprise this role may be defined as the business owner (i.e., General Manager of a business unit). Furthermore, a gap analysis between the assigned risk owner and the risk work role can be conducted to see if the practitioner has the necessary skills to address the problem. If not, the assigned individual can be upskilled, a new hire employed, or the risk response changed if necessary. The NICE Workforce Framework [10] can be used for this gap analysis. Although the notional risk register in this series only depicts a column for a risk owner, risk data should include both the role and specific designee; one column or two can be used here. Since risk conditions may change as information is aggregated, responsibility and accountability should be periodically reviewed (e.g., monthly) to ensure that the risk owner is the appropriate designee.
- Risk status for each aggregated cybersecurity risk should use a consistent set of indicators. Status could be a simple indicator (e.g., open, closed, pending, waived, transferred) or provide a more detailed explanation (e.g., “risk accepted pending review by the Jan. 24 quarterly risk committee meeting”).

While the methods and algorithms used will vary by enterprise, there should be a consistent risk aggregation strategy that is expressed as part of CSRM policy within a given enterprise. Given the roll-up process, CSRM — working in conjunction with enterprise risk managers — can include relevant risk policy statements, such as requirements for registering risks, regular updates, and communications about risk activities with enterprise managers and leadership.

Through these procedures and by policy statements, the various cybersecurity risks are integrated into a comprehensive E-CSRR. Note that the processes are described as a bottom-up integration, but real-world scenarios are likely to be interactive and iterative. Integration is important for gathering data and provides opportunities for analysis and adjustment, which are described in the next section.

3. Determining Top-Down Priority: Integration of Cybersecurity Risk into the ERR/ERP

From a top-down perspective, enterprise leaders establish the mission, strategic goals, and strategic objectives. These strategic objectives, and the risks to them, must be prioritized to maximize the efficiency of resources available to the enterprise. Through these prioritized objectives and enterprise risks, cybersecurity risk can be determined and managed through key performance indicators (KPIs) and key risk indicators (KRIs). Therefore, it is critical to have a clear and coherent approach to the categorization and analysis of strategic objectives.

For federal entities, U.S. Office of Management and Budget (OMB) Circular A-11 [11] requires agencies and departments to engage in strategic planning which defines, among other things, the mission, strategic goals, strategic objectives, and performance goals. These performance goals are then tied to cybersecurity risks related to those goals or other indicators as listed, such as KPIs and KRIs, to manage cybersecurity risk to enterprise-defined objectives. This linkage prevents cybersecurity risk management from operating in a vacuum or being executed devoid of enterprise context. Fig. 5 depicts the hierarchy of concepts associated with this strategic planning process. While non-federal enterprises do not have to follow OMB A-11, defining enterprise goals and objectives is a common practice in strategic planning. Critically, enterprises can use their strategic planning initiatives to inform the ERM, and thus CSRM, process. Furthermore, Fig. 5 depicts the setting of performance indicators along with other indicators. These indicators will be crucial to translating objective risk appetite, through risk tolerance, into KPIs and KRIs. These topics are covered in Sec. 5.

Establishing objectives aligned with the stated strategic goals is critical to the success of the enterprise. Certain objectives will include cybersecurity risk components. Federal agencies establish those objectives in strategic, operational, reporting, and compliance categories, while non-federal enterprises may use other objective categories. For example, some organizations establish technical objective types within their own category, while others include them among those listed above. Some entities will define objective categories unique to their lines of business or types of activity. Regardless of the method, it is important that the enterprise establish a relationship between strategic planning objectives and related risk categories. If there is no standardized way for risks to be categorized, the enterprise will find it difficult to align risk mitigation activities with performance results, and performance results with achievement of strategic objectives. This presents a challenge for traceability of lower-level actions to enterprise-level impacts. Commercial enterprises can, at a minimum, evaluate risk in light of impact on revenue and managing expenses.

Ultimately, an enterprise will not have risks only to strategic objectives, but also to other types of objectives which must be managed and prioritized depending on enterprise-specific context and process. An example of this would be the determination of materiality for public companies. The enterprise must evaluate the cybersecurity risk to these objectives to determine the priority of risk response. Each of the steps described thus far in the IR 8286 series contributes to an enterprise-wide understanding of the strengths and weaknesses of cybersecurity risk. Cyber risk is only one of many risks affecting an enterprise, but, considering modern enterprises' extensive dependency on information and technology, cybersecurity represents an important subset of the overall risk posture.

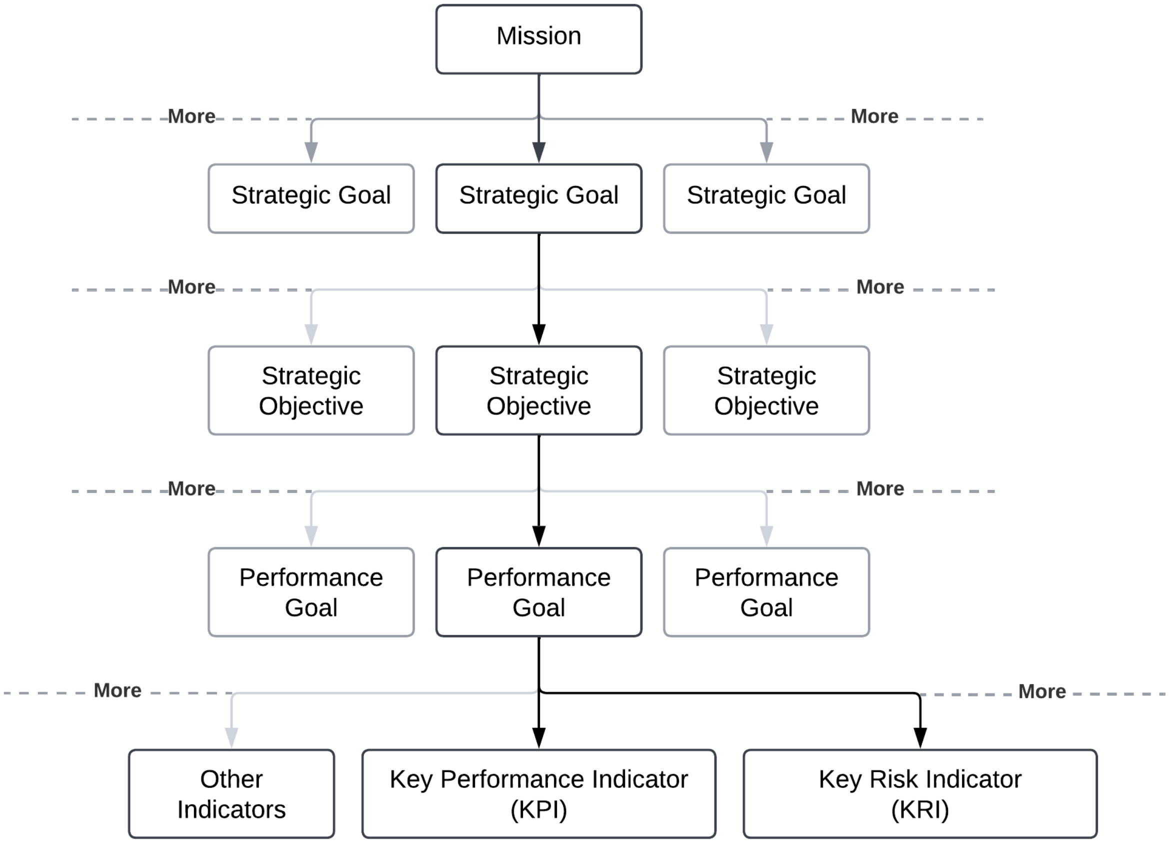


Fig. 5. OMB A-11 strategic planning concepts

The ERR, which reflects the major enterprise-level risks that require sustained management attention, is a useful tool for ERM. A companion artifact, the ERP, describes a selected and prioritized subset of top risks from the ERR. Federal entities maintain an ERP to better catalog the prioritized risks that they face. ERP helps to facilitate discussion and decisions about the aggregate level and types of risk that the agency is managing.

The federal ERM playbook further points out that the risk profile differs from a risk register in that the risk profile is a “prioritized inventory of the most significant risks identified and assessed through the risk assessment process versus a complete inventory of risks” [12].[5] This statement supports ERP use by private-sector entities as well, since the profile and the registers that inform it enable evidence and periodic reviews (e.g., year-over-year comparison, previous quarter, trailing twelve months) of stakeholder decisions, disclosures, and budget adjustments. The selection of prioritized top risks should be informed by the objectives and goals of the enterprise as described above.

Fig. 6 illustrates the flow of risk communication, recorded in various risk registers, to inform the creation of the ERR and — once the ERR contents are prioritized relative to enterprise objectives — the ERP. While this illustrates the flow of information into the ERP, this is an

[5] The United States’ Chief Financial Officers Council, Performance Improvement Council Playbook: *Enterprise Risk Management for the U.S. Federal Government*, provides extensive information regarding ERP formation, including foundational questions listed in its Appendix D. While the publication is provided for U.S. federal agencies, it is useful for any organization that seeks to develop a prioritized and informative understanding of enterprise risk conditions.

iterative and cyclical process. Management of the ERR and ERP drives strategic planning and direction that cascade through the enterprise as part of the standard ERM process.

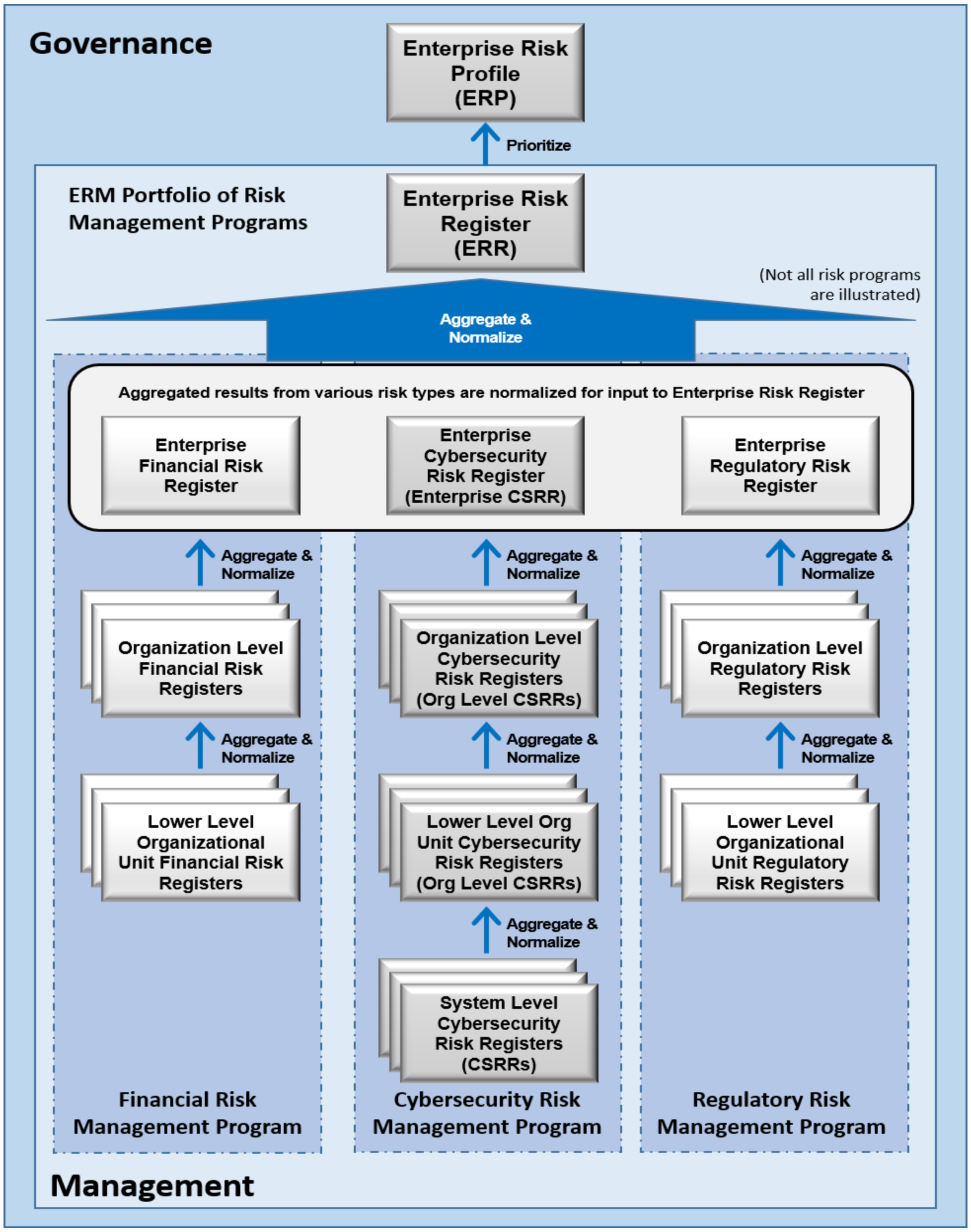

Governance
Enterprise Risk Profile (ERP)
Prioritize
ERM Portfolio of Risk Management Programs
Enterprise Risk Register (ERR)
(Not all risk programs are illustrated)
Aggregate & Normalize
Aggregated results from various risk types are normalized for input to Enterprise Risk Register
Enterprise Financial Risk Register
Enterprise Cybersecurity Risk Register (Enterprise CSRR)
Enterprise Regulatory Risk Register
Aggregate & Normalize
Organization Level Financial Risk Registers
Organization Level Cybersecurity Risk Registers (Org Level CSRRs)
Organization Level Regulatory Risk Registers
Lower Level Organizational Unit Financial Risk Registers
Lower Level Org Unit Cybersecurity Risk Registers (Org Level CSRRs)
Lower Level Organizational Unit Regulatory Risk Registers
System Level Cybersecurity Risk Registers (CSRRs)
Financial Risk Management Program
Cybersecurity Risk Management Program
Regulatory Risk Management Program
Management

Fig. 6. Bottom-up integration of risk registers to create E-CSRR, ERR, and ERP

3.1. Enterprise Value of Incorporating Enterprise CSRRs into the ERP

As with other elements of enterprise risk governance, the specific methods and measures used to incorporate enterprise cybersecurity risk will vary. For some, simply providing the E-CSRR, perhaps supplemented by a risk map, might fulfill stakeholder expectations. Other organizations may take advantage of advances toward better quantification of cybersecurity risk for which visualizations include a range of the percentage of likelihood and financial impacts. ISACA’s Risk IT Practitioner Guide points out that if the board and management have a requirement to quantify risk in financial terms, aggregation might be reported in terms of probable maximum loss (PML) or maximum foreseeable loss (MFL) [13]. Another approach would be to use Value at Risk (VAR) from financial risk analysis.

A primary benefit of this aggregation is visibility. OMB Circular A-123 states,

> In addition, the agency head annually must evaluate and report on the control and financial systems that protect the integrity of federal programs. The three objectives of internal control are to ensure the effectiveness and efficiency of operations, reliability of financial reporting, and compliance with applicable laws and regulations. The safeguarding of assets is a subset of all of these objectives [1].

The aggregation of cybersecurity risks at the enterprise level provides a panorama that is not visible at the system or organization level. In this way, cybersecurity risk aggregation helps to identify both future risks and current issues to be addressed within multiple enterprise subdivisions and potentially determine risk response activities that might be shared among disparate groups.

Notably, while the quote above is based on a U.S. government directive, similar considerations for aggregate cybersecurity risk evaluation apply to private-sector organizations. These include requirements from the U.S. Securities and Exchange Commission (SEC)[6] core principles from the international Basel Committee on Banking Supervision[7] and COSO’s notion of having a portfolio view of risk. (Committee of Sponsoring Organizations of the Treadway Commission: Enterprise Risk Management Integrating with Strategy and Performance).

Since exposure can affect investments, partner cooperation, credit lines, and other financial aspects, evaluation is critical for all types of enterprises.

An ERP that accurately weighs cybersecurity risks is dependent on:

- Accurate and ongoing understanding of the key business and mission-essential functions of the organization;
- Accurate understanding of the relationships and dependencies among enterprise functions and supporting information and communications technology systems (ICT);[8]
- Adequate consideration and factoring of cybersecurity risks in the ERR, including the mission, financial, and reputational impacts of cybersecurity risks; and
- Accurate and comprehensive understanding and timely reporting of key cybersecurity risks and related information (e.g., likelihood, impact, exposure) via the CSRR roll-up described in Sec. 2.

[6] As an example, SEC Regulation S-K requires that publicly traded organizations periodically disclose the material factors that make an investment in the registrant or offering potentially speculative or risky. See https://www.ecfr.gov/current/title-17/chapter-II/part-229.

[7] The Basel Committee on Banking Supervision is the primary global standard setter for the prudential regulation of banks and provides a forum for regular cooperation on banking supervisory matters. See https://www.bis.org/bcbs.

[8] NIST SP 800-221A

3.2. Considerations in Priority: Operational Objectives and Enterprise Impact of Cybersecurity

To better interpret the enterprise impact of various cybersecurity risks in the E-CSRR, and as a prerequisite for contributing to the ERR, enterprise-level risk managers will consider the primary types of consequences into which these risks can be organized. While technology has long been a risk consideration, the increasing complexity and reliance on cyber-connected systems introduce new exposures. For example, while technology failures have always been represented as a risk, highly connected systems and sensors which are part of the Internet of Things can be affected by network latency and duration of connection as well. Thus, latency and connection duration can be viewed as risks.

A subset of the risks described in the enterprise CSRR represents potential losses that could jeopardize one or more operational objectives. Senior leaders (e.g., Chief Information Security Officer [CISO]) will determine whether a failed internal process (related to enterprise people, process, technology, or governance) will directly cause a significant operational impact, which would subsequently present a mission, financial, or reputational enterprise impact.

From the ERM perspective (e.g., Chief Risk Officer, Board Risk Committee), the cybersecurity risk consequences to finance, mission, and reputation inform deliberations of enterprise operational risk (OpRisk) alongside other enterprise risks (e.g., market, credit, geopolitical). OpRisk response activities directly protect mission operations. An example of this is the *Principles for the Sound Management of Operational Risk* described by the Basel Committee on Banking Supervision [14]. It describes operational risk management (ORM), stating that “Operational risk is defined as the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. This definition includes legal risk but excludes strategic and reputational risk.” Enterprise leaders, particularly those in the financial industry, should define these OpRisk parameters as part of enterprise risk strategy.

In its revised ERM framework, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) more fully emphasizes the connection among risk, strategy, and performance, and the revised framework’s name reflects that change [15].[9] COSO posits that risks are to be considered in both strategy-setting and implementation (performance against objectives). Risk practitioners should use these integration and communication processes to manage risks and align activities with the enterprise’s business strategy.

For these reasons, there is a need for a dynamic and iterative process for connecting the entity’s understanding of cybersecurity risk with its strategy. To allow for comparability of risks at an ERP level, a common set of risk criteria should be utilized, similar to normalization at the E-CSRR level. The ERM function may have established a unique taxonomy and ontology for enterprise risks that should be considered when communicating risks at the enterprise level. At all levels of an organization, there needs to be a clear process on how each level of risk registers will inform the next level of risk registers. To ensure the relevance and effective translation of cybersecurity risks at the enterprise level, the CISO (or their equivalent), who is familiar with

[9] COSO ERM Framework: *Enterprise Risk Management–Integrating with Strategy and Performance* (2017). The COSO is a joint initiative of five professional organizations and is dedicated to helping organizations improve performance by developing thought leadership that enhances internal control, risk management, governance, and fraud deterrence.

stating risks in terms of impacts to the enterprise objectives, will need to coordinate with existing ERM functions.

Fig. 7 illustrates a notional risk breakdown structure that aligns cybersecurity risks with enterprise purposes and impacts. These impacts can be cross-cutting. One risk may apply to multiple objectives, and one objective may have multiple risks. Therefore, as risks are identified, evaluated, and monitored, enterprise leaders must analyze risks across the enterprise objectives to determine priority. From there, resourcing and focus can be given to those risks presenting the greatest impact to enterprise objectives.

Prioritization is largely based on the intersection of each risk type (within each risk category) and the enterprise objectives. For example, a particular key risk from Fig. 7 that is likely to affect multiple enterprise objectives may represent a higher priority in the ERP than a risk that affects only one objective. Note that risks that do not affect *any* objectives are unlikely to represent a priority, since risk is defined as the effect of uncertainty on objectives.

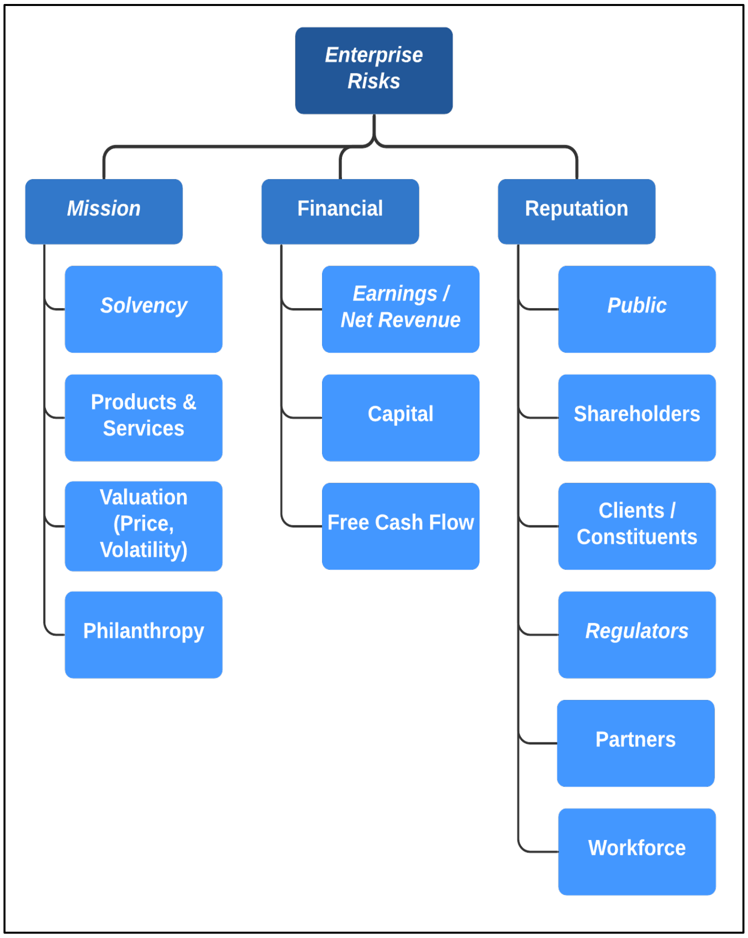


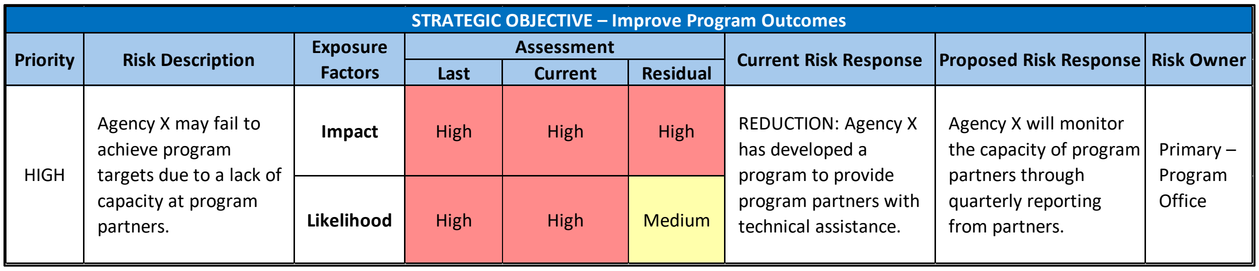
Fig. 7. Notional risk breakdown structure depicting enterprise risk impacts

The following provides more information on elements of Fig. 7:

- **Mission:** Risk conditions that affect the enterprise's ability to achieve objectives.

- **Financial:** Practices that represent exposure to net income, capital, cash flow, and solvency factors, including appropriations and investments.
- **Reputation:** Considerations that might be measurable through key stakeholder surveys or sentiment analysis.
- **Secondary Impacts:** Risk considerations that relate to impacts from cascading consequences. For example, a risk that impedes mission objectives may have a subsidiary reputational impact that may subsequently cause a financial impact. Negative sentiment from a regulator or legislator may impede funding or authorities, restricting operations and, ultimately, mission achievement. For example, a supply chain services provider whose operations are disrupted may impact a number of domains.

The ERR informs the ERP once the risks are prioritized at the highest level of the Risk Management Function in the enterprise, as was depicted in Fig. 5. The ERP is a subset of carefully selected risks from the larger ERR. As the federal ERM playbook points out, there is no single best way to document a risk profile. It should, however, show the connection among objectives, risks, risk changes over time, and proposed risk response information. A notional example from an ERP is provided in Fig. 8.



STRATEGIC OBJECTIVE – Improve Program Outcomes								
Priority	Risk Description	Exposure Factors	Assessment			Current Risk Response	Proposed Risk Response	Risk Owner
			Last	Current	Residual			
HIGH	Agency X may fail to achieve program targets due to a lack of capacity at program partners.	Impact	High	High	High	REDUCTION: Agency X has developed a program to provide program partners with technical assistance.	Agency X will monitor the capacity of program partners through quarterly reporting from partners.	Primary – Program Office
		Likelihood	High	High	Medium			

Fig. 8. Notional ERP example

The ERP reflects assessments of mission, financial, and reputational exposures (combined in the Assessment columns) and is organized according to the four enterprise objectives (Strategic, Operations, Reporting, and Compliance). They may be full-value exposures or may be modified (and so noted) by the likelihood assessments of enterprise leaders. At the top enterprise level, ERM officials have the prerogative to add their judgment of likelihood and impact as part of the normalization process, along with other members of the enterprise risk executive function. When this occurs, it presents an opportunity for these senior leaders to initiate dialogue with the original risk managers to resolve any disparity.

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, impact estimations and risk reserves based on a changing risk landscape. ERPs should also reflect comparable occurrence incidents and trends for the subject enterprise and peer organizations.

3.3. Considerations in Priority: Dependencies Among Enterprise Functions and Technology Systems

Various external factors may also influence priority within an ERR and an ERP. For example, a new move toward digital transformation may heighten sensitivity to cybersecurity risks. For federal agencies, Executive Orders have established supply chain risk management and secure software development as priority focus areas, so those might become key areas of consideration (priorities) for the ERP. Risks related to high value assets (HVAs) and critical enterprise functions represent key dependencies that should be factored into decisions and reporting.[10]

As with many processes in risk management, prioritization is likely to be an iterative progression. As the aggregation of CSRM risks provides an understanding of and visibility into specific cybersecurity risk types, it might gain the attention of senior leaders and become a priority point of focus for subsequent reporting periods. This may, in turn, promote increased scrutiny of the extent to which those risks exist within the enterprise.

Objectives and priorities are rarely tied directly to a cybersecurity activity but instead could be related to a particular set of technical services, processes or resources, (assets). For example, a new customer service offering online sales will have dependencies on various types of technology, such as networks, external payment card processors, and web servers. As mentioned above, the organization may draw upon the information provided by one or more BIA analyses (see IR 8286D for more information [8]) and possibly companion analyses in the form of privacy impact assessments (PIAs) or risk scenario analyses. At the enterprise level, the BIA might be used to consider the impact of cybersecurity risks on balance sheet assets and risk-weighted assets, . The analysis may also record potential impacts on real-time control signals or sensor readings (such as might impact cyber-physical systems or operational technology). In each of these cases, understanding the dependencies and impacts may be strongly influenced by the potential duration, breadth or latency of cybersecurity events.

The BIA provides the connection between technology systems and enterprise risks, helping to inform the understanding of how entries in the E-CSRR may impact enterprise services. The BIA is essential for identifying:

- Business, mission, and enterprise functions;
- The relative priority of those business, mission, and enterprise functions; and
- The relationship between those functions and technology systems.

For this reason, the BIA is a valuable tool for accurately and efficiently factoring cybersecurity into ERM. Other aspects of information technology asset management (ITAM) are critical to understanding the enterprise connection between technology and business functions, so many ITAM processes (such as an accurate asset management database which contains criticality tags like revenue generating, PII or credit card repository or customer facing) are important for fully interpreting cybersecurity risks.

[10] The valuation of enterprise assets, including the determination of HVAs, is described in Sec. 2.2.1 of IR 8286A.

4. Risk Governance as the Basis for Cybersecurity Risk Management

The final two steps of the CSRM/ERM integration process — risk management adjustments and ongoing assessment/reporting — depend directly on effective enterprise risk governance. The topic of governance, including the governance of enterprise information and technology, is sometimes enigmatic for cybersecurity professionals. The principles are straightforward: governance is simply the process of determining enterprise objectives, setting direction to achieve those objectives, and monitoring performance to adjust strategy as necessary.

There can be many details, however, and few enterprise factors are more complex than the evolving fields of IT and OT. The risks associated with governing and managing technology are numerous, but some common processes support consistent implementation. While this section reviews many of the topics covered in IR 8286A, the intent is not to repeat what has already been documented, but to demonstrate how risk management results will be compared with the risk direction and context initially provided, thereby enabling comparison, evaluation, and action.

4.1. Frameworks in Support of Risk Governance and Risk Management

This series highlights the distinction between governance and management. Risk governance is not intended to take the place of risk management activities, and doing so would represent a conflict. Instead, risk governance seeks to set the criteria and expectations by which risk management, including CSRM, will be conducted. It provides the transparency, responsibility, and accountability that enables managers to acceptably manage risk. In this regard, there can be multiple participants in the governance process, depending on context and enterprise type. Larger entities might implement risk governance mechanisms across the enterprise, with more specific governance mechanisms at the organization level (e.g., division, portfolio, or bureau), and apply that strategy at the system or program level. Table 2 illustrates some notional roles and responsibilities at each level.

Table 2. Examples of risk oversight functional roles and responsibilities

Risk Functions	Notional Private-Sector Roles	Notional Federal Government Roles	Notional Responsibilities
Enterprise-Level Oversight	Board of Directors, Regulators, Chief Executive Officer, Chief Operating Officer	U.S. Office of Management and Budget (OMB), U.S. Congressional Oversight Committees, Head of Agency	Ensures alignment with strategic priorities. Monitors and corrects misalignments. Holds management accountable for performance. Receives periodic progress reports.
Enterprise-Level Risk Governance	Chief Risk Officer (or Enterprise Risk Officer), Vice President – Risk Management, Enterprise Risk Management	Senior Accountable Official for Risk Management, Chief Risk Officer, Senior Agency Information Security Officer, Senior Agency Official for Privacy, Risk	Provides oversight, direction, and priorities for the enterprise risk management function. Identifies those risks that may require external reporting or disclosure, including to the public, stakeholders, or regulators.

Risk Functions	Notional Private-Sector Roles	Notional Federal Government Roles	Notional Responsibilities
	Council, Audit Committee Lead	Executive (Function) (e.g., Enterprise Risk Management Council)	
Enterprise-Level Risk Management	Chief Operating Officer, Chief Financial Officer or Controller,[11] Chief Risk Officer	Chief Operating Officer, Chief Financial Officer, Chief Risk Officer, Enterprise Risk Management Officer	Leads and implements the enterprise risk management program. Ensures frequent visibility for high-priority risks that affect the enterprise (e.g., reports quarterly to senior executives on top risks and status of integration of risk management principles in various functions/lines of business). Aggregates and normalizes risks for comparison at the enterprise level in consultation with risk owners. Determines enterprise risk threshold (risk appetite and tolerance) for high-priority risks in consultation with business leads, and ensures that it is communicated to and known by the appropriate staff.
Organization-Level Risk Governance (Subsidiary, Bureau, Operative, or Division)	Division President, Director of Security, Chief Information Officer, Chief Information Security Officer, Division/Unit Risk Officer	Division/Unit Risk Officer, Senior Agency/Chief Information Security Officer, Senior Agency Official for Privacy, Risk Executive (Function)	Establishes and communicates risk management policies, priorities, and expectations across and through the organization in specific risk domains, such as information security and cybersecurity. Partners with enterprise-level risk functions to ensure continued visibility of organization-level risk. Ensures that sub-organization staff are aware of policies, procedures, and risk parameters (e.g., risk appetite and tolerance) to effectively balance risk with mission performance.
System-Level Risk Management	Business System Owner, Risk Owner, Information Owner, Information System Security Manager (ISSM)	Authorizing Official, System Owner, Risk Owner, Information Owner, Information System Security Manager (ISSM), Information System Security Officer (ISSO)	Coordinates with organization-level risk managers (e.g., the CISO) to document and track identified risks and provide input on alignment with established risk parameters. Ensures that risks are being monitored, periodically reports the status to the CISO, and ensures that risk response decisions are communicated back to the Risk Owner.

[11] In U.S. Federal Government, the Chief Financial Officer may be given purview over enterprise risk management functions due to the partnership of those functions with internal controls per OMB Circular A-123. In some agencies, the Chief Operating Officer leads these functions to achieve an integrated view of all types of risk.

As shown in the table, certain enterprise and organization risk governance functions may be delegated to other senior leaders, as determined to be appropriate by the head of the agency or the Chief Executive Officer (CEO). Individual risk programs — including cybersecurity, privacy, and cyber supply chain risk management (C-SCRM) — might then further translate enterprise risk direction (e.g., risk appetite statements) into program-specific risk direction, enabling holistic risk processes while supporting system owners' decision authority. This extended division of responsibility is typical in larger organizations where an officer is specifically assigned to be responsible for program governance (e.g., Chief Information Security Officer, Chief Privacy Officer, etc.).

This enterprise-wide approach is consistent with previous illustrations in the IR 8286 series. Fig. 9 demonstrates how strategic oversight and direction at the enterprise level (Level 1) support organization-specific decisions (at Level 2), which in turn support system-level (Level 3) risk management and reporting. The Cybersecurity Framework [3] helps support a hierarchical approach to coordinating risk management activities across multiple levels, including the activities described within this publication. To illustrate this connection, each of the methods described in Fig. 9 is categorized by the Cybersecurity Framework steps for creating an organizational profile. The correlation of activities is further detailed in Table 3.

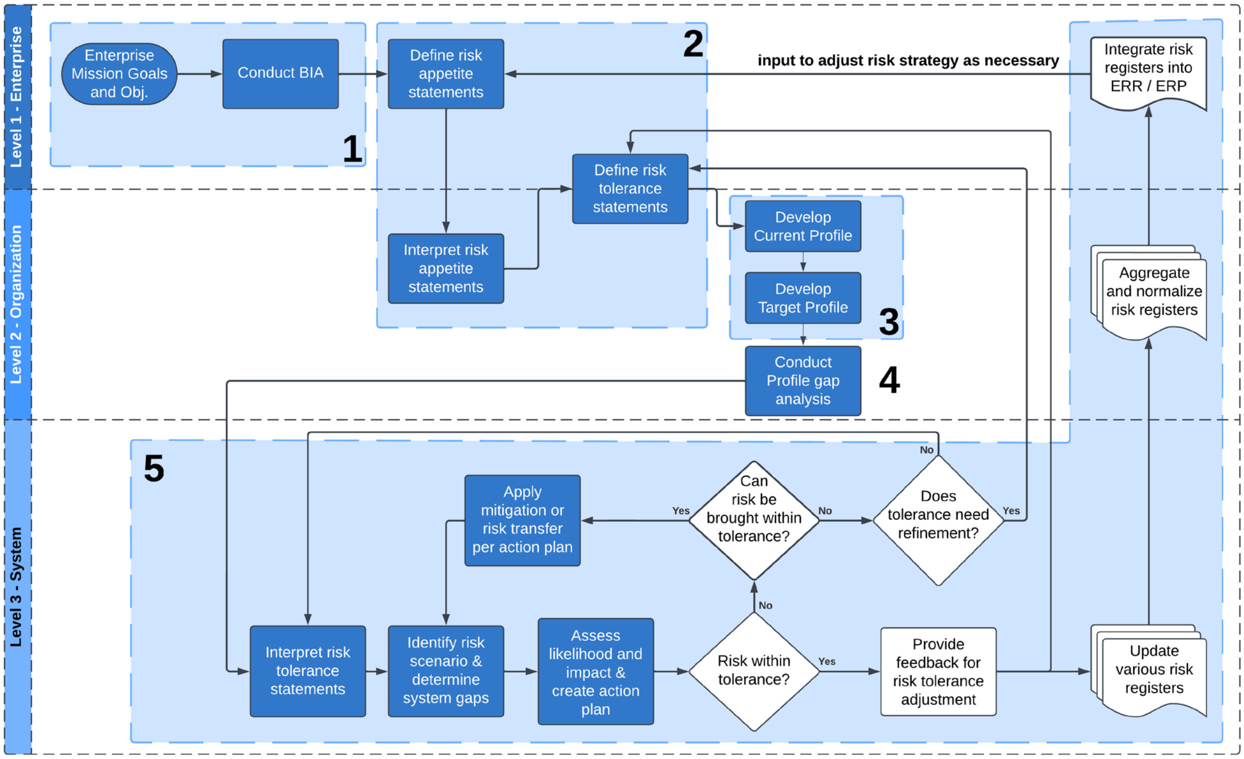

Level 1 - Enterprise
Level 2 - Organization
Level 3 - System
Enterprise Mission Goals and Obj.
Conduct BIA
1
Define risk appetite statements
2
input to adjust risk strategy as necessary
Integrate risk registers into ERR / ERP
Define risk tolerance statements
Interpret risk appetite statements
Develop Current Profile
Develop Target Profile
3
Conduct Profile gap analysis
4
Aggregate and normalize risk registers
5
Apply mitigation or risk transfer per action plan
Yes
Can risk be brought within tolerance?
No
Does tolerance need refinement?
No
Yes
No
Interpret risk tolerance statements
Identify risk scenario & determine system gaps
Assess likelihood and impact & create action plan
Risk within tolerance?
Yes
Provide feedback for risk tolerance adjustment
Update various risk registers

Fig. 9. CSF steps in support of CSRM integration

Fig. 9 shows an overlay of IR 8286A, Fig. 6, *Continuous Interaction Between ERM and CSRM Using the Risk Register*, and the implementation steps described in Section 3.1 of the Cybersecurity Framework [3]. This process demonstrates the application of some of the topics addressed in previous IRs to maintain a comprehensive CSRM program. Specific activities for integrating CSF into CSRM/ERM are described in Table 3.[12]

Table 3. CSF steps as aligned with CSRM/ERM integration

Cybersecurity Framework Step	CSRM/ERM Integration Activity
Step 1: Scope the Organizational Profile	The organization identifies its enterprise mission goals, objectives, and high-level priorities, which are used to inform enterprise risk appetite statements. Senior leaders' direction regarding the applicable budget is an important input to this step since that will influence resource implications and priorities. Pursuant to the established mission and supporting objectives, enterprise leaders conduct ongoing BIAs, which include assets that are critical to achieving those objectives. This list of assets, sometimes referred to as high value assets (HVAs), provides input as to the scope of the CSF Organizational Profile. IR 8286D [8] provides more detail on executing the BIA and the BIA register. This assessment is used in the next step.
Step 2: Gather the information needed to prepare the Organizational Profile	Senior leaders set the direction for risk management strategy with respect to the HVAs determined in part by the BIA and risk scenario analyses. These inputs are often in the form of risk appetite and risk tolerance statements. These statements are used to define parameters for determining acceptable levels of risk. To account for varying types of hierarchical levels, risk tolerance may be interpreted at either the organization or system level to account for variance in business lines or processes. Additional consideration is given to organizational priorities, internal and external context, and risk criteria established for risk assessments at the various levels. Cybersecurity risk managers can use the BIA to make high-level determinations of general threats, vulnerabilities, and their potential impacts. IR 8286A Section 2 provides more detail on these concepts. Results from previous aggregation and integration activities (as described in Sec. 2 and 3 of this report) may help inform the list of potential threats, vulnerabilities, and impacts from system level up through the organization level.
Step 3: Create the Organizational Profile	Iterating through the relevant CSF Functions, Categories, and Subcategories, cybersecurity risk managers document the current processes and activities that contribute to achieving each outcome. The resulting "current profile" provides a comprehensive report of the current risk management program. Observations and results from previous aggregation and integration activities (as described in Sec. 2 and 3 of this report) may help to populate both positive and negative aspects of the current profile. Step 3 provides an opportunity for enterprise stakeholders to review what is currently being done and analyze those activities while considering enterprise risk context and risk strategy (e.g., risk appetite, risk tolerance, compliance requirements). The analysis is also informed by what is already known from previous iterations of the cycle, including risk analysis (see IR 8286A, Sec. 2.3) and risk exposure ratings (see IR 8286A, Sec. 2.4). (continued on next page)

[12] Because NIST has applied a consistent approach for the Privacy Framework, similar activities occur with that model but are not enumerated in this report.

Cybersecurity Framework Step	CSRM/ERM Integration Activity
Step 3: Create the Organizational Profile (continued)	Subsequently, cybersecurity risk managers, informed by an understanding of the risk implications defined in the current profile, determine the desired set of processes and activities that will accomplish stakeholder expectations cost-effectively and efficiently. Development of the target state includes collaboration with enterprise stakeholders regarding the suitable balance of risk optimization and resource optimization. Resources to achieve the targeted outcomes are not unlimited, so this target profile must be developed with an understanding of the priorities and budget described in Step 1. It is also essential that an agency/organization's "first party" risk incorporates supply chain or third-party risk.
Step 4: Analyze the gaps between the Current and Target Profiles, and create an action plan	Using the risk determinations from Step 3 and considering risk tolerance statements, risk practitioners at Level 2 compare the desired set of activities (as documented in the target profile) with current activities (as documented in the current profile). Any outcomes that do not match provide input for planning and implementing improvement. The identification of gaps will help determine system-specific scenarios (as described in IR 8286A, Sec. 2.2) and analyze their likelihood and impact (see IR 8286A, Sec. 2.3) on cybersecurity objectives (such as confidentiality, integrity, and availability). This determination drives the selection of necessary actions to respond to risk and prioritize based on stakeholder direction (see IR 8286B, Sec. 2.2 and 2.3).
Step 5: Implement the action plan, and update the Organizational Profile	Having determined the actions that will align the CSRM processes and activities with stakeholder expectations, budget, and priority, cybersecurity risk practitioners then determine the appropriate risk treatment for the various risk scenarios (including the projected risk response cost) and document the known risks in a CSRR. Scenarios that have not fully satisfied the criteria for risk acceptance but that have been approved by a cognizant official to be treated at a future time (or based on a future condition) might also be documented in a Plan of Actions and Milestones register.
Iteration	As CSRRs from throughout the enterprise are reviewed, aggregated, normalized, analyzed, and integrated in an ERR and ERP, data points from these registers provide input into subsequent iterations of the cycle. Continuous monitoring and learning enable input to the cybersecurity risk strategy, adjustments to that strategy to pursue opportunities, and reduced exposure throughout the enterprise.

By applying these steps, risk practitioners at various hierarchical levels will be able to consistently evaluate and communicate necessary actions and document any adjustments needed to ensure continued alignment. Many of the Core outcomes described in the Cybersecurity Framework and Privacy Framework contribute directly to ongoing governance processes.

4.2. Adjustments to Risk Direction

The detailed workflows in Fig. 9 (above) illustrate six points where risk decisions drive activity to adjust risk response, risk constraints, or both. Adjustments provide inputs to and feedback from the dynamic enterprise CSRM life cycle (Fig. 10, below) as a critical component of a healthy risk management ecosystem.[13] Monitoring of performance and risk indicators provides data points that, along with other enterprise performance information, can be used to identify whether adjustments in risk direction are necessary. The high-level approach described below, informed

[13] The ERM Quick Start Guide provides additional guidance on how to implement Fig. 9 using the CSF. https://doi.org/10.6028/NIST.SP.1303

by detailed considerations as shown in previous illustrations, provides input into the ongoing assessment and reporting of enterprise cybersecurity risk conditions. Because enterprise objectives, risk landscape, and stakeholder needs are continually evolving, this ongoing life cycle includes dynamic adjustments. Information from the risk register, including data gathered about potential risk scenarios, their impacts, and ongoing response actions provides input to the BIA process. Information about BIA and asset valuation is described in IR 8286D [8].

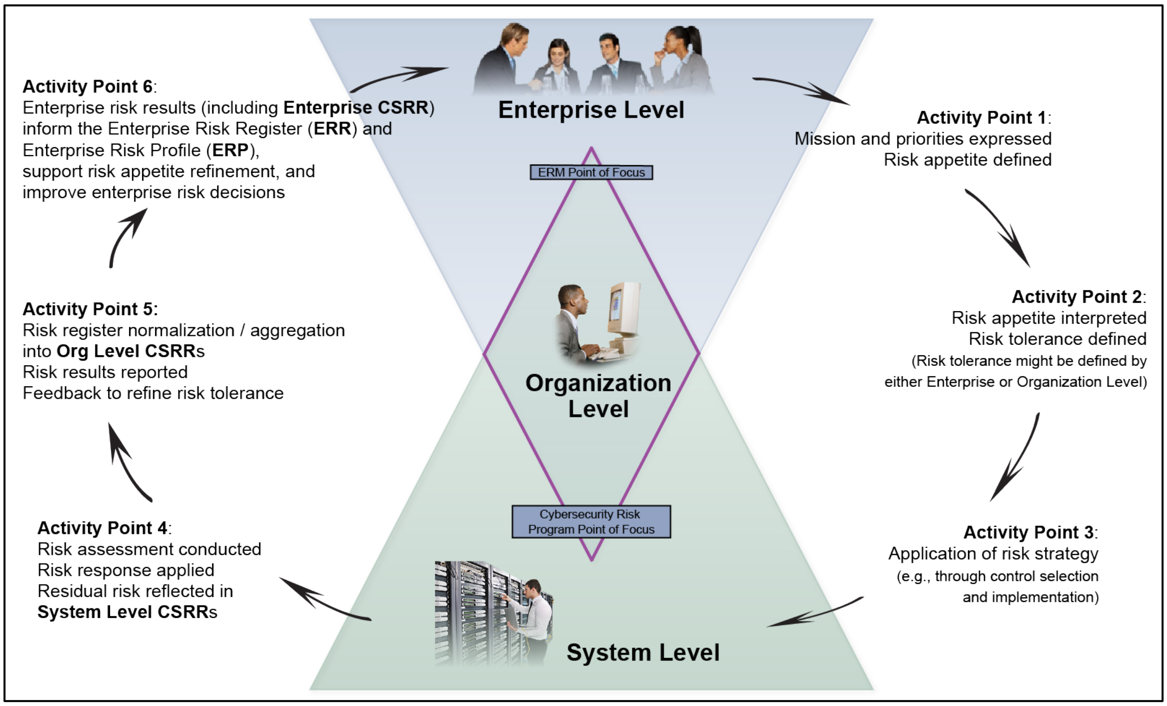

Enterprise Level
ERM Point of Focus
Organization Level
Cybersecurity Risk Program Point of Focus
System Level
Activity Point 1:
Mission and priorities expressed
Risk appetite defined
Activity Point 2:
Risk appetite interpreted
Risk tolerance defined
(Risk tolerance might be defined by either Enterprise or Organization Level)
Activity Point 3:
Application of risk strategy
(e.g., through control selection and implementation)
Activity Point 4:
Risk assessment conducted
Risk response applied
Residual risk reflected in **System Level CSRRs**
Activity Point 5:
Risk register normalization / aggregation into **Org Level CSRRs**
Risk results reported
Feedback to refine risk tolerance
Activity Point 6:
Enterprise risk results (including **Enterprise CSRR**) inform the Enterprise Risk Register (**ERR**) and Enterprise Risk Profile (**ERP**),
support risk appetite refinement, and
improve enterprise risk decisions

Fig. 10. Illustration of enterprise CSRM and coordination

These adjustments might be related to budget considerations (i.e., capital and operating expenses to support risk management investments). They may also involve changes to the risk appetite and tolerance parameters that drive subsequent risk management decisions. Some considerations for each of these elements are described below.

4.2.1. Adjustments to Cybersecurity Program Budget Allocation

In both public- and private-sector enterprises, resource considerations are often described as a contributing factor for diminished cybersecurity performance or increased risk. To some extent, the claim that a program “needs more resources” is justifiable in that there are always more tools, personnel, and services that could be added. However, effective CSRM requires a balance among risk optimization, resource optimization, and the value delivered by the technology being protected. If any of these three factors results in an imbalance, the solution is untenable. For this reason, CSRM informs the decisions around which areas receive priority within limited budget environments.

The factors that have been discussed thus far in the IR 8286 series can help to evaluate the extent to which the risk/resource balance is well-tuned. For example, because risk decisions are based on stakeholder needs (and the resulting enterprise and alignment objectives), cybersecurity activities can be traced back to actual business value. In theory, one can simply build a business case that demonstrates the value proposition/financial impact of investment in cybersecurity protection, detection, and response resources. It can be quite challenging to directly report the subsequent return on that security investment. One way to address this challenge is by applying detailed risk assessment and reporting activities, such as those described in this IR series. Quantitative methods provide calculations that enable the risk practitioner to simulate risk likelihood and financial impact before and after implementation of the cybersecurity improvement. This drives a straightforward cost-benefit analysis of the resource investment.

These recommendations are intended to help the enterprise develop a balanced approach for providing the information needed for management decision support. Practitioners should not presume that collecting more operational data is always better, nor that a single number (as determined from a model) is what leadership needs for management decision-making. The methodology implemented must provide the complete range of information that leadership might rely on for making risk-informed decisions.

Organizational leadership is seeking assistance with translation, integration, structuring, and analysis to deal with the volume of data and the complexity of the decision calculus while risk-informing strategic decisions. Many organizations have plenty of cyber operational data yet are unable to frame and aggregate analyses in a transparent and repeatable way that helps leadership consistently interpret, synthesize, and act on the messy multiple streams of data to make strategic decisions. Quantitative analysis methodologies are an example of one approach that uses cyber operational data to evaluate the likelihood and impact or risk scenarios like ransomware.

Another budgetary consideration results from the aggregation activities described in Sec. 2. As managers and leaders review the activities performed and the risk results provided, they might identify opportunities to centrally fund and operate risk management activities that had previously been the responsibility of individual system owners. It might make fiscal sense to combine activities to gain efficiencies or reduce duplication. As such opportunities become apparent during the review of CSRR reports and results, leaders might make fiscal adjustments to gain an advantage.

4.2.2. Adjustments to Risk Appetite and Risk Tolerance

In addition to fiscal considerations, observations during the life cycle may also provide feedback on leaders' risk criteria, risk appetite and tolerance statements. Fig. 10 (above) illustrates several key decision points, including:

- Risk acceptance at the system level. In selecting the appropriate controls for a given information system (or shared set of controls), is a risk already acceptable, given the applicable risk tolerance statements?

  - If it is not acceptable, the system owner has the option of applying additional risk response (as described in IR 8286B, Sec. 2.3), through either risk sharing or mitigation by various security and privacy controls.
  - At times, risk cannot be brought within tolerance through any combination of controls, or the cost of the controls might be unreasonable for the system being protected. In such a case, it is possible that there might be limited ability to adjust risk tolerance. Discussion with decision-makers is necessary to determine the appropriate course of action. That discussion might also support guidance for other enterprise systems facing similar risk scenarios.
- Additional decision points occurring after the aggregation and integration of CSRRs at various levels. As risk managers review the risk registers, risk management results will be compared with stakeholder expectations. Based on the aggregated results, cybersecurity risk managers may need to consider the following questions:
  - Is risk response consistent across various organizational structures and levels? Based on risk analysis, response, and monitoring results, risk managers may determine that additional guidance is needed to better achieve repeatable and reliable risk management activities. Adjustments in policy, procedure, staff training, and other governance components might be necessary to improve process maturity.
  - Has the risk environment evolved (perhaps due to changes in internal or external context, such as new regulations or customer agreements) to such an extent that the risk direction or criteria need to be adjusted? If so, this provides an opportunity to repeat the cycle illustrated in Fig. 10.

In addition to these programmatic adjustments, specific risk treatment adjustments might be identified during continuous monitoring and ongoing assessment activities. Such adjustments are described in Sec. 5.

4.2.3. Reviewing Whether Constraints Are Overly Stringent

A challenge for senior managers is ensuring that their organizations are permitting enough risk, especially those risks that help realize benefits (i.e., opportunities, rewards). Asking questions concerning the appropriate balance between risk and opportunity helps those in risk governance roles identify whether their risk managers are using the risk governance tools and processes correctly or if the risk governance tools and processes need adjustment.

This Cybersecurity Framework [3] process can help manage the pursuit of opportunities. The IR 8286 series stresses the importance of recording and acting upon positive risk. Each risk aggregation, normalization, analysis, and integration activity should identify the impacts of beneficial uncertainty that will accentuate the likelihood of achieving enterprise objectives. Examples could include recognition that the addition of machine-learning technology would significantly increase the throughput of the enterprise research team and could lead to expansion into new marketing areas; or that the addition of high-availability services for the enterprise web server will improve availability from 93.4 % to 99.1 % over the next year and will also improve market share by 3 % due to improved customer satisfaction.

Comments received throughout the development process of this series continue to reflect that the management of positive risk/opportunity is a field of interest that is new to many readers and merits further exploration. In that way, the topic itself represents a positive risk or opportunity for the risk community to create a more balanced approach to considering, measuring, and managing the uncertainty of all types of risk in pursuit of the enterprise mission.

It is rare that an opportunity can be realized without a negative risk. One might also question why anyone would embark on a circumstance that results in a negative risk without a corresponding opportunity that makes such an endeavor worthwhile. A basic objective of risk management programs is to identify individual negative risks so that they can be matched to their corresponding positive risks, enabling trade-off analysis. With individual negative risks identified, the risk program is prepared to move ahead with a risk response, should the trade-off analysis render a decision to proceed with the positive risk.

4.2.4. Adjustments to Priority

A final program-level adjustment relates to enterprise priorities. As has been expressed throughout this series, all cybersecurity risk decisions flow from the enterprise's mission and priorities. This is illustrated by Activity Point 1 in Fig. 10 where senior leaders establish the mission and priorities, which drive strategic objectives and planning, which are then used to direct CSRM activities. Subsequently, risks that are identified and assessed are recorded in the CSRR in accordance with those priorities. As shown in IR 8286B, Sec. 2.2, the order in which risks are addressed, the direction of appropriate responses, and even the agreement about which risks will be addressed are all derived from the enterprise priorities. For this reason, a key enterprise activity will be a periodic review of those priorities and the effects that they have on CSRM. Reviewing priorities should be done in concert with the internal cadence of the key risk committee meetings (e.g., quarterly). Based on the results of such reviews, priorities might be adjusted or clarified to ensure continued alignment between CSRM activities and mission objectives.

5. Cybersecurity Risk Monitoring, Evaluation, and Adjustment

As shown throughout the IR 8286 series, it is important to remember that risk management is not simply managing lists of risks. For the activities to be meaningful, risk managers throughout the enterprise must be informed about objectives, results, priorities, and opportunities. A key purpose of the various risk registers is to enable ongoing monitoring of enterprise risk activities. These activities are tied to objectives defined by enterprise leadership (and detailed in Sec. 3). Based on those activities, senior leaders evaluate available options and adjust guidance and operations to help realize opportunities and minimize harmful impact.

This iterative approach begins where IR 8286A started: with an understanding of what risk limits are acceptable, given enterprise context and strategic objectives. The purpose of CSRM integration in support of ERM is to enable senior leaders to remain aware of ongoing risk management activities and apply corrective measures to achieve enterprise objectives. To do so, leaders apply a Monitor-Evaluate-Adjust cycle, as illustrated in Fig. 11.

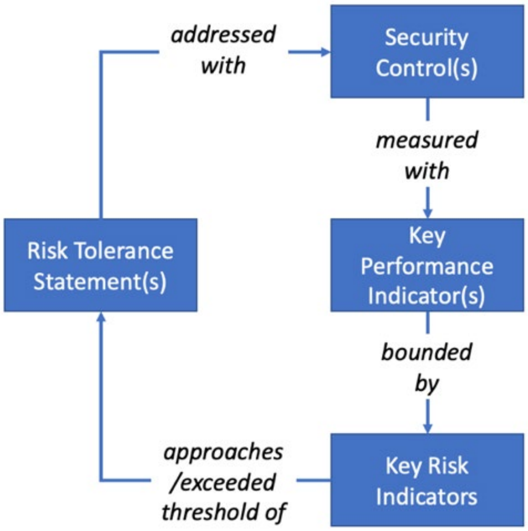

addressed with
Security Control(s)
measured with
Risk Tolerance Statement(s)
Key Performance Indicator(s)
bounded by
approaches /exceeded threshold of
Key Risk Indicators

Fig. 11. Monitor-Evaluate-Adjust cycle

Risk tolerance interpreted based on risk appetite direction is achieved through the application of various risk responses, including the application of security controls. The measurement of the performance of those controls through KPIs, especially those metrics that represent KRIs, enables oversight and management of the achievement of the risk tolerance.

Previous discussions highlighted risk direction based on risk appetite statements and their interpretation as risk tolerance statements. There is a third component of risk direction that must be observed: risk capacity, defined as the maximum amount of risk that an organization is able to endure. While the enterprise should always take steps not to exceed risk appetite, the consequences of doing so are rarely catastrophic. Exceeding risk capacity, on the other hand, could have dire consequences and may even jeopardize the continuance of the enterprise. Catastrophic results are not limited to the private sector. Many government entities have experienced severe consequences because their risk management processes permitted them to approach or exceed risk capacity. Such cases can end the careers of senior leaders whose risk monitoring should have identified the risk conditions. It is noteworthy that, like risk appetite and tolerance, risk capacity can extend throughout the hierarchical enterprise layers. For example, if a business unit or government bureau exceeded its risk capacity, that portion of the enterprise could be severely impeded or closed.

ISACA states that exceeding risk capacity could result in the enterprise's continued existence being questioned.[14] International Organization for Standardization (ISO) 31010:2019 describes a similar example: "For a commercial firm, capacity might be specified in terms of maximum retention capacity covered by assets, or the largest financial loss the company could bear without having to declare bankruptcy" [16]. While exceeding risk capacity might not immediately result in enterprise extinction, it is clearly a criterion that must be monitored closely. Because capacity reflects the aggregate risk, it is relevant to the functions described here and is an important consideration for those aggregating CSRM and evaluating the overall risk posture. In the private sector, risk capacity should be evaluated to determine if cyber insurance is appropriate and how much risk can be transferred.

5.1. Key CSRM Mechanisms

To monitor, evaluate, and adjust risk, risk tolerance statements are translated into the inter-related triad of security controls, KPIs, and KRIs. While these mechanisms are administered at Level 3, they are dependent on the foundational Level 2 cybersecurity risk activity of establishing and communicating risk tolerance.

Risk tolerance statements are central to all risk management activities and represent a decomposition of risk appetite. In that respect, tolerance is always more specific than appetite. To help support performance measurement and reporting, it may be helpful for both risk appetite and tolerance to be specific and quantifiable. Through actionable, measurable direction, results can be measured over time through performance metrics, risk trends, and outcomes achieved. Those performance measures that demonstrate program success (i.e., KPIs) and those that are particularly valuable for predicting risk (i.e., KRIs) help to both document progress and enable necessary adjustments.

5.2. Monitoring Risks

Risk communication at each level is based on the risk management activities feeding into it. For example, reporting and communication about cybersecurity risks at the Organizational Level are informed by the System Level results. Each integration and aggregation cycle provides an opportunity for monitoring the results and considering any changes that have occurred since previous iterations.

KRIs can be observed to monitor trends and identify potentially beneficial (or harmful) circumstances. A risk practitioner who observes changes in a KRI might look to determine, for example, whether:

[14] Retrieved from ISACA's online interactive glossary, https://www.isaca.org/resources/glossary

- The likelihood of an identified risk is increasing,
- The severity of the consequences is increasing,
- A new risk has entered the environment, or
- Controls are failing.

The practitioner will be further aided by the use of the CSRR, especially the risk category. At each of the hierarchical levels, the subordinate CSRRs are examined, and:

- The risks in a particular category are grouped together.
- Similar risks within each category are normalized. A specific taxonomy can be applied, or the practitioner can simply adjust the wording as needed.
- The enterprise (or organization) strategy can decide how the aggregate scores will be determined.
    - Evaluation could be as straightforward as counting how many of each type of risk are present and then dividing by the number of samples.
    - Since certain sub-organizations or systems have a higher priority, there might be some weighting score applied, or the total exposure could simply be summed, resulting in a composite exposure value.

Because much of the aggregation and integration will have already been applied, the E-CSRR represents a straightforward list of the descriptions, categories, assessment results, and status. A key element of the E-CSRR will be the priority column since this is a key input to the overall enterprise risk considerations.

At each sub-level, risks that exceed leading KRIs may be reported according to normal periodic reporting. However, risks that exceed lagging KRIs should be reported in some form of intermediate communication, such that applicable parties understand that the risk has exceeded risk tolerance.

It may be helpful for enterprise risk stakeholders to develop a list of various actions to take during monitoring. For example, upon determining significant changes in particular risk areas, actions might include:

- Create a working group to identify root causes and recommended next steps.
- Assign a group of risk types to a centralized risk owner to reduce variance and ensure accountability.
- Determine other organizational processes to improve protection, detection, and response in preparation for those risks that seem both likely and impactful. Such processes might include the introduction of additional tools (e.g., logging and event orchestration), response training (e.g., incident response handling exercises), or review of insurance coverage.

Depending on enterprise strategy and policy, additional reporting actions might also be required. For example, government entities might need to advise those providing oversight, including inspectors general or regulators. Commercial organizations may have similar reporting requirements to shareholders, key stakeholders, and external auditors. For larger enterprises, a cybersecurity risk management system may be appropriate to ensure that all activities are effectively and efficiently captured and managed.

Given the dependency of the ERP and ERR on program risk assessment and evaluation, the periodicity of risk assessment and roll-up should be architected to enterprise risk reporting and disclosure requirements. For instance, publicly traded organizations may have a quarterly risk disclosure obligation, which means that the basis of that disclosure — the ERP — needs to be updated quarterly. In this case, all subordinate assessment, evaluation, adjustment, and reporting (i.e., risk register) processes need to cycle at least quarterly, if not more frequently.

5.3. Evaluating Risks

Risk evaluation is a vital element of the continuous risk monitoring process. The purpose of the evaluation is to assess changes to any of the four components of a cybersecurity risk (i.e., asset valuation, threat event probability, vulnerability, and impact).

As an input to ERM, CSRM requires a dynamic and collaborative process to maintain balance by continually monitoring risk parameters, evaluating their relevance to organizational objectives, and responding accordingly when necessary (e.g., by adjusting controls). As noted above, this evaluation also represents an opportunity to learn whether the positive risk has changed. If the likelihood of an opportunity has increased, the offsetting risk analysis might need to be adjusted. If positive conditions have decreased, additional scrutiny might be necessary for the cost side of a cost-benefit analysis.

Fig. 11 (above) shows that evaluation takes place by considering whether security controls have performed effectively (through KPIs) and the extent to which that performance manages risk to an acceptable level (KRIs). While level 3 security control assessments provide an understanding of whether a given set of controls (as described in the system security plan) is achieving its objectives, the evaluation described here fulfills a broader need. Observations during the Manage-Evaluate-Adjust (MEA) process are intended to inform whether adjustments are needed to strategy, policy, or general practices. For example, a KPI for determining the number of business applications that have not been adequately protected by proven backup solutions might inform a KRI that documents an organization-level exposure. This observation may, in turn, trigger a review of whether the risk tolerance statements adequately provide direction (and metrics) regarding system and data backup requirements.

Monitoring protects the value provided by enterprise information, and technology requires the continual balancing of benefits, resources, and risk considerations. Frequent and transparent communication regarding risk options, decisions, changes, and adjustments improves the quality of information used in making 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. Using automated risk management tools for reporting and dashboarding can help provide ongoing insight to various levels of stakeholders, including operations managers and senior leaders.

Risk evaluation also involves the ongoing determination of a target state. An ongoing process of considering the gaps between the current state and the desired state enables risk managers to quickly identify opportunities for improvement and to document those observations (e.g., in risk detail records). A healthy enterprise risk culture can engage the whole enterprise in proactively monitoring risk successes, shortcomings, and results. Table 4 (drawn from IR 8286) shows examples of evaluation opportunities that enable determining if the program is on track or needs adjustment.

Table 4. Examples of proactive risk management evaluation activities

Example Risk Area	Example Supporting Activities
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 the effective management of risks is an important part of everyone's job.
Risk Response Preparedness	Conduct exercises to provide practical and meaningful experience in recognizing, reporting, and responding to cybersecurity risk scenarios.
Risk Management Governance	Remind staff of organizational policies and procedures that are established to help improve risk awareness and response.
Risk Transparency	Enable an environment where employees and partners may openly and proactively report potential risk situations without fear of reprisal.
Risk Leadership	A group of individuals dedicated to driving risk management culture.

A comprehensive risk evaluation process at all hierarchical levels, particularly at the enterprise level, enables the effective and efficient detection of positive risk trends that can be exploited and negative risk trends that must be rapidly addressed to avoid harmful impact.

5.4. Adjusting Risk Responses

Based on the evaluation, risk managers adjust their risk response approach. In some cases, the evaluation will provide evidence that risk response has been effective and is efficiently achieving the necessary level of risk treatment. In other cases, adjustments to risk direction, risk treatment, or both may be necessary.

Aristotle is commonly credited with teaching that the whole is not the same as the sum of its parts. Such an observation highlights that the composite set of enterprise risk likelihood and impact is something besides and not necessarily equivalent to the sum of the risk analyses described in the various CSRRs.

As controls are applied throughout the enterprise and as indicators are produced (and reported through metrics), various managers and leaders will consider the evaluation produced in the previous section. Given the resulting observations, several adjustments may be warranted, as described below.

- **Adjust Strategic Direction** – Based on collective results, senior leaders may update risk appetite statements to increase or decrease risk limits, such as adjusting specific quantitative direction. In addition to or in place of risk appetite adjustment, risk tolerance interpretation may similarly be adjusted to take advantage of opportunities or to reduce the likelihood or impact of harmful risks.
- **Adjusting Risk Responses** – To address inconsistent responses to risks or achieve a different result, leaders may choose to direct specific response actions to one or more risk scenarios or family of scenarios. For example, if some organizations decided to mitigate a given risk type and others chose to accept it, risk managers may clarify which treatment is the appropriate response (or clarify the criteria by which that decision is made). As with previous discussions, this adjustment may be to reduce the overall exposure by enacting a more stringent response, or it may direct a loosening of restrictions to gain some advantage in exchange for a measured risk increase. Such changes may occur gradually to ensure sufficient CSRM at all hierarchical levels.
- **Adjusting Key Performance or Risk Indicators** – While the enterprise may adjust their specific direction or treatment of risk, the result of the evaluation will often be increased monitoring of the various conditions. Especially when conditions indicate broad variance in resulting metrics, managers may direct changes to the KPIs and KRIs that are monitored to gain better visibility. If changes to impact and/or likelihood cannot be adequately observed with the current indicators, different (or additional) metrics may be justified. Increased frequency is indicated when impact and/or likelihood change more rapidly than the current monitoring interval.

The adjustments described are intended to provide improvement that is directly based on the results of monitoring and evaluating risk. Additional adjustments may be based on external direction, such as requirements by a regulator for increased risk management or new reporting criteria (e.g., updated quarterly metrics for the Federal Information Security Modernization Act [FISMA]).

5.5. Monitor, Evaluate, and Adjust Examples

To tie it all together, Table 5 provides several examples of related risk appetite, risk tolerance, controls, KPIs, and KRIs. Some of the risk appetite and tolerance statements (indicated in *italics*) are drawn from Table 1 in Sec. 2.1.1 of IR 8286A.

Table 5. Notional examples of MEA activities

	Example 1	Example 2	Example 3
Risk Appetite	*Mission-critical systems must be protected from known cybersecurity vulnerabilities.*	*To safeguard protected health information, we must ensure that only authorized parties have access to our computer systems.*	*Our customers associate reliability with our company's performance, so service disruptions must be minimized for any customer-facing websites.*
Risk Tolerance	*Systems designated as mission-critical must be patched against critical software vulnerabilities (CVSS score of 10) within 14 days of discovery.*	*We will issue unique user accounts and will monitor failed login attempts for both the individual user and all users. A maximum of 5 failed login attempts per user per hour and 30 across all users per hour is acceptable.*	*Regional managers may permit website outages lasting up to 2 hours for no more than 5 % of its customers.*
Control(s)	• Periodic vulnerability assessments • Patch deployment capabilities	• Unique user accounts • Authentication methods • Audit logs • Audit log alerting/evaluation	• Power generator • AC unit • Upstream network provider • Web load balancers • Web servers
KPI	• Percentage of critical vulnerabilities patched	• Unsuccessful logins in a 1-hour period	• Outage time in hours • Customer outage percentage
Leading KRI	Number of mission-critical systems with critical (CVSS score of 10) vulnerabilities that have not been patched in 10 days	• 4 failed logins for a single user within an hour • 25 failed logins across all users within an hour	• Outages lasting 1.5 hours affecting more than 5 % of customers • Outages lasting over 2 hours that affect fewer than 5 % of customers
Lagging KRI	Number of mission-critical systems with critical (CVSS score of 10) vulnerabilities that have not been patched in 15 days	• 6 failed logins for a single user within an hour • 35 failed logins across all users within an hour	• Outages lasting over 2 hours affecting more than 5 % of customers

When quantitative assessments are used, increases in the values for likelihood and financial impacts can be used as KRI's.

6. Conclusion

Systematic aggregation, normalization, and analysis of cybersecurity risk registers (CSRRs) help risk managers gain a comprehensive understanding of an enterprise's cybersecurity risk posture, effectively supporting enterprise-level decision-making and governance.

The integration approach described in this publication enables organizations to transform disparate, system-level cybersecurity risk information into actionable data for senior leadership. By establishing clear processes for consolidating CSRRs into enterprise-level risk registers and risk profiles, organizations gain the visibility necessary to make informed strategic decisions about resource allocation, risk appetite adjustments, and operational priorities.

The bottom-up integration of risk information through organizational levels provides comprehensive visibility into cybersecurity risks while maintaining the granular detail necessary for effective risk management at operational levels. This bidirectional sharing of information, including application of the NIST Cybersecurity Framework and other risk management models, enables prioritization while preventing critical risks from being overlooked.

The cybersecurity risk landscape continues to evolve rapidly, driven by changing threat environments and evolving technological advances. The frameworks and processes described in this publication provide a foundation for managing this complexity, but they must be implemented as part of a broader commitment to adaptive risk management that can evolve with changing circumstances. The use of both bottom-up and top-down risk approaches supports robust, mature enterprise risk management. Organizations that establish standardized templates, taxonomies, and processes from the enterprise level down will gain efficiencies and a broad perspective across the risk landscape; bottom-up integration of risk management documentation and results will support comprehensive understanding and coordination. This integrated risk management practice is described in the next document in this series, NISTIR 8286D. [8]

References

[1] 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://trumpwhitehouse.archives.gov/sites/whitehouse.gov/files/omb/memoranda/2016/m-16-17.pdf

[2] 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://trumpwhitehouse.archives.gov/sites/whitehouse.gov/files/omb/circulars/A130/a130revised.pdf

[3] 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

[4] Quinn SD, Ivy N, Chua J, Barrett M, Feldman L, Topper D, Witte GA, Gardner RK, Scarfone K (2023) Enterprise Impact of Information and Communications Technology Risk: Governing and Managing ICT Risk Programs Within an Enterprise Risk Portfolio. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-221. https://doi.org/10.6028/NIST.SP.800-221

[5] Quinn SD, Ivy N, Chua J, Scarfone K, Barrett M, Feldman L, Topper D, Witte GA, 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) 800-221A. https://doi.org/10.6028/NIST.SP.800-221A

[6] Quinn SD, Chua J, Ivy N, Gardner RK, Kent 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. https://doi.org/10.6028/NIST.IR.8286r1

[7] 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. Includes updates as of February 26, 2025. https://doi.org/10.6028/NIST.IR.8286B-upd1

[8] 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. Includes updates as of February 26, 2025. https://doi.org/10.6028/NIST.IR.8286D-upd1

[9] 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. https://doi.org/10.6028/NIST.IR.8286Ar1

[10] Petersen R, Santos D, Wetzel KA, Smith MC, Witte GA (2020) Workforce Framework for Cybersecurity (NICE Framework). (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-181, Rev. 1. https://doi.org/10.6028/NIST.SP.800-181r1

[11] 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://trumpwhitehouse.archives.gov/wp-content/uploads/2018/06/a11.pdf

[12] Chief Financial Officers Council (CFOC) and Performance Improvement Council (PIC) (2022) Playbook: Enterprise Risk Management for the U.S. Federal Government. Available at https://comptroller.defense.gov/Portals/45/documents/micp_docs/Authoritative_Laws_and_Regulations/FINAL-ERM-Playbook.pdf

[13] ISACA (2020) Risk IT Framework, 2nd Edition. Available at https://www.isaca.org/resources/it-risk

[14] Basel Committee on Banking Supervision (2011) Principles for the Sound Management of Operational Risk. Available at https://www.bis.org/publ/bcbs195.pdf

[15] 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

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

Appendix A. List of Symbols, Abbreviations, and Acronyms

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

BIA
Business Impact Analysis

CEO
Chief Executive Officer

CISO
Chief Information Security Officer

COSO
Committee of Sponsoring Organizations

CSF
Cybersecurity Framework

CSRM
Cybersecurity Risk Management

CSRR
Cybersecurity Risk Register

CVSS
Common Vulnerability Scoring System

E-CSRR
Enterprise-Level Cybersecurity Risk Register

ERM
Enterprise Risk Management

ERP
Enterprise Risk Profile

ERR
Enterprise Risk Register

FISMA
Federal Information Security Modernization Act

HVA
High Value Asset

ICT
Information and Communications Technology

IR
Interagency Report

ISO
International Organization for Standardization

ISRM
Information Security Risk Management

ISSM
Information System Security Manager

ISSO
Information System Security Officer

ITAM
Information Technology Asset Management

KPI
Key Performance Indicator

KRI
Key Risk Indicator

MEA
Monitor, Evaluate, and Adjust

MFL
Maximum Foreseeable Loss

OMB
Office of Management and Budget

OpRisk
Operational Risk

ORM
Operational Risk Management

OT
Operational Technology

PIA
Privacy Impact Assessment

PML
Probable Maximum Loss

SEC
U.S. Securities and Exchange Commission

SP
Special Publication

Appendix B. Change Log

In July 2025, the following changes were made to the report:

- All — Made minor editorial changes throughout the report to implement the current IR template. Made revisions throughout the report to streamline its content.
- Section 1 — Added a brief summary of IR 8286D.
- Section 2 — Made significant content changes throughout the section that provide additional information on aggregation, normalization, and analysis of cybersecurity risk registers.
- Section 3 — Made significant content changes throughout the section that include material primarily based on OMB Circulars A-11 and A-123.
- Section 4.1 — Revised Figure 8, Table 3, and the related text to reflect the update of the Cybersecurity Framework from version 1.1 to version 2.0.
- Section 4.2.3 — Expanded the discussion of positive risks and opportunities.
- Section 5.5 — Expanded and clarified notional examples in Table 5.
- Section 6 – Added a Conclusion to summarize the report.
- References — Updated references to reflect current versions and URLs. Renumbered references to indicate their current order within the document.