Draft NISTIR 8286C

Staging Cybersecurity Risks for Enterprise Risk Management and Governance Oversight

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

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

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

Draft NISTIR 8286C

Staging Cybersecurity Risks for Enterprise Risk Management and Governance Oversight

Stephen Quinn
Computer Security Division
Information Technology Laboratory

Matthew Barrett
CyberESI Consulting Group, Inc.
Baltimore, MD

Nahla Ivy
Enterprise Risk Management Office
Office of Financial Resource Management

Greg Witte
Huntington Ingalls Industries
Annapolis Junction, MD

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

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

January 2022

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
James K. Olthoff, Performing the Non-Exclusive Functions and Duties of the Under Secretary of Commerce for Standards and Technology & Director, National Institute of Standards and Technology

National Institute of Standards and Technology Interagency or Internal Report 8286C
44 pages (January 2022)

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

Public comment period: January 26, 2022 – March 11, 2022

Submit comments on this publication to: 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

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

Reports on Computer Systems Technology

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

Abstract

This document is the third in a series that supplements NIST Interagency/Internal Report (NISTIR) 8286, *Integrating Cybersecurity and Enterprise Risk Management (ERM)*. This document provides additional detail regarding the enterprise application of cybersecurity risk information. The previous documents, NISTIRs 8286A and 8286B, provided detail regarding stakeholder risk direction and methods for assessing and managing cybersecurity risk in light of enterprise objectives. NISTIR 8286C describes how information, as recorded in cybersecurity risk registers (CSRRs), 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 (ERR) and enterprise risk profile (ERP) that, in turn, support the achievement of enterprise objectives.

Keywords

cybersecurity risk management; cybersecurity risk measurement; cybersecurity risk register (CSRR); enterprise risk management (ERM); key performance indicator (KPI); key risk indicator (KRI); risk acceptance; risk aggregation; risk avoidance; risk conditioning; risk mitigation; risk optimization; risk prioritization; risk response; risk sharing; risk transfer.

Acknowledgments

The authors wish to thank those who have contributed to the creation of this draft. A detailed acknowledgment will be included in the final publication.

Document Conventions

For this document, the terms "cybersecurity" and "information security" are used interchangeably. While information security is generally considered to be all-encompassing – including the cybersecurity domain – the term cybersecurity has expanded in conventional usage to be equivalent to information security. Likewise, the terms Cybersecurity Risk Management (CSRM) and Information Security Risk Management (ISRM) are used interchangeably based on the same reasoning.

Note to Reviewers

The authors are grateful for the feedback and support provided by the community in response to draft publications. In support of the final edition of this report, NIST asks that readers review the following questions and consider these in your feedback and recommendations.

1. Is the use of risk criteria for risk reporting, escalation and elevation, and the normalization of cybersecurity risks at the organizational and enterprise level effectively discussed?
2. Have the differences and distinctions between risk aggregation, deduplication, normalization, optimization, and prioritization been made clear?
3. Is there existing industry guidance that would inform the format and content of Enterprise CSRR and the Enterprise Risk Profile?
4. Are organizational responsibilities for the conveyance of cybersecurity risk information to the enterprise level effectively and clearly described?
5. Does the reputation risk analysis help you see and perhaps respond to different stakeholders' impacts on valuation, volatility, and other enterprise issues?
6. Does NISTIR 8286C provide sufficient information to inform different stakeholder groups' sentiment analysis and reputation consequences?
7. Are common challenges in the translation of cybersecurity risks to enterprise level impacts adequately addressed (e.g., via the CSF mapping)?
8. As NISTIR 8286C completes the description of the CSRM/ERM integration life cycle, what additional related topics would be helpful to readers?
9. Does the draft sufficiently help an entity consider the various roles and responsibilities for integrating CSRM and ERM?
10. Are the key elements of cybersecurity risk evaluation, monitoring, and adjustment represented?
11. Does the publication effectively relate to both private and public sector enterprises in its structure, terminologies, and examples?
12. Throughout the NISTIR 8286 series, has a clear definition and understanding of "positive risk" been presented along with clear and helpful examples?
13. Does the NISTIR 8286 series provide sufficient information to generate a form that would enable effective comparisons between cyber risk and other non-cyber risk consequences and concomitant resource allocations?
14. Does the information outlined in the NISTIR 8286 series provide sufficient information to inform SEC/IRS disclosures regarding financial statements and MDA narratives?
15. Do you think the NISTIR 8286 series provides sufficient information to enable the allocation trade-offs of an organization's operating expenses (OpEx) and capital expenditures (CapEx) for cyber issues and among non-cyber risk issues?

Call for Patent Claims

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

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

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

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

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

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

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

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

Executive Summary

This NIST Interagency/Internal Report (NISTIR) explores the methods for integrating disparate cybersecurity risk management (CSRM) information from throughout the enterprise to create a composite Enterprise Risk Profile (ERP) 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, and reputation exposure. Figure 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]

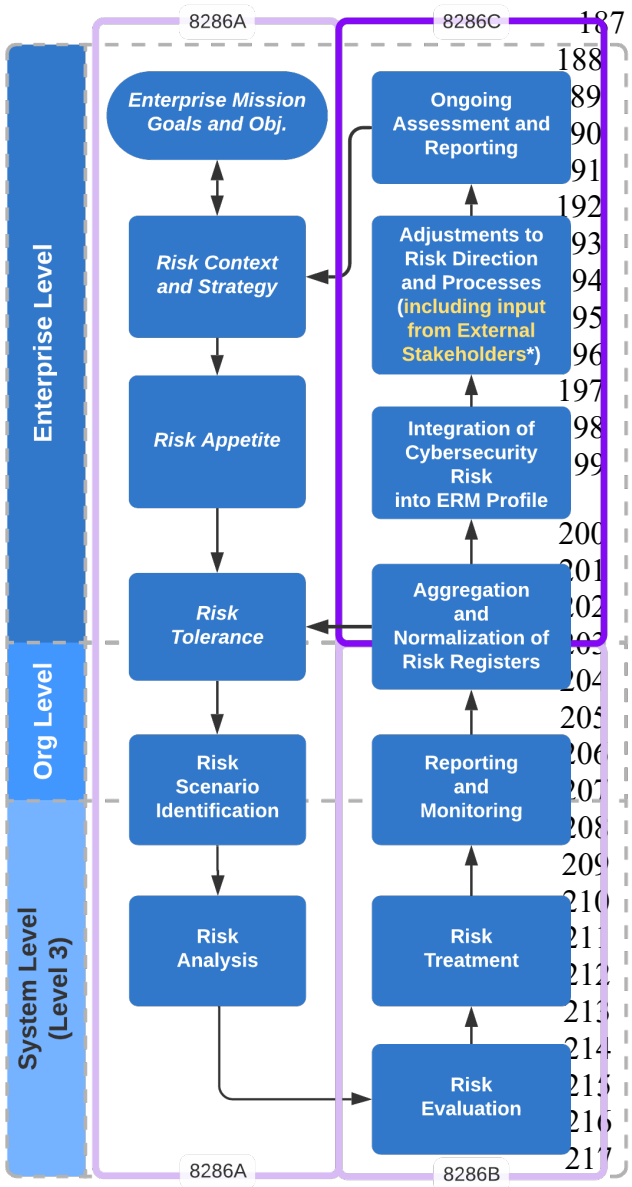

Figure 1: NISTIR 8286 Series Publications Describe C-SCRM/ERM Integration

The importance of information and technology risks to the enterprise risk posture makes it critical to ensure broad visibility into related activities. A comprehensive enterprise risk register (ERR) and enterprise risk profile (ERP) support communication and disclosure requirements. 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 NISTIR explores the methods for integrating disparate cybersecurity risk management (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 NISTIR 8286B 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 the 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.

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

NISTIR 8286C 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) to achieve risk objectives. The report describes how the CSRM Monitor, Evaluate, and Adjust (MEA) process supports enterprise risk management. This process also supports a repeatable and consistent use of terms, including an understanding of how the context of the 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 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. Future points of focus may include information regarding business impact assessments (BIA), which are foundational to understanding exposure and opportunity. Additional reports may explore specific guidance regarding risk limits (i.e., risk appetite, tolerance, and capacity) and further explanation of risk analysis techniques. 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.

NISTIR 8286C continues the discussion regarding the inclusion of CSRM priorities and results in support of improved understanding about the agency and enterprise impacts of cybersecurity risks on financial, reputation, and mission considerations.

239 **Table of Contents**

267

List of Appendices

List of Figures

List of Tables

1 Introduction

This document provides guidance that supplements NIST Interagency or Internal Report (NISTIR) 8286, *Integrating Cybersecurity and Enterprise Risk Management (ERM)* [1]. NISTIR 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, NISTIR 8286, since many of the concepts described in this report are based on the practices and definitions established in that NISTIR. Each publication in the series, as illustrated in Figure 2, provides detailed guidance to supplement topics from NISTIR 8286. Activities in dark blue boxes are described in this report; those in other documents are shown in a lighter shade.

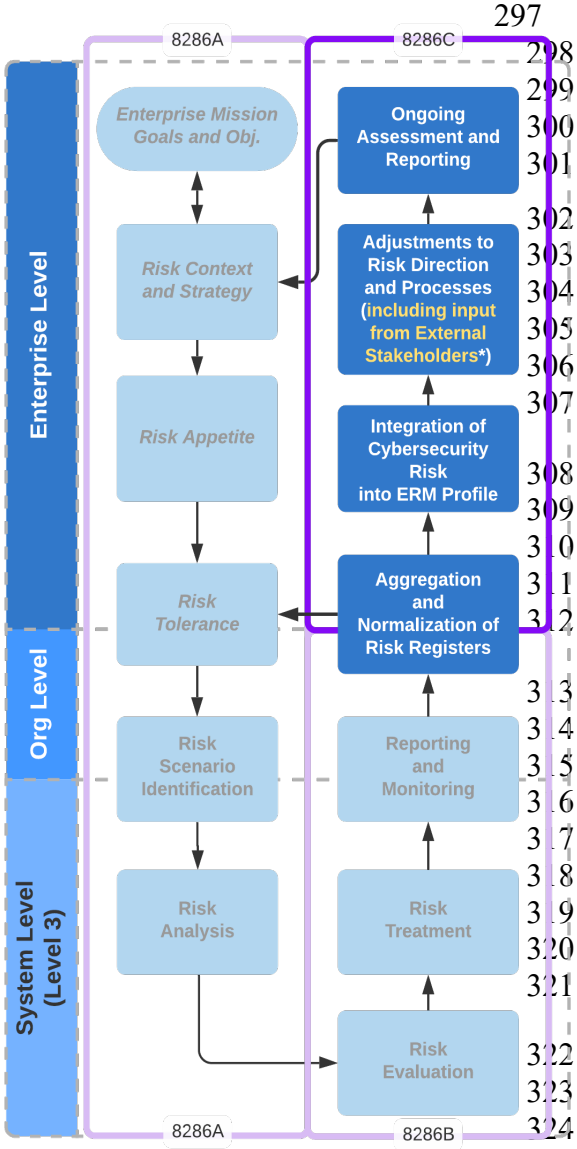

Figure 2: NISTIR 8286C Activities as part of CSRM/ERM Integration

- NISTIR 8286A details the context, scenario identification, and analysis of likelihood and impact of cybersecurity risk. It also includes methods to convey risk information, such as cybersecurity risk registers (CSRRs) and risk detail records.

- NISTIR 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.

- NISTIR 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 any changes to risk strategy, and use the combined information to maintain awareness of risk factors and positive risks (or opportunities).

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 organizational structure (e.g., a federal agency or company). It further defines the *enterprise level* as a unique type of

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

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

NISTIR 8286C brings the elements from preceding documents together 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 the risk practitioners to take appropriate actions and to report those actions in a consistent and timely manner.

The NISTIR 8286 series has focused heavily on the use of risk registers to record and share information within and among hierarchical levels. The authors have worked to make it clear that the goal of risk management is not simply to maintain lists of risks but 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. NISTIR 8286C describes the integration of the various CSRM activities, as recorded in 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 rather 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, NISTIR 8286C describes four key ERM activities:

1. Aggregation 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 ERR and ERP

3. Adjustments to risk direction (including risk limits and risk treatment options) within governance system components to optimize enterprise CSRM results

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 improve subsequent risk assessments. Because cybersecurity risk is only one of the 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. When all of this data is collected and analyzed by those in an enterprise risk governance role, those senior leaders will be able to create or maintain a

comprehensive ERR and ERP, enabling stakeholder communication regarding ERM effectiveness, changes to the entity's risk posture, and the achievement of enterprise ERM strategy.

NISTIR 8286C 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 the 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's 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.
- Section 6 provides a conclusion to the entire NISTIR 8286 series in support of CSRM/ERM integration.
- The References section provides a comprehensive list of all in-text citations used in NISTIR 8286C, as well as links to external sites or publications that offer additional information.
- Appendix A contains a list of the acronyms and abbreviations used in this publication.

2 Aggregation and Normalization of Cybersecurity Risk Registers

The NISTIR 8286 series has presented the value of a consistent cybersecurity risk register (CSRR). The precise contents and format will vary by enterprise but generally follow the structure that has been illustrated throughout the series.

2.1 Aggregation of Cybersecurity Risk Information

The activities described in NISTIRs 8286A and 8286B provide guidance to help complete the CSRR for a given system by 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 NISTIR 8286B contains information about steps for conditioning information in the CSRRs to ease subsequent integration, and that integration represents the next activity in CSRM/ERM coordination.

Aggregation activities are performed using the hierarchical levels described in NISTIR 8286A Figure 3.[3] 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 and normalized. The method for managing the risk ID is left to the practitioner, but note that a source identifier might be needed (e.g., "System A" CSRR risk ID #1 might be tagged as aggregated risk ID A-1) to support the ability to trace a risk back to the original register.

2.2 Normalization of CSRR Information

While aggregation is occurring, the cybersecurity risk manager will normalize the information contained in the various CSRRs. 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. Decisions about what to integrate and how to depend on the use of a common risk rating scheme enable risk assessments to be translated and integrated at higher enterprise levels. At a minimum, the normalization process at the higher level (e.g., for the enterprise CSRR) should use the same rating criteria to enable comparison and tracking. This typically includes definitions for how negative and positive consequences and likelihood are to be measured to allow comparability across 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 as well as internal and external context. The criteria for risk escalation or risk elevation may also be considered as part of the equation for whether specific cybersecurity risks meet the minimum threshold for enterprise-level discussions. For example, the enterprise may note shared risks that represent a broad threat that would benefit from centralized risk mitigation or a reputational risk that demands immediate preventative action.

During normalization, risk managers review the results from the various CSRRs to support consistent risk treatment and communication. Some examples of risk normalization are described

[3] 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.

in Table 1. A key element of normalization 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 the 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 Normalization

De-duplicate and combine identical or similar risks	• An external attacker deploys a remote access tool and exfiltrates the plans for the company's upcoming merger. • 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 appetite, tolerance, and sensibilities	• Since priorities have been established at 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: 1. 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 mitigated the above exfiltration risk and one chose to accept it, then the risk would appear in the combined CSRR twice, with each row indicating the number of times the relevant risk was selected. 2. The combined cybersecurity risk would be included once in the CSRR, with both of the responses included in the risk response type column.
Adjudicate key risks	• Risks that warrant tracking and further communication in the 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 of 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 different risk descriptions for the same scenario. For example, consider the following risks from various lower-level organizations within the enterprise of the same business unit.

The risk manager of that business unit would transliterate the cybersecurity risks into a single representative risk on the business unit's CSRR, perhaps "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 represent varying likelihood and impact. 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, those might provide input into those risk criteria.

It is important to note that the activities described in this report are solely intended to support corporate 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 should not impede the ability of managers to review specific risk decisions.

Aggregating the risk analysis from multiple CSRRs follows the same approach as that described in NISTIR 8286A, Section 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 cases, 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 such that, if they know that a particularly detailed study had been performed to develop one or more of the estimates, that might influence the understanding of the most likely value.

2.3 Integrating CSRR Details

For some enterprises, the aggregation of these risk analysis and risk response values may be more art than science. Some organizations have skilled practitioners with actuarial experience and will be able to 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 NISTIR 8286C are primarily communicative, sharing information after risk response has been implemented. The information provides valuable data that will guide enterprise-level risk decisions, but the level of precision needed at higher hierarchical levels will likely be less than what is needed at the system level.

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 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 continually knowledgeable about relevant risk conditions and have the accountability and authority to manage the risk. Since risk conditions may change as information is aggregated, responsibility and accountability should be periodically reviewed 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) 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 expressed as part of CSRM policy within a given enterprise. Given the roll-up process, CSRM can work in conjunction with enterprise risk managers to include relevant risk policy statements, including requirements for registering risks, regularly providing updates, and communicating risk activities with enterprise managers and leadership.

Through policy statements and these procedures, various cybersecurity risks are integrated into a comprehensive enterprise-level CSRR (or 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 Integration of Cybersecurity Risk into the ERR/ERP

Each of the steps described thus far in the NISTIR 8286 series contributes to an enterprise-wide understanding of strengths and weaknesses about cybersecurity risk. Cyber risk is only one of many risks in the risk universe, but considering the extensive dependency of the modern enterprise on information and technology, cybersecurity represents an important subset of the overall risk picture. For most enterprises, that overall picture is an enterprise risk register (ERR), which reflects the major enterprise-level risks that require sustained management attention. A companion artifact, the enterprise risk profile (ERP), describes a selected and prioritized subset of top risks from the ERR.

U.S. Office of Management and Budget (OMB) Memorandum A-123 requires an ERP for federal entities. It states:

> The primary purpose of a risk profile is to provide a thoughtful analysis of the risks an agency faces toward achieving its strategic objectives and arising from its activities and operations. The risk profile assists in facilitating a determination around the aggregate level and types of risk that the agency and its management are willing to assume to achieve its strategic objectives. [2]

The federal ERM playbook further points out that the risk profile differs from a risk register in that it is a prioritized inventory of the most significant risks identified and assessed through the risk assessment process versus a complete inventory of risks.[4] This statement also supports ERP use by private-sector entities since the profile and the registers that inform it enable evidence and periodic reviews (e.g., year-over-year comparison, previous quarter, trailing 12 months) of stakeholder decisions, disclosures, and budget adjustments.

Figure 3 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 for enterprise objectives – the ERP. While this illustrates the flow of information into the ERP, the reader should remember that this is an 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.

[4] 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.

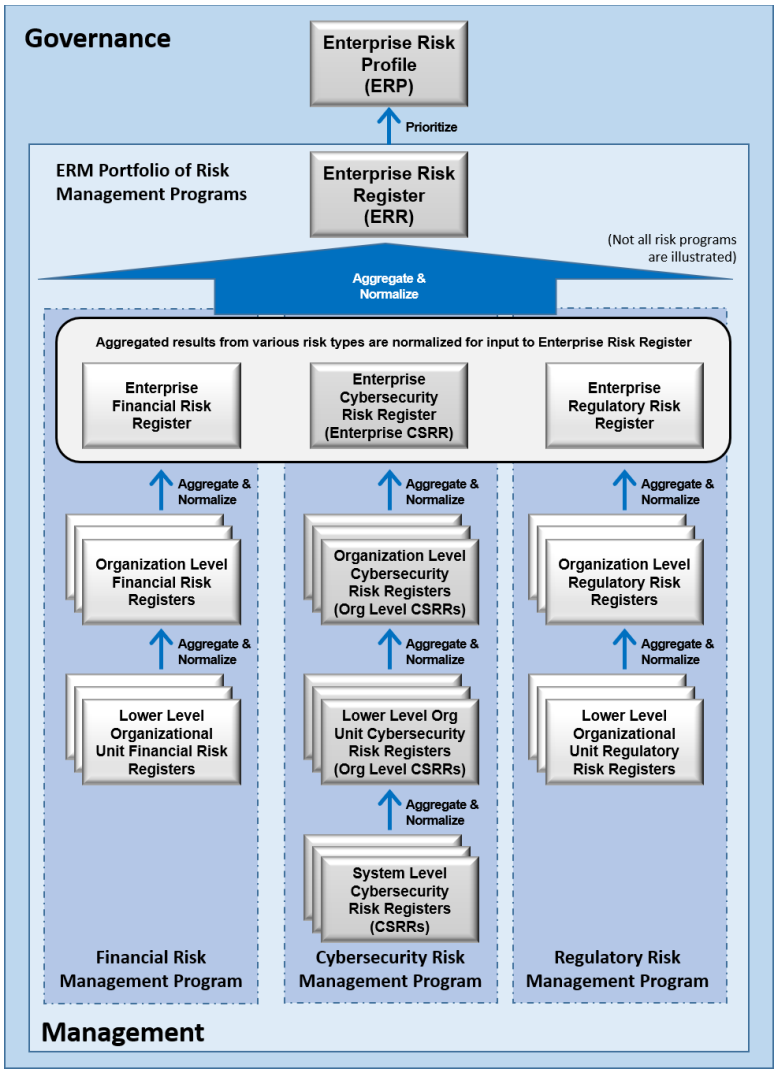

Figure 3: Integration of Risk Registers to Create E-CSRR, ERR, and ERP

3.1 Enterprise Impact of Cybersecurity

Enterprise-level risk managers will consider the primary types of consequences into which risks can be organized to better interpret the enterprise impact of the various cybersecurity risks in the E-CSRR (enterprise-level CSRR) and as a prerequisite for contributing to the ERR. While technology has long been a risk consideration, increasing complexity and reliance on cyber-connected systems introduces new exposures. For example, while technology failures have always represented a risk, highly connected systems and sensors that are part of the Internet of Things (IoT) are affected by latency and duration. Many of the information technology (IT) and operational technology (OT) dependencies (for both criticality and sensitivity) can be recorded in a business impact assessment (BIA). As with other elements of the risk management life cycle, asset valuation drives understanding of exposures (including those with impacts on the balance sheet, revenue, and cash flow). This understanding of exposure enables improved risk assessment, response, and monitoring results throughout the enterprise based on stakeholder governance and direction.

In addition to the E-CSRR, ERM officials use the information about enterprise cybersecurity risks to prioritize the risks in the context of achieving the enterprise objectives – strategic, operations, reporting, and compliance – to develop the ERP. This process can be dynamic, and the four categories are further described in OMB Circular A-123 (2016). In its revised ERM framework, COSO more fully emphasizes the connection among risk, strategy, and performance, and the revised framework's name reflects that change.[5] COSO posits that risks are to be considered both in strategy-setting and implementation (performance against objectives). Comments received to previous publications in the NISTIR 8286 series cautioned against using these integration and communication processes to simply manage lists of risks without considering strategic alignment. For these reasons, there is a need for a dynamic and iterative process of connecting the entity's understanding of cybersecurity risk with its strategy.

Similar to normalization at the E-CSRR level, a common set of risk criteria should be utilized to allow comparability of risks at an ERP level. The ERM function may have established a unique lexicon for enterprise risks that should be considered when communicating risks at Level 1. To ensure the relevance and effective translation of cybersecurity risks at the enterprise level, the chief information security officer or equivalent will need to coordinate with existing ERM functions, which are familiar with stating risks in terms of strategic and business impacts.

Figure 4 illustrates a notional risk breakdown structure that aligns cybersecurity risks with enterprise purposes and impacts.

- **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.
- **Mission:** Risk conditions that affect the enterprise's ability to achieve objectives.
- **Secondary Impacts:** Risk considerations that relate to secondary (or even tertiary) impacts from cascading consequences. For example, a risk that impedes mission objectives may have a subsidiary reputational impact that may subsequently cause financial impact. Negative sentiment

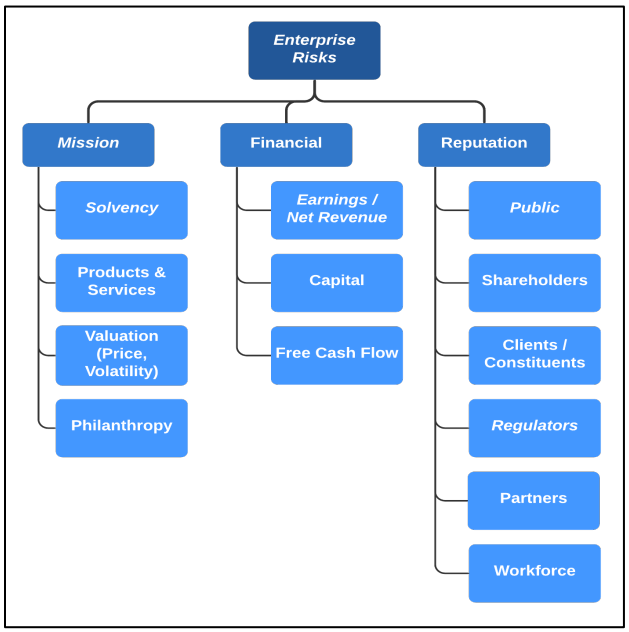

Figure 4: Notional Risk Breakdown Structure Depicting Enterprise Risk Impacts

[5] COSO ERM Framework: *Enterprise Risk Management – Integrating with Strategy and Performance* (2017). The Committee of Sponsoring Organizations of the Treadway Commission (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.

589 from a regulator or legislator may impede funding, authorities, operations, and – ultimately –
590 mission achievement.

591 NIST often references a strategic view at the enterprise level that is supported by business units
592 that implement the strategy and are, in turn, supported by information and systems that enable
593 tactical implementation of the enterprise objectives. For nearly 10 years, NIST has maintained
594 the Cybersecurity Framework, which helps provide an enterprise action plan to develop and
595 refine that understanding, as illustrated by the Information and Decision Flows diagram from that
596 framework (Figure 5). Notably, while the Cybersecurity Framework was created to help
597 providers of critical infrastructure better integrate CSRM into ERM, it was developed and has
598 been implemented in such a way that it is useful for any organization.

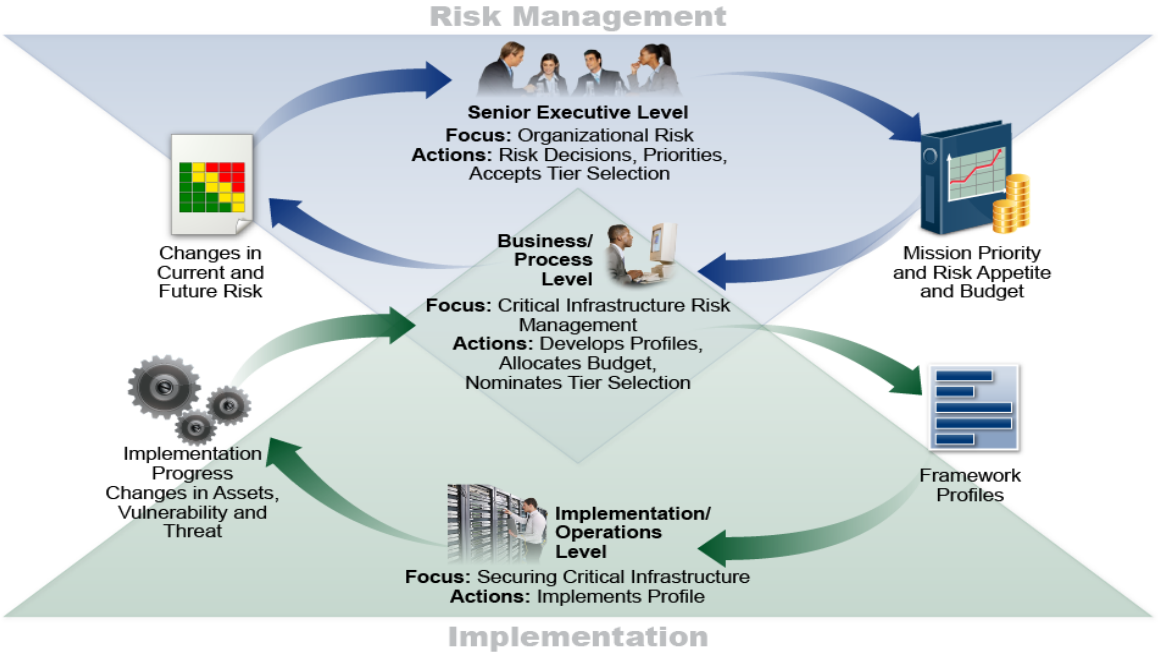

Figure 5: Notional Information and Decision Flows from Cybersecurity Framework

599 This framework process can also help manage the pursuit of opportunities. The NISTIR 8286
600 series has stressed the importance of recording and acting upon positive risk. Each risk
601 aggregation, normalization, and integration activity should identify the impacts of beneficial
602 uncertainty that will accentuate the likelihood of achieving enterprise objectives. Examples
603 might be the recognition that the addition of machine learning technology would significantly
604 increase the throughput of the enterprise research team and could lead to expansion into new
605 marketing areas or that the addition of high-availability services for the enterprise web server
606 will improve availability from 93.4 % to 99.1 % over the next year and improve market share by
607 3 % due to improved customer satisfaction.

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

The ERR informs the ERP once the risks are prioritized at the highest level of the risk management function in the enterprise, as depicted in Figure 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 is provided in Figure 6.

STRATEGIC OBJECTIVE – Improve Program Outcomes							
Risk Description	**Exposure Factors**	**Assessment**			**Current Risk Response**	**Proposed Risk Response**	**Risk Owner**
		Last	**Current**	**Residual**			
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			

Figure 6: Notional Enterprise Risk Profile (ERP) Example

The ERP reflects assessments of mission, financial, and reputation exposures organized according to the four enterprise objectives. They may be full-value exposures or modified (and so noted) by the likelihood assessments of enterprise leaders. At the top enterprise-level, ERM officials have the prerogative to add their 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 and impact estimations and reserves based on a changing risk landscape. ERPs should also reflect comparable occurrence incidents and trends for the subject enterprise and peer organizations.

3.2 Dependencies Among Enterprise Functions and Technology Systems

Various external factors may also influence priority. For example, a new move toward digital transformation may heighten sensitivity toward cybersecurity risks. For federal agencies, recent Executive Orders have established supply chain risk management and secure software development as priority focus areas, so those might become key areas of consideration 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.[6]

As with many processes in risk management, prioritization is likely to be an iterative progression. As the aggregation of CSRM risks improves the understanding and visibility of

[6] Valuation of enterprise assets, including determination of HVAs, is described in section 2.2.1 of NISTIR 8286A.

particular cybersecurity risk types, they 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 are rarely tied directly to a cybersecurity activity but are instead related to a particular set of technical resources. 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. The organization may draw upon the information provided by one or more BIA analyses and possibly companion analyses in the form of privacy impact assessments, or PIAs. At the enterprise hierarchical 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, an understanding of dependencies and impact may be strongly influenced by the potential duration 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 to identifying:

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

For this reason, the BIA is a valuable tool for accurately and efficiently factoring cybersecurity into enterprise risk management. Other aspects of information technology asset management (ITAM) are critical to understanding the enterprise connection among technology and business functions, so many ITAM processes (such as an accurate asset management database) are important for fully interpreting cybersecurity risks.

3.3 Enterprise Value of the ERP

As with other elements of enterprise risk governance, the specific methods and measures used in aggregating 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. The Risk IT Practitioner Guide from the international security association, ISACA, 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 the maximum foreseeable loss (MFL) [3].[7]

[7] Example definitions of PML and FML are available from https://www.investopedia.com/terms/p/probable-maximum-loss-pml.asp and https://www.investopedia.com/terms/m/maximum-foreseeable-loss.asp.

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.[2]

The aggregation of risks at the enterprise level provides a panorama that is not visible at the system or organizational 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 risk evaluation apply to private-sector organizations. These include requirements from the Security and Exchange Commission (SEC) and core principles from the international Basel Committee on Banking Supervision. [8] 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 upon:

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

3.4 Typical Enterprise Objectives, Functions, and Prioritization

As mentioned in Section 3.1, ERR and ERP contents are frequently organized in terms of four discrete enterprise objectives – strategic, operations, reporting, and compliance – and are often used as guideposts for enterprise risk reporting. Clear direction from senior leaders about how to align various types of cybersecurity risk with strategic objectives will help enable subsequent

[8] 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. https://www.ecfr.gov/current/title-17/chapter-II/part-229

aggregation, normalization, and prioritization. Effectively capturing and reporting on the risks that are relevant to the execution of that strategy will also help monitor this alignment.

For example, OMB A-123 Section B1 recommends the following objectives for federal agencies to organize various risk categories and types. Tying CSRM risks to these objectives will help align and normalize results.

- **Strategic:** Risks impacting the core mission or objectives of the enterprise, including those related to the implementation of a new service or product offering; cybersecurity concerns that might impact an upcoming federal agency reorganization or a private-sector acquisition
- **Operations:** Cybersecurity risks regarding existing operational systems, such as a ransomware attack that disables a manufacturing line; business continuity/disaster recovery issues
- **Reporting:** Cybersecurity risks regarding the availability, integrity, and confidentiality of financial or information management systems, including those that might impact the accuracy or timeliness of reporting functions
- **Compliance:** Cybersecurity risks where a negative event might result in a failure to meet a contractual service agreement or in a regulatory penalty or fine

These are simply suggested categories and can be changed or supplemented.[9] For example, some organizations move technical risk types to their own category while others include them among those listed above. Some entities will define categories unique to their lines of business or type of activity.

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

[9] For federal agencies, OMB Circular A-123 states, "Risk must be analyzed in relation to achievement of the strategic objectives established in the Agency strategic plan (see OMB Circular No. A-11, Section 230), as well as risk in relation to appropriate operational objectives. Specific objectives must be identified and documented to facilitate identification of risks to strategic, operations, reporting, and compliance." [2]

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, 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. Governing and managing technology risks are numerous, but some common processes support consistent implementation. While this section reviews many of the topics covered in NISTIR 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 has highlighted the distinction between governance and management. Risk governance is not intended to take the place of risk management activities; 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 (e.g., division, portfolio, or bureau level), 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 Council	Senior Accountable Official for Risk Management, Chief Risk Officer, Senior Agency Information Security Officer, Senior Agency Official for Privacy, Risk Executive (Function), such as the Enterprise Risk Management Council	Provides oversight, direction, and priorities for the enterprise risk management function. Identifies those risks that may require external reporting or disclosure to the public, stakeholders, or regulators.

Risk Functions	Notional Private-Sector Roles	Notional Federal Government Roles	Notional Responsibilities
Enterprise Level Risk Management	Chief Operating Officer, Chief Financial Officer or Controller,[10] Chief Risk Officer	Chief Operating Officer, Chief Financial Officer,[11] Chief Risk Officer, Enterprise Risk Management Officer	Leads and implements the enterprise risk management program. Ensures frequent visibility for high priority risks affecting 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 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 sub-organization staff are aware of policies, procedures, and risk parameters (e.g. risk appetite and tolerance) to effectively balance risk with mission performance.

[10] 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.

Risk Functions	Notional Private-Sector Roles	Notional Federal Government Roles	Notional Responsibilities
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 and that risk response decisions are communicated back to the Risk Owner. Periodically reports the status to the CISO.

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 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). This enterprise-wide approach is consistent with previous illustrations in the NISTIR 8286 series. Figure 7 demonstrates how strategic oversight and direction at the enterprise level support organization-specific decisions, which in turn support system-level risk management and reporting. The NIST Cybersecurity Framework helps support a hierarchical approach to coordinating risk management activities across multiple levels, including the activities described in NISTIR 8286C. To illustrate this connection, each of the methods described in Figure 7 is depicted with a relevant subcategory from one or more NIST Cybersecurity Framework steps. The correlation of activities is further detailed in Table 3.

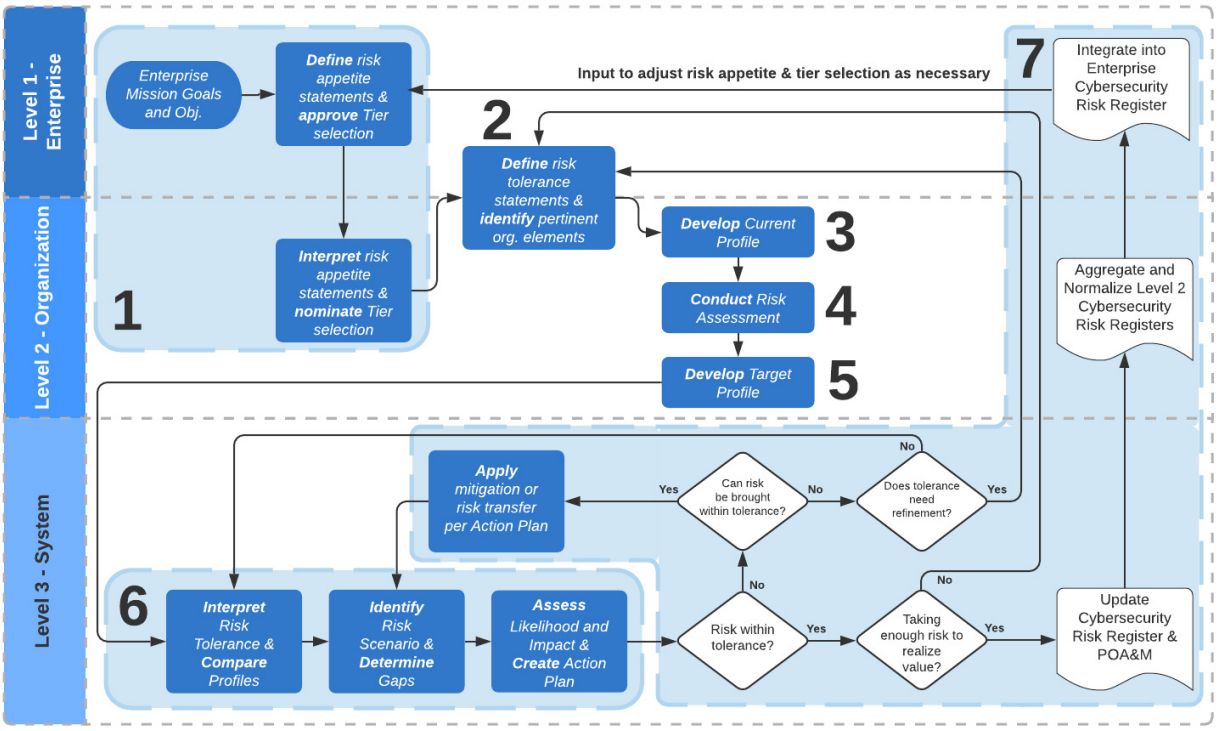

Figure 7: Cybersecurity Framework Steps in Support of CSRM Integration

Figure 7 shows the overlay of NISTIR 8286A, Figure 6, *Continuous Interaction Between ERM and CSRM Using the Risk Register*, and the implementation steps described in Section 3.2 of the Cybersecurity Framework. This process demonstrates the application of some of the topics addressed in previous NISTIRs to maintain a comprehensive CSRM program. Specific activities for integrating CSF into CSRM/ERM integration are described in Table 3. [12]

Table 3: Cybersecurity Framework Steps as Aligned with CSRM/ERM Integration

Cybersecurity Framework Step / Activity	CSRM / ERM Integration Activity
Step 1: Prioritize and Scope.	The organization identifies its business/mission objectives and high-level organizational 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. Stakeholders review the characteristics of the four framework implementation tiers and recommend the tier that best aligns with enterprise strategy. Senior leaders may review and approve (or adjust) the tier recommendation.

[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 / Activity	CSRM / ERM Integration Activity
Step 2: Orient.	To account for varying types of hierarchical levels, risk tolerance may be interpreted at either Level 2 or Level 3 to account for variance in business lines or processes. An additional consideration is given to organizational priorities, internal/external context, and risk criteria established for risk assessments at the various levels of the enterprise. Cybersecurity risk managers will determine the relevant assets to be protected and their relative importance (see NISTIR 8286A, Section 2.2.1). A high-level determination of general threats, vulnerabilities, and their impacts is performed. These will be used in Step 4 to consider the risk implications of the current state profile outcomes. (See NISTIR 8286A, Sections 2.2.2 through 2.2.4). Results from previous aggregation and integration activities (as described in Sections 2 and 3 of this report) may help inform the list of potential threats, vulnerabilities, and impacts.
Step 3: Create a Current Profile.	Iterating through the relevant CSF functions, categories, and subcategories in the CSF Core, designees document the current processes and activities that contribute to the achievement of 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 Sections 2 and 3 of this report) may help to populate both positive and negative aspects of the current profile.
Step 4: Conduct a Risk Assessment.	Having documented the "as-is" for each Core outcome, one or more enterprise personnel consider the risk implications, if any, of the processes and activities described in the current profile. Unlike the high-level determination of threats and vulnerabilities in Step 2 and system-specific control assessment that may occur in Step 6, this review is focused on the current state. Step 4 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 NISTIR 8286A, Section 2.3) and risk exposure ratings (see NISTIR 8286A, Section 2.4).
Step 5: Create a Target Profile.	Informed by an understanding of the risk implications defined in Step 4, risk practitioners determine the desired set of processes and activities that will accomplish stakeholder expectations cost-effectively and efficiently. These outcomes are not intended to eliminate all risk but rather to reduce exposure to an acceptable level based on risk appetite, risk tolerance, and previously approved and implemented risk management actions. 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. The target profile also offers an opportunity to describe the implementation of the characteristics described in the target framework implementation tier. The variance between current and desired outcomes as they relate to enterprise risk management processes, integration, external participation, and cyber supply chain are included in the "to-be" description.

Cybersecurity Framework Step / Activity	CSRM / ERM Integration Activity
Step 6: Determine, Analyze, and Prioritize Gaps.	Using the risk determinations from Step 4, in light of risk tolerance statements, risk practitioners at Level 3 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 implementation improvement. The determination of gaps will help to identify system-specific scenarios (as described in NISTIR 8286A, Section 2.2) and analyze their likelihood and impact (see NISTIR 8286A Section 2.3). This determination drives the selection of necessary actions to acceptably respond to risk and prioritize based on stakeholder direction (see NISTIR 8286B, Sections 2.2 and 2.3).
Step 7: Implement Action Plan.	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 which have been approved by a cognizant official to be treated at a future time (or based upon some future condition) might also be documented in a Plan of Actions and Milestones register.
Iteration	As CSRRs from throughout the enterprise are reviewed, aggregated, and integrated, data points from these registers provide input into subsequent iterations of the cycle. Continuous monitoring and learning allow for input to the cybersecurity risk strategy, enabling adjustments to that strategy to pursue opportunities and reduce exposure throughout the enterprise. Stakeholders may also adjust the desired framework implementation tier and apply the same process to adjust risk management, risk criteria, information sharing, and supply chain management activities to achieve that goal.

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 Figure 7 illustrate six points where risk decisions drive activity to adjust risk response, risk constraints, or both. Adjustments provide both inputs to and feedback from the dynamic enterprise CSRM life cycle (Figure 8) as a critical component of a healthy risk management ecosystem. Monitoring performance and risk indicators provides data points that can be used along with other enterprise performance information to identify whether adjustments to risk direction are necessary. The high-level approach described below, informed by detailed considerations as shown in previous illustrations, provides input into ongoing assessment and reporting of the enterprise cybersecurity risk conditions. Because the enterprise objectives, risk landscape, and stakeholder needs are continually evolving, this ongoing life cycle includes dynamic adjustments.

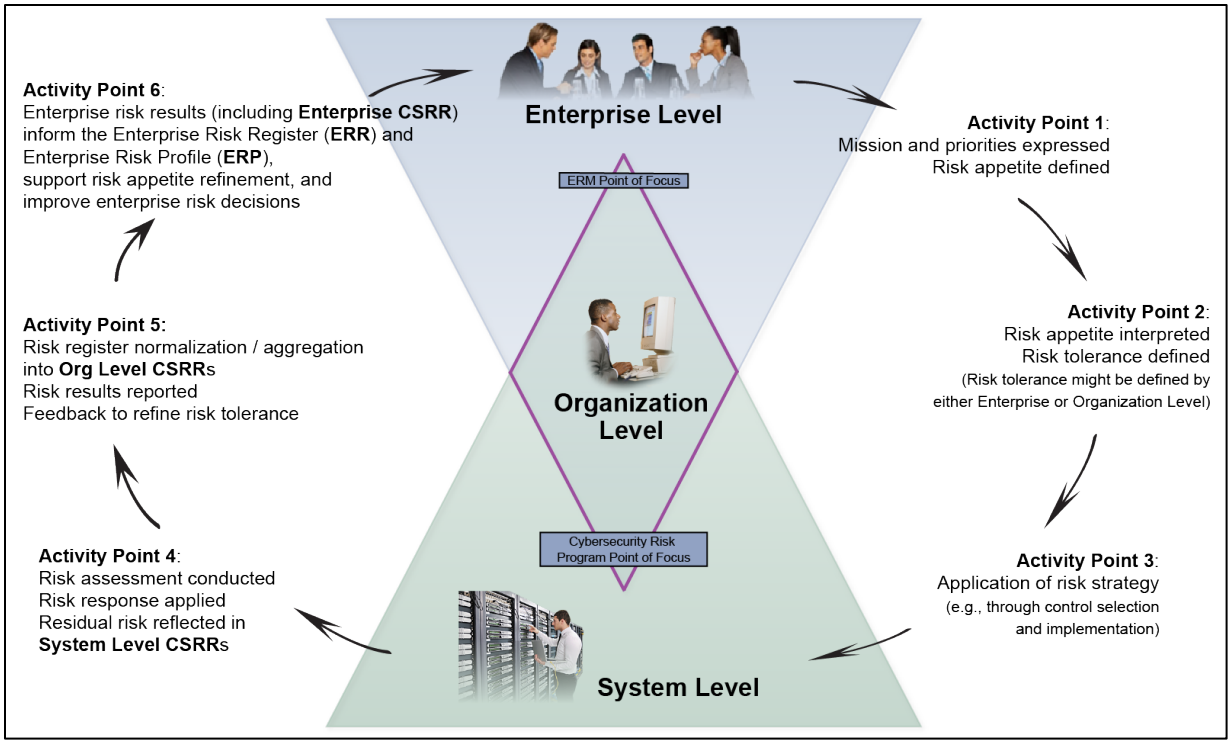

Figure 8: Illustration of Enterprise CSRM and Coordination

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 direction 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 to 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 between risk optimization, resource optimization, and the value delivered by the technology being protected. If any of these three factors result in an imbalance, the solution is untenable. For this reason, CSRM informs the decisions around what areas receive priority within limited budget environments.

The factors that have been discussed thus far in the NISTIR 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 of investment in cybersecurity protection, detection, and response resources. In reality, 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 publication series. Quantitative methods provide specific calculations that enable the risk practitioner to simulate

risk likelihood and financial impact before and after implementation of the cybersecurity improvement. This, then, drives a straightforward cost-benefit analysis regarding the resource investment.

Another budgetary consideration results from the aggregation activities described in Section 2. As managers and leaders review the activities performed and the risk results provided, they may identify opportunities to centrally fund and operate risk management activities that had previously been the responsibility of individual system owners. It may, therefore, make fiscal sense to combine particular activities to gain efficiencies or to reduce duplication. As such opportunities become apparent during the review of CSRR reports and results, leaders can 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 regarding leaders' risk criteria regarding risk appetite and tolerance. Figure 8 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 NISTIR 8286B, Section 2.3), either through risk sharing or through 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. In either case, discussion with decision-makers is necessary to determine the appropriate course of action. That discussion might also support guidance for other enterprise systems that face similar risk scenarios.
- Additional decision points occur after aggregation and integration of CSRRs at various levels. As risk managers review the risk registers (and detailed 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 activity. 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

risk direction or criteria need to be adjusted? If so, this provides an opportunity to repeat the cycle illustrated in Figure 7.

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 Section 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 (e.g., opportunities, rewards). These introspective questions help those in risk governance roles identify whether their risk managers are using the risk governance tools and process correctly or if the risk governance tools and process need adjustment.

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. All cybersecurity risk decisions flow from the enterprise mission and priorities. This is illustrated by Activity Point 1 in Figure 8 where senior leaders establish 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 NISTIR 8286B, Section 2.2, the order in which risks are addressed, direction regarding appropriate response, and even agreement about which risks will be addressed all derive from the enterprise priorities. For this reason, a key enterprise activity will be a periodic review of those priorities and the effects they have on CSRM. Based on the results of such reviews, priorities might be adjusted or clarified to ensure continued alignment between CSRM activity and mission objectives.

5 Cybersecurity Risk Monitoring, Evaluation, and Adjustment

Risk management should not simply be 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. Based on those activities, senior leaders evaluate available options and adjust guidance and operations to help realize opportunities and minimize harmful impact.

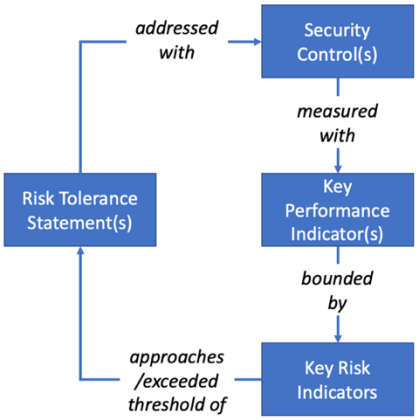

Figure 9: Monitor-Evaluate-Adjust Cycle

This iterative approach begins where NISTIR 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 in order to achieve strategic objectives. To do so, leaders apply a monitor-evaluate-adjust cycle, as illustrated in Figure 9. Risk tolerance that is 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 key performance indicators (KPIs), especially those metrics that represent key risk indicators (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, which is 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 the risk management processes permitted those enterprises to approach or exceed risk capacity. Such cases can end the career 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 bring the enterprise's continued existence into question. 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" [4]. 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 in NISTIR 8286C and is an important consideration for those aggregating CSRM and evaluating the overall risk posture.

5.1 Key CSRM Mechanisms

Risk tolerance statements are translated into the inter-related triad of security controls, KPIs, and KRIs to monitor, evaluate, and adjust risk. 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. With 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

Figure 3 illustrates that risk communication at each level is based on the risk management activities feeding into it. For example, reporting and communication about cybersecurity risks at Level 2 are informed by the results from Level 3. 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. For example, a risk practitioner who observes changes in a KRI might look to determine whether the:

- Likelihood of an identified risk is increasing,
- Severity of the consequences is increasing, 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:

- Each of the risks in a particular category is grouped together.
- Similar risks within each category are normalized. A specific taxonomy can be applied, or the practitioner(s) 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 is 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 it could be that the total exposure is simply summed, resulting in a composite exposure value.

Since much of the aggregation and integration will have already been applied, the Enterprise 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 will be 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:

- The creation of a working group to identify root causes and recommended next steps
- The assignment of a group of risk types to a centralized risk owner to reduce variance and ensure accountability
- Determination of 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 the 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.

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, 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, then the offsetting risk analysis might need to be adjusted. If positive conditions have decreased, then additional scrutiny might be necessary for the cost side of a cost-benefit analysis.

Figure 9 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) are achieving their objectives, the evaluation described here fulfills a broader need. Observations during the MEA process are intended to inform whether adjustments to strategy, policy, or general practices are needed. 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 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 success, shortcomings, and results. Table 4 (drawn from NISTIR 8286) shows some evaluation opportunities that can help identify whether the program is on track or if it needs adjustment.

Table 4: Examples of Proactive Risk Management Evaluation 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.

A comprehensive risk evaluation process at all hierarchical levels, particularly at the enterprise level, enables effective and efficient detection of positive risk trends that can be exploited or 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 may be necessary to risk direction, risk treatment, or both.

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 might update risk appetite statements to increase or decrease risk limits, potentially including 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 from harmful risks.

- **Adjusting Risk Responses –** To address inconsistent responses to risks or to achieve a different result, leaders might choose to direct specific response actions to one or more risk scenarios. For example, if some organizations decided to mitigate a given risk type and others chose to accept it, risk managers might clarify which treatment is the appropriate response or clarify the criteria by which that decision is made. As with previous discussions, this adjustment might either be to reduce the overall exposure by enacting a more stringent response, or it might 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 might adjust a 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, then different (or additional) metrics might 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 observations resulting from monitoring and evaluating risk results. Additional adjustments might 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, or FISMA).

3.5 Monitor, Evaluate, Adjust Examples

Table 5 provides several examples of related risk appetite, risk tolerance, controls, KPIs, and KRIs. Some example risk appetite and tolerance statements (indicated in *italics*) are drawn from Table 1 in Section 2.1.1. of NISTIR 8286A.

Table 5: Notional Example 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 first 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 (severity score of 10) within 14 days of discovery.*	*We will issue unique user accounts, and our computer systems will audit both positive and negative log-on events.*	*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 method(s) • Audit logs	• Power generator • AC unit • Upstream network provider • Web load balancers

		• Audit log alerting/evaluation	• Web servers
KPI	Percentage of vulnerabilities patched	Unsuccessful logins in a 1-hour period	Outage time in hours
Leading KRI	Number of computers with critical (CVSS 10) vulnerabilities that have not been patched in 10 days	• 4 failed logins for a single user • 29 failed logins across all users	• Outages affecting more than 5 % of customers that have lasted 1.5 hours • Outages lasting over 2 hours that affect fewer than 5 % of customers
Lagging KRI	Number of computers with CVSS 10 vulnerabilities that have not been patched in 15 days	• 5 failed logins for a single user • 30 failed logins across all users	Current outages affecting more than 5 % of customers that have lasted more than 2 hours

1082

6 Conclusion

The NISTIR 8286 series enables risk practitioners to more fully integrate CSRM activities into the broader enterprise risk processes. Because information and technology comprise some of the enterprise's most valuable resources, it is vital that directors and senior leaders have a clear understanding of cybersecurity risk posture at all times. It is similarly vital that those identifying, assessing, and treating cybersecurity risk understand enterprise strategic objectives when making risk decisions.

The series is intended to introduce this integration, and extensive additional research and collaboration are necessary. Future points of focus may include information regarding business impact analysis (BIA), specific guidance regarding risk limits (i.e., risk appetite, tolerance, and capacity), and further explanation of risk analysis techniques. NIST also continues to perform extensive research and publication development regarding metrics – a topic that will support ERM/CSRM performance measurement, monitoring, and communication.

The authors of the NISTIR 8286 series hope that these publications will spark further industry discussion. As NIST continues to develop frameworks and guidance to further support the application and integration of information and technology, many of the series' concepts will be considered for inclusion.

It is important that risk practitioners within each enterprise conduct conversations to better understand the alignment of cybersecurity risks as part of the overarching enterprise risk universe. Historically, technology risks have not been a focus at the executive level. Given the increasing reliance of society on interconnected communications and technology, that trend is reversing and provides the opportunity for increased awareness and coordination. That coordination may include communication tools, such as the risk registers that have been described within these publications.

Technology is a key element of enterprise objectives, and those who manage cybersecurity risks have an important role in ensuring their enterprise's success. By identifying and maximizing opportunities while ensuring that harmful impact is maintained within acceptable limits, public- and private-sector entities can realize great value.

1111 # References

[1] Stine K, Quinn S, Witte G, Gardner RK (2020) Integrating Cybersecurity and Enterprise Risk Management (ERM). (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8286. https://doi.org/10.6028/NIST.IR.8286

[2] Office of Management and Budget (2016) Managing Information as a Strategic Resource. (The White House, Washington, DC), OMB Circular No. A-130, July 28, 2016. Available at https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/circulars/A130/a130revised.pdf

[3] ISACA (2020) *Risk IT Framework* (ISACA, Schaumburg, IL), 2nd Ed.

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

1112

Appendix A—Acronyms and Abbreviations

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

BIA	Business Impact Assessment
CEO	Chief Executive Officer
CISO	Chief Information Security Officer
COSO	Committee of Sponsoring Organizations of the Treadway Commission
CSF	NIST Cybersecurity Framework
CSRM	Cybersecurity risk management
CSRR	Cybersecurity risk register
ERP	Enterprise Risk Profile
ERR	Enterprise risk register
FOIA	Freedom of Information Act
HVA	High value assets
IRS	Internal Revenue Service
ISRM	Information Security Risk Management
ISSM	Information System Security Manager
IT	Information technology
ITAM	Information Technology Asset Management
ITL	Information Technology Laboratory
KPI	Key performance indicator
KRI	Key risk indicator
MEA	Monitor, Evaluate, and Adjust
MFL	Maximum foreseeable loss
NIST	National Institute of Standards and Technology
NISTIR	NIST Interagency/Internal Report
OMB	Office of Management and Budget
OT	Operational technology
PML	Probable maximum loss
RDR	Risk detail records
RMC	Risk management council or committee
SEC	U.S. Securities and Exchange Commission