Draft NISTIR 8286B

Prioritizing Cybersecurity Risk for Enterprise Risk Management

Kevin Stine
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.8286B-draft

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

Draft NISTIR 8286B

Prioritizing Cybersecurity Risk for Enterprise Risk Management

Kevin Stine
Applied Cybersecurity Division
Information Technology Laboratory

Matthew Barrett
CyberESI Consulting Group, Inc.
Baltimore, MD

Stephen Quinn
Computer Security Division
Information Technology Laboratory

Greg Witte
Huntington Ingalls Industries
Annapolis Junction, MD

Nahla Ivy
Enterprise Risk Management Office
Office of Financial Resource Management

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

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

September 2021

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 8286B
42 pages (September 2021)

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

Public comment period: September 1, 2021 through October 15, 2021

National Institute of Standards and Technology
Attn: Applied Cybersecurity Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 2000) Gaithersburg, MD 20899-2000
Email: nistir8286@nist.gov

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

Reports on Computer Systems Technology

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

Abstract

This document is the second in a series that supplements NIST Interagency/Internal Report (NISTIR) 8286, *Integrating Cybersecurity and Enterprise Risk Management (ERM)*. This series provides additional detail regarding the enterprise application of cybersecurity risk information; the previous document, NISTIR 8286A, provided detail regarding stakeholder risk guidance and risk identification and analysis. This second publication describes the need for determining the priorities of each of those risks in light of their potential impact on enterprise objectives, as well as options for properly treating that risk. This report describes how risk priorities and risk response information are added to the cybersecurity risk register (CSRR) in support of an overall enterprise risk register. Information about the selection of and projected cost of risk response will be used to maintain a composite view of cybersecurity risks throughout the enterprise, which may be used to confirm and, if necessary, adjust risk strategy to ensure mission success.

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 acknowledgement will be included in the final publication.

Document Conventions

For the purposes of 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.

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

All organizations face a broad array of risks, including cybersecurity risk. For U.S. Federal Government agencies, the Office of Management and Budget (OMB) Circular A-11 defines risk as "the effect of uncertainty on objectives" [1]. An organization's mission and business objectives can be impacted by such effects and must be managed at various hierarchical levels.

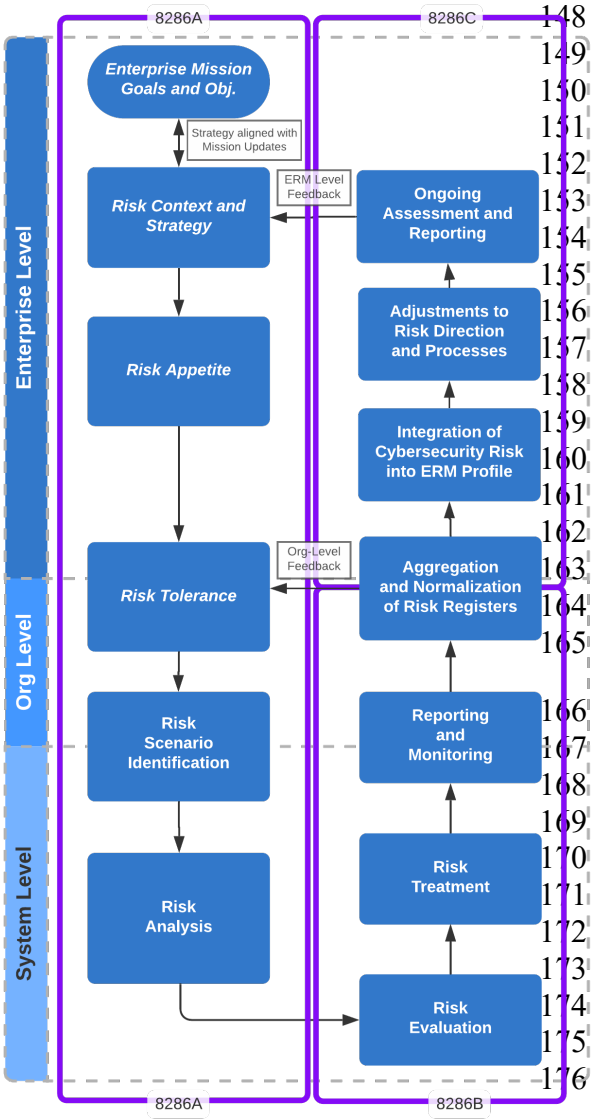


Figure 1: NISTIR 8286 Series Publications Describe Detailed CSRM/ERM Integration

This report highlights CSRM aspects that are inherent to enterprises, organizations, and systems. The terms *organization* and *enterprise* are often used interchangeably; for the purposes of this document, both an *organization* and an *enterprise* are defined as an entity of any size, complexity, or positioning within a larger organizational structure. The term *enterprise level* refers to the top level of the hierarchy where senior leaders have unique risk governance responsibilities. Each enterprise, such as a corporation or government agency, is comprised of *organizations* supported by *systems*.[1] The term *organizational level* refers to the various middle levels of the hierarchy between the *system level* (lowest level) and the enterprise level (highest level).

Enterprise risk management (ERM) calls for understanding the key risks an organization faces. This document provides supplemental guidance for aligning cybersecurity risks within an organization's overall ERM program. Lessons learned from historical cybersecurity incidents demonstrate the importance of collaboration between CSRM and ERM. This document helps enterprises apply, improve, and monitor the quality of that cooperation and communication.

This NIST Interagency/Internal Report (NISTIR) is the second part of a series of publications supporting NISTIR 8286, *Integrating Cybersecurity and Enterprise Risk Management (ERM)* [2].

[1] A system is defined as "a discrete set of information resources organized expressly for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information."

Figure 1 illustrates that additional detail and guidance are provided in each report:

- NISTIR 8286A provides detail regarding cybersecurity risk context, scenarios, and analysis of likelihood and impact. It includes methods to convey risk information, such as cybersecurity risk registers (CSRRs) and risk detail records (RDRs).

- NISTIR 8286B (this report) describes ways to apply risk analysis to help prioritize cybersecurity risk, evaluate and select appropriate risk response, and communicate risk activities as part of an enterprise CSRM strategy.

- The next document in this series, NISTIR 8286C, describes processes for aggregating information from CSRM activities throughout the enterprise. As that information is integrated and harmonized, organizational and enterprise leaders monitor 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).

All participants in the enterprise should use consistent methods to prioritize and respond to risk, including methods for communicating results. This report provides guidance for applying a consistent risk strategy at all enterprise levels. Based on the risk identification and risk analysis described in NISTIR 8286A, this NISTIR 8286B document describes the prioritization of specific risk scenarios and integration touch points with the central level(s) of the organization (see Section 2.1) based upon business objectives and the enterprise's mission. Section 2.2 describes methods for evaluating the potential response to those risks in light of enterprise risk direction, including the consideration of cost factors. Section 2.3 provides guidance regarding the use of risk categories and other criteria to support the aggregation of cybersecurity risk. Intentional conditioning (i.e., normalization of metrics, use of categories, consistent use of terms) enables risk aggregation and supports enterprise communication of risk trends, common issues, and performance results. That information is then used to monitor, evaluate, and adjust risk strategy, as described in NISTIR 8286C.

207 **Table of Contents**

List of Appendices

List of Figures

List of Tables

1 Introduction

This document provides guidance that supplements NISTIR 8286, *Integrating Cybersecurity and Enterprise Risk Management (ERM)* [2]. This is the second of 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 upon practices and definitions established in that NISTIR.

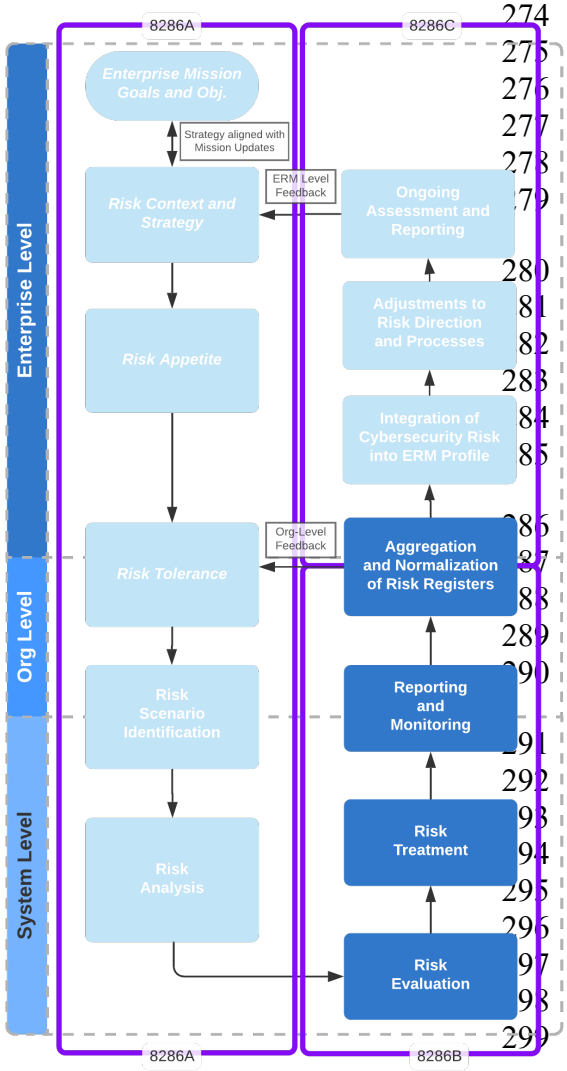


Figure 2: NISTIR 8286B Activities as part of CSRM/ERM Integration

Each publication in the series, as illustrated in Figure 2, provides detailed guidance to supplement topics from NISTIR 8286. Activities shown in dark blue are described in this report; those in other documents are shown in a lighter shade.

- 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 (this report) 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 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).

A key point established by NISTIR 8286 is that the terms *organization* and *enterprise* are often used interchangeably. That 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 defines the *enterprise level* as a unique type of organization, one in which individual senior leaders govern at the highest point in the hierarchy and have unique risk management responsibilities, such as fiduciary reporting and

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

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.

As shown in Figure 2, NISTIR 8286B draws upon the risk identification and analysis described in NISTIR 8286A, *Identifying and Estimating Cybersecurity Risk for Enterprise Risk Management*, and focuses on steps for evaluating, selecting, implementing, and recording risk response. The sections below describe the need to treat cybersecurity risk in alignment with enterprise risk strategy and applying and maintaining risk response in ways to achieve risk direction that have been conveyed through risk appetite and risk tolerance statements. The publication also follows the convention from NISTIRs 8286 and 8286A of using a CSRR to record and communicate risk information. NISTIR 8286A offers recommendations for completing five of the CSRR columns, and Section 3 of this publication will illustrate how to complete the remaining six columns that relate to risk prioritization and response. The reader will also benefit from the use of the risk detail record (RDR), described in Appendix B of NISTIR 8286A, for communicating extended risk description, analysis, and response details.

1.1 Purpose and Scope

This document focuses on improving understanding and communications between and among CSRM and ERM managers, high-level executives, and corporate officers to help ensure the effective integration of cybersecurity considerations as a critical subset of the overarching enterprise risks. The risk management community has observed an opportunity for increased rigor in the way cybersecurity risk identification, analysis, and reporting are performed at all levels of the enterprise. This publication is designed to provide guidance and to further conversations regarding ways to improve CSRM and the coordination of CSRM with ERM.

The goals of this document are to:

- Describe how enterprise risk strategy and other governance processes (e.g., organizational oversight, risk governance, risk management) help to establish the relative priority of scenarios in the CSRR,
- Present various enterprise risk factors that influence risk priorities, and
- Aid in preparing risk response details and results in preparation for feedback to refine and adjust risk direction.

This document continues the discussion to bridge existing private industry risk management processes with government-mandated federal agency enterprise and cybersecurity risk requirements derived from OMB Circulars A-123 and A-130 [3][4]. It builds upon concepts introduced in NISTIR 8286 and complements other documents in this series. It also references some materials that are specifically intended for use by federal agencies and will be highlighted as such, but the concepts and approaches are intended to be useful to all enterprises.

1.2 Supporting the Risk Management Cycle

NISTIR 8286A describes how to coordinate CSRM and ERM through the use of risk registers and risk detail reports (RDRs) and expands on topics that were introduced in NISTIR 8286, *Integrating Cybersecurity and Enterprise Risk Management*. Such lists of risks are critical for organizing and communicating risk information throughout the enterprise, but unless that communication is paired with effective risk analysis, evaluation, response, and monitoring, those lists are of little value. NISTIR 8286A focuses on ways to identify cybersecurity risk scenarios and to analyze the likelihood that those risks would have a harmful impact on the enterprise mission. NISTIR 8286B continues that discussion by detailing processes for responding to those risks and further completing and communicating the risk registers and RDRs as informed by enterprise drivers.

In support of effective risk decisions, NISTIR 8286B focuses on the risk evaluation process and on ways to select, report and monitor risk response. This publication helps the reader populate the priority, risk response, risk owner, and status fields columns of the CSRR (see Figure 10 in Section 2).

Results of the activities described in NISTIR 8286B support the communication of risk response and reporting as feedback for senior leaders' risk direction. Details of that communication are described in NISTIR 8286C. As organization-level and system-level risk managers respond to risks in accordance with enterprise strategy and guidance, the results of that response (both individually and in aggregate) inform senior leaders about the efficacy of their direction. Based on the results, leaders may then adjust risk responses to ensure ongoing support for enterprise mission objectives.

1.3 Supporting the Enterprise Cybersecurity Risk Life Cycle

The activities in Section 2 of this publication draw upon those in NISTIR 8286A that focus on the first half of the CSRM process. The CSRR is used to record and communicate various cybersecurity risk considerations that support the ERM process. Guidance throughout this series references stakeholders at various levels, with senior leaders defining ERM scope, context, and strategy at enterprise levels and others providing management and implementation throughout that enterprise. Senior leaders also establish a *risk appetite* that sets the tone and, where possible, a quantified range for how risk – including cybersecurity risk – will be handled within the enterprise. The risk appetite is interpreted at enterprise and organizational levels and, in turn, helps to define the *risk tolerance* for specific risks, types of risk, or performance benchmarks. Tolerance defines the specific level of performance risk deemed acceptable according to the stated risk appetite.

The risk prioritization and response in this report are based upon the risk scenario descriptions that help to put each type of risk into perspective and enable the analysis of risk likelihood and consequences. Figure 3 illustrates the inputs to risk scenarios as detailed in NISTIR 8286A.

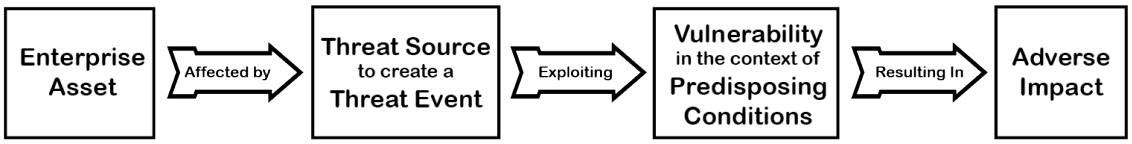


Figure 3: Inputs to Risk Scenario Identification

As described in Section 2, prioritization and response will take place based on an analysis of risk scenarios to determine the likelihood that a threat source will act, that a vulnerability does or will exist, and that an asset will experience an undesirable effect that impacts objectives. By considering this information with other details from throughout the enterprise, stakeholders can review and monitor risk management to ensure that performance is aligned with enterprise strategy and direction. Because all risk is dynamic, monitoring also enables ongoing adjustments to risk appetite, risk identification methods, and risk response.

Practitioners at all levels of the enterprise will also benefit from considering opportunities that represent beneficial uncertainty (sometimes referred to as positive risks). NISTIR 8286 provides the example of an organization that is evaluating moving a major financial system from an in-house data center to a commercial hosting provider and the potential financial gain of reducing space and utility requirements. While many cybersecurity risk managers have traditionally focused on negative risk, it is important to consider all types of uncertainty and to use that information to perform cost-benefit analyses to better inform decision-making.

1.4 Document Structure

This publication provides recommendations for determining, responding to, and reporting the relative priorities of risks, as documented in the CSRR, in light of the enterprise's risk strategy. Each of the sections below provide information and recommendations for determining risk priority based on the impact to enterprise objectives (Section 2.2), selecting one or more risk response actions (Section 2.3), finalizing the CSRR (Section 2.4), and conditioning results in preparation for risk report aggregation (Section 2.5). The document is organized into the following major sections:

- Section 2 details CSRM considerations for evaluating, responding to, communicating, and monitoring cybersecurity risk as an input to an ERM strategy and program.
- Section 3 provides a conclusion and highlights important elements regarding connections between this publication and NISTIR 8286C.
- The References section provides links to external sites or publications that offer additional information.
- Appendix A contains selected acronyms and abbreviations used in this publication.

2 Cybersecurity Risk Considerations

NISTIR 8286A illustrates methods for creating a CSRR for recording and communicating information about risks to information and technology. While NISTIR 8286A focuses on the identification and analysis of various risks representing the middle five fields of the risk register, this section focuses on completing the rest of the risk register based upon that analysis. This section will provide information to help complete the columns of the register shown in red boxes below.

Notional Cybersecurity Risk Register

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

Continually Communicate, Learn, and Update

Figure 4: Notional Cybersecurity Risk Register Template

As shown in NISTIRs 8286 and 8286A, a great deal of information can be collected and maintained in reference to various cybersecurity risks. While the CSRR provides a meaningful snapshot or summary of a given set of risk scenarios, it would be impractical to attempt to record all of the relevant information in such an artifact. Therefore, each risk in the CSRR links to a corresponding RDR. In some cases, the CSRR, the RDR, or both are instantiated in digital records within a risk management tool, such as a Governance/Risk/Compliance (GRC) product. A GRC product can be as simple as a set of connected databases or as complex as a global data infrastructure, but the goal is the same: to aggregate the relevant information that is known about various risks in light of enterprise governance direction and known compliance requirements to better inform decision makers.

NISTIR 8286A, Appendix B, contains an example of a risk detail record template. As each enterprise develops risk strategy and direction, the specific model for a CSRR and an RDR should be prescribed. Although this NISTIR 8286 series provides templates, they should be tailored to meet the needs of each enterprise. The use of such templates supports consistent risk tracking and reporting and enables the aggregation and integration of risk information. At a minimum, NIST recommends that a single record be recorded for each scenario in each CSRR. The use of separate registers and detail records enables each to communicate the appropriate level of detail. Many of the items described in the list above represent point-in-time information and should be updated at various points within the life cycle. Whether through a GRC tool or by updating risk records through some other method, information should be kept current based on a frequency established by senior leaders.

2.1 Assessment, Response, and Monitoring Across Enterprise Levels

A key challenge for risk managers is the confusion caused by common risk terms being used for divergent tasks. When considering the application of risk management processes in different contexts, communication among stakeholders may require additional information or clarification about activities. For example, even the meaning of the term *control* can vary depending on the context in which that term is used.

OMB A-123 states that *internal controls* "are tools to help program and financial managers achieve results and safeguard the integrity of their programs." It explains that "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." In this sense, an internal control provides an enterprise-level mechanism by which overall effectiveness, efficiency, reliability, and compliance can be enacted. Internal controls provide executives and senior leaders with methods and procedures to help ensure that enterprise objectives related to operations, reporting, and compliance are achieved. As the enterprise's leadership establishes an environment by which those internal controls are enacted (the "control environment") they also perform a *risk assessment* to determine conditions that may prevent the effective application of those internal controls. Business managers and system owners select and implement security and privacy control activities (e.g., those described in SP 800-53, *Security and Privacy Controls for Information Systems and Organizations*) to achieve the desired objectives and monitor their effectiveness [5]. Figure 5 illustrates that the terms *control*, *assess*, and *monitor* are used at all three hierarchy levels yet include different activities.

	Control	Assess	Monitor
Enterprise Level	Establish internal controls for effectiveness, efficiency, reliability, and compliance.	Identify internal and external risks (informed by current and previous findings) that may prevent the enterprise from meeting objectives. Analyze the potential enterprise effects of those risks.	Monitor the effectiveness of internal control and perform periodic reviews, reconciliation, and comparison of data. Integrate measures that promote and support effective internal control in accordance with applicable contractual, legislative, and regulatory requirements.
Organization Level	Establish general and shared controls (including risk management roles and strategy) to support enterprise-level controls and control objectives.	Assess risk through aggregated information from system level risk assessment results, continuous monitoring, and strategic risk considerations.	Implement policies and procedures to regularly receive information about the achievement of control objectives within the organization, and provide systematic processes for addressing deficiencies.
System Level	Select and implement control activities (e.g., security and privacy controls as described in NIST SP 800-53) to achieve control objectives within defined risk appetite and risk tolerance levels.	Assess whether the system level controls selected for implementation are applied correctly, operating as intended, and producing the desired outcome with respect to meeting the security and privacy requirements for the system and the enterprise.	Maintain ongoing situational awareness about the security and privacy posture of the information system in support of risk management decisions.

Figure 5: ERM and CSRM Actions Apply Common Terms in Different Ways

In the same way that controls, risk assessment, and monitoring are applied across these three hierarchy levels, metrics define performance measurement (including Key Performance Indicators, or KPIs) and risk tracking (including Key Risk Indicators, or KRIs). Figure 5 shows that as control, assessment, and monitoring activities occur, they support monitoring, evaluation, and adjustment at each level of the hierarchy. Risk practitioners should keep in mind that

because there are distinctions in terms at each organizational level, it is important to be clear about expectations and activities.

2.2 Prioritizing Cybersecurity Risks

After having calculated the risk exposure resulting from each risk in the CSRR, as detailed in IR8286A,[3] the next step in the process is to determine their relative priority. Because the priority reflects an order of precedence, the highest priority risks will not always be those with the greatest exposure value. Since risk response has not yet been determined, priority is not necessarily a reflection of the chronological order in which risk should be mitigated. Ultimately, the relative priority of various types of risk must by decided upon by those with appropriate authority at the executive level, usually through guidance provided through the risk management strategy. That strategy and the resulting internal guidance are interpreted at each level (such as by application at the system level in the CSRR) and may then be adjusted as risk management activities are reported and monitored (as illustrated in Figure 2). In this way, those in the enterprise who are accountable for cybersecurity oversight (e.g., a Chief Information Security Officer) establish priorities for cybersecurity risks, while enterprise executives have the final authority over how risk will be managed in the context of other enterprise risks.

The priority column describes the relative importance of each risk (usually ordered from most important to least important) based on the enterprise's risk management guidance. For some enterprises, this descending priority might influence the risk response (as described in Section 2.3) in that there are limited resources available for treating risk. Capital and operating expenses will likely be applied to those risks with the highest priority. There may be a point where resources are not available to treat risks below a particular importance, so it is necessary to be sure that the prioritization criteria are clearly agreed upon and communicated. Because it is important to convey both the risk exposure value and the determined priority, both data points are represented in the risk register template in the NISTIR 8286 series.

The OpenFAIR Risk Analysis standard (O-RA) points out that a mathematical calculation is limited in its ability to convey risk information [6]. For example, that standard reminds the reader that thinking about risk exposure as a function of "threat multiplied by vulnerability" does not necessarily convey sufficient information and that "any risk equation that ignores impact is going to be meaningless to the very people who need to use risk analyses to make risk decisions." This shortcoming of simplistic risk calculation also relates to challenges with prioritization.

2.2.1 Factors Influencing Prioritization

Numerous factors (e.g., financial loss, enterprise reputation, shareholder sentiment) influence priority and should be included in the enterprise risk strategy. A cybersecurity risk that directly impacts mission is likely to be a high priority, but many other considerations – such as agency or

[3] These values are described in NISTIR 8286A and may be based upon risk analysis methods, various sources of impact information (e.g., a traditional business impact analysis [BIA]), and other enterprise information such as from previous iterations of the cybersecurity risk management cycle. The formula for calculating risk exposure is described in NISTIR 8286A, Section 2.4, and represents the total loss if the risk occurs multiplied by the probability that the risk will happen.

corporate reputation – might move a particular type of risk to the top of the list. Another consideration might occur if a corporate entity were preparing for a merger. The community has seen recent examples that have demonstrated that discovery of a cybersecurity risk can affect the valuation of an enterprise and subsequent negotiations. There may also be factors that are not directly related to security but that might support organizational improvement (e.g., quick wins that will build team confidence and gain momentum, risks related to an objective that leaders have established as a key priority). Priority values such as low, moderate, and high are often used as risk prioritization categories. For example, this is the convention used for categorizing federal systems as described in Federal Information Processing Standards (FIPS) 199 and 200. This qualitative approach may be more limiting than quantitative analysis in that it is easier to sort a range of numerical values, even those that are relatively close, than it is to sort a list of risks marked "Very High." In most enterprises, risk strategy should provide direction for both generalization (e.g., low, moderate, high) and for more specific risk prioritization methods.

2.2.2 Cybersecurity Risk Optimization

As shown in various diagrams throughout the NISTIR 8286 series, a key goal of ERM/CSRM coordination is to help enterprise stakeholders collect various risk data for decision support, monitoring, and communications. Specific processes for bringing this information together are described in NISTIR 8286C, but there are several foundational definitions that are relevant to properly prioritizing risk at each state of the life cycle, including aggregating and prioritizing CSRR data discussed in this document:

- **Risk aggregation** – combination of a number of risks into one risk to develop a more complete understanding of the overall risk [ISO 73 definition] [7]

- **Risk criteria** – terms of reference against which the significance of a risk is evaluated, such as organizational objectives, internal/external internal context, and mandatory requirements (e.g., standards, laws, policies) [ISO 73 definition]

- **Risk optimization** – a risk-related process to minimize negative and maximize positive consequences and their respective probabilities; risk optimization depends on risk criteria, including costs and legal requirements [ENISA definition] [8]

The processes to aggregate, prioritize, and optimize risk will be different at each level of the enterprise, based on the risk criteria relevant to that level. At hierarchically lower levels in an enterprise, a certain amount of risk prioritization and treatment authority will have been delegated by the stated risk strategy guidance to streamline operations, but decisions at each level are considered to be provisional and subject to oversight (and override) from higher-level management.

Methods used for optimizing risk are at the discretion of enterprise leaders and are often carried out by a risk leadership council or other risk governance body. Since capital and operating expense budgets for risk response are likely to be limited, each method must include a process for how to respond to those scenarios when funding is not available. Some examples include:

- **Fiscal optimization** – a straightforward ranking of risks in descending order from most impactful to least. Risk managers would simply tally the total of risk response costs until funding is exhausted.

- **Algorithmic optimization** – the application of mathematical formulae to calculate the aggregate cost benefit to the enterprise, given the estimated costs, in a purely mechanical approach.

- **Operational optimization** – selection of those risks from the register that are most valuable based upon leadership preferences, mission objectives, stakeholder sentiment (e.g., those of customers, citizens, or shareholders), and other subjective criteria. Another optimization factor is operational and based on an iterative communications cycle of risk reporting and analytics.

- **Forced ranking optimization** - prioritizing risks in the way that will best use available resources to achieve the maximum benefit given specific negative and positive consequences. Various business drivers and risk consequences have differing weights for developing a score, helping to move beyond the simplistic "threat multiplied by vulnerability" approach to build business objectives into that equation. Because these factors and their weights are based on business drivers, the factors should be defined by senior stakeholders but can be applied at all levels of the enterprise, subject to adjustment and refinement.

Ultimately, the optimization performed will likely be some combination of these methods. For some enterprises, risk optimization may also have a temporal factor. For example, risk owners might be willing to accept some risk scenarios in order to reduce expenses and boost profitability near the end of a fiscal quarter. Those same scenarios might be fully treated in more favorable financial circumstances. The goal of this report is not to advocate for any particular optimization process but rather to determine how optimization and prioritization will occur, since these decisions must precede risk response itself.

Keep in mind that these management processes are iterative. Generally speaking, as risk information is aggregated throughout the enterprise, more information becomes available about risk commonalities. As risk managers observe similar types of positive and negative risk events, they can note contributing factors, highlight common opportunities, and gain a broader understanding of risk conditions. Because leaders and executives often have a broader view of factors that contribute to and result from various risks, including cybersecurity risks, they can provide additional criteria to hierarchically lower levels to help sort and prioritize.

2.2.3 Cybersecurity Risk Priorities at Each Enterprise Level

In support of risk prioritization, as with cybersecurity risks themselves, the ranking factors reflect the various strata of the enterprise. At Level 3, the CSRR reflects risk priorities related to particular systems and technologies. The organization level has its own priorities based on unique mission and business unit drivers. The enterprise has overarching cybersecurity priorities that may not be the same as those at lower technical levels of abstraction, and they can be of varying priority when considered along with other enterprise risks. This balance is foundational to the concept of CSRM as an input to ERM. While risks to institutional information and

technology are critical parts of the enterprise and a primary focus of those charged with leading CSRM, corporate officers and fiduciaries have a broad perspective and must balance the dozens of types of uncertainty in the enterprise risk universe. Bi-directional communication is critical, enabling senior leaders to convey strategy and direction while also enabling system and business level managers to keep leadership informed. This process does not mean that every system level risk decision should be elevated to top leadership but rather that many risk decisions at the system and organization levels should be considered provisional and that leaders may subsequently recommend a different priority or approach based on their understanding of the aggregate impact to enterprise factors (e.g., revenue, reputation, regulations, or political). Additional information regarding risk aggregation and subsequent communication is described in NISTIR 8286C.

Since prioritization factors vary by enterprise, this report does not prescribe an approach. Many entities begin by sorting within the risk register from largest to smallest risk exposure rating. Specific risks can then be moved to tailor prioritization based on guidance provided in the enterprise strategy (and from leaders and managers at appropriate enterprise, organizational, and system levels). Figure 6 shows a notional set of risks and example assessments.

ID	Priority	Risk Description	Risk Category	Current Assessment		
				Likelihood	Impact	Exposure Rating
2	1	External malicious actor deploys a ransomware attack causing unavailability of financial systems	System and Information Integrity (SI)	0.9	0.9	.81
5	2	Portable workstation containing digital designs is lost (e.g., left on an airplane)	System and Communication Protection (SC)	0.8	0.5	.40
3	3	A natural disaster disrupts communications circuits impeding customer access	Contingency Planning (CP)	0.4	0.3	.12
1	4	A computer tower is stolen from the reception area	Physical and Environmental Protection (PE)	0.75	0.1	.075
4	1	Human Resource Management Systems move to a cloud solution, providing in-house IT infrastructure savings and improving availability.	System and Services Acquisition (SA)	0.5	0.5	.25

Figure 6: Excerpt from a Notional Cybersecurity Risk Register (from NISTIR 8286)

While this order represents the initial sort, there may be additional information, including guidance provided through risk appetite and risk tolerance instructions. Risk 3, for example, may become a higher priority if:

- Senior leaders have designed availability as a key mission objective,
- Service-level agreements with customers or constituents would be jeopardized, or
- A critical event is occurring, during which a communications outage would have serious reputational effects even if the direct financial impact would be relatively low (in this case, 30 %).

The example above illustrates that prioritization and tailoring may use the term *impact* in a non-technical sense to indicate a general or adverse effect, or it could be used in a more technical sense to indicate a calculable and measurable loss. Recalling the very definition of risk as "the

effect of uncertainty on objectives," prioritization considers each uncertainty represented in the CSRR and the overall effects of that uncertainty on enterprise mission and business objectives.

2.2.4 Considerations of Positive Risks as an Input to ERM

Uncertainty can be positive, negative, or sometimes both, and risks of all types should be included in communications and prioritization. Figure 6 includes an example of an opportunity expressed as a positive risk. This integration of positive and negative risks on the same CSRR helps with the dual-faceted prioritization process described above. Colocation of both types of risk ensures that senior managers are fully aware of all of the uncertainties that might bring benefit or harm. If multiple positive risks are listed in the CSRR, then the negative risks can be ranked in descending order of their negative impact, as tailored by enterprise factors, and the positive risks (or opportunities) can be listed in descending order of their enterprise benefit in a similar way.

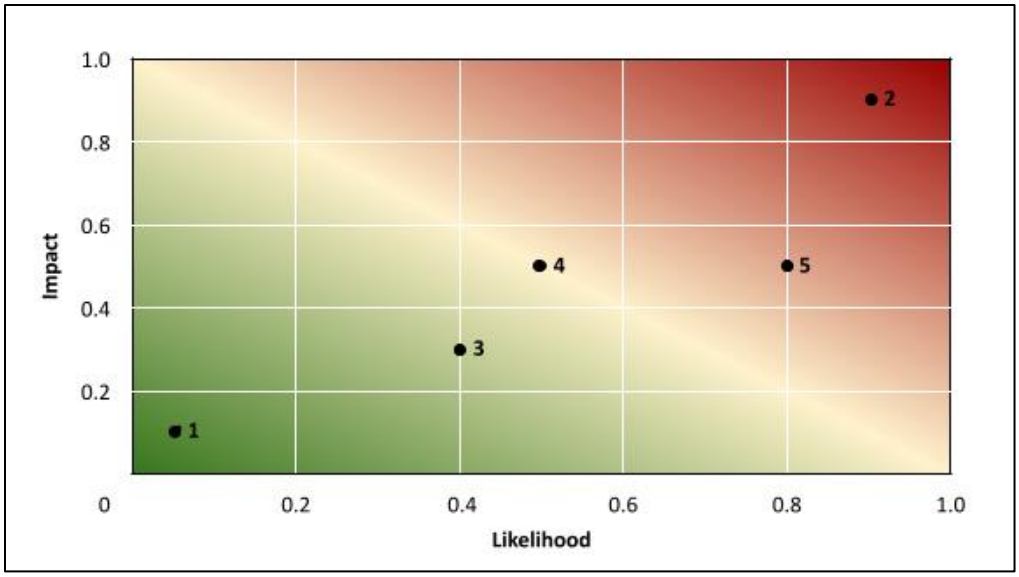
Prioritization and risk evaluation must also consider the positive risks that might evolve from an opportunity. Risk calculations are often based on analysis of both the cost of response and the benefit of proceeding. For example, while there have been many cybersecurity risks inherent to telework scenarios, organizations are increasingly realizing that a remote workforce brings positive benefits (e.g., reduced office space costs and utilities, reduced commuting time for employees, wider access to a skilled workforce). Understanding and calculating the various factors – such as through a strength, weakness, opportunity, and threat (SWOT) analysis – helps to prioritize all risks and evaluate available responses.

Such an analysis must also keep in mind the consequences of failure to pursue an opportunity, even in light of certain negative risks. An organization that is considering creating a new product offering that works through a mobile device application must weigh the potential negative risks (e.g., intentional attacks by cyber criminals, software errors that might create customer support needs) against the positive risks (e.g., additional customer revenue and market share opportunities) made available through that offering. Basing risk considerations on benefits to and consequences on enterprise drivers, such as the factors described in Section 2.2.1 (including risk appetite and risk tolerance directives), supports mission-focused prioritization.

2.2.5 Visualizing Risk Priority

Heat map diagrams are often used to help visualize the relative priority of the risks, though such a graphic should be used with caution. The background colors and relative positions of the various uncertainties are a guide for quick reference, not necessarily an indicator of rigid boundaries. As discussed in Section 2.2, a mathematical calculation – in this case based upon likelihood and impact – is limited in its ability to convey risk information. A matrix illustration based on such a calculation is helpful for visualization but is equally limited.

Both the positive and negative uncertainties are reflected in Figure 7. While some readers may automatically associate red areas of the map with "bad" and green areas with "good," the red (the top right in the case below) area may also represent a highly likely and beneficial opportunity. In fact, it is not unusual to hear someone reference a "red-hot opportunity" in a positive light. It is also notable that Figure 7 illustrates positive and negative risks together, highlighting those risks and opportunities that are likely to have the greatest impact (whether harmful or beneficial).



654

655 **Figure 7: Example Risk Map Illustrating Prioritization of the Risks in Figure 6**

656 Alternatively, the positive and negative uncertainties might be reflected on separate risk maps, as
657 shown in Figure 8. This model shows both risks and opportunities together, calling attention to
658 both the most valuable opportunities and the most threatening risks. Each of these prioritization
659 considerations will factor into risk response, as described below, but the reader should keep in
660 mind that risk management itself is a dynamic process and that conditions can change frequently
661 and rapidly. Through the methods described, coordination within and among levels and
662 collaborative communications among risk management participants help to ensure consistent and
663 appropriate adjustment in a changing environment.

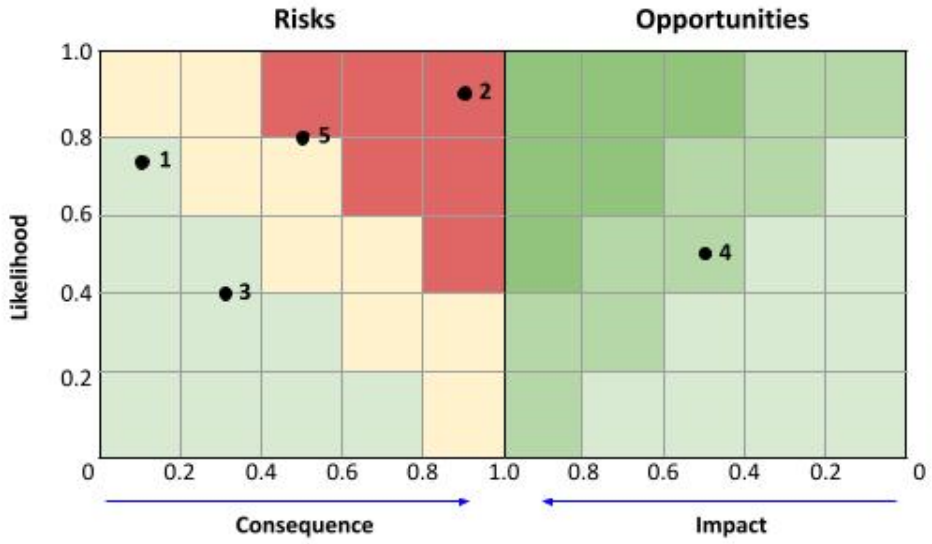


Figure 8: Alternative Risk Map with Separate Risk and Opportunity Mapping

Whichever method is used, it is important that a consistent methodology be applied throughout the enterprise. Using consistent prioritization, optimization, and visualization throughout all levels and describing risk factors and weighting that have been agreed upon by appropriate stakeholders help improve consistent and effective risk management.

2.3 Selection of Risk Response Types

Having established the relative priority of the risks in the CSRR, the next step is to determine the appropriate actions necessary to ensure suitable and cost-effective risk treatment. Risk response selection is an important element of maintaining appropriate balance among value, risk, and resources. Risk response should result in residual risk levels at or below the risk appetite and risk tolerance directives provided in previous activities.

Enterprise risk strategy often describes levels of authority regarding who may approve risk treatment decisions. For example, the selection and approval of controls for a system that has been confirmed to be low impact may generally be approved by the system owner. As the potential impact of risk consequences increases, the level of coordination and oversight usually increases. Because these levels may vary greatly, it is important that levels of authority are well defined by role as part of the ERM policy and process.

There may be occasions when unacceptable risk cannot be adequately treated within the reporting period (such as due to insufficient resources). In such a case, the risk is implicitly accepted, and the risk manager has – at least temporarily – adjusted the risk tolerance range until the risk scenario can be sufficiently treated. For Federal Government enterprises, information security risk responses planned but not yet implemented are often recorded in a Plan of Action and Milestones (POA&M). While POA&Ms reflect a subset of the types of risk contained within a CSRR, the enterprise risk register is used for aggregating information with other risk data (e.g., other enterprise considerations, such as reputational, financial, and market risks) since POA&Ms do not exist for that non-cybersecurity data. While data can be exchanged among various formats and protocols, the data will often need to be transliterated as well. For example, using a POA&M in place of the CSRR would not describe the positive risks (opportunities) that are required by A-123 for federal agencies' enterprise risk profiles.

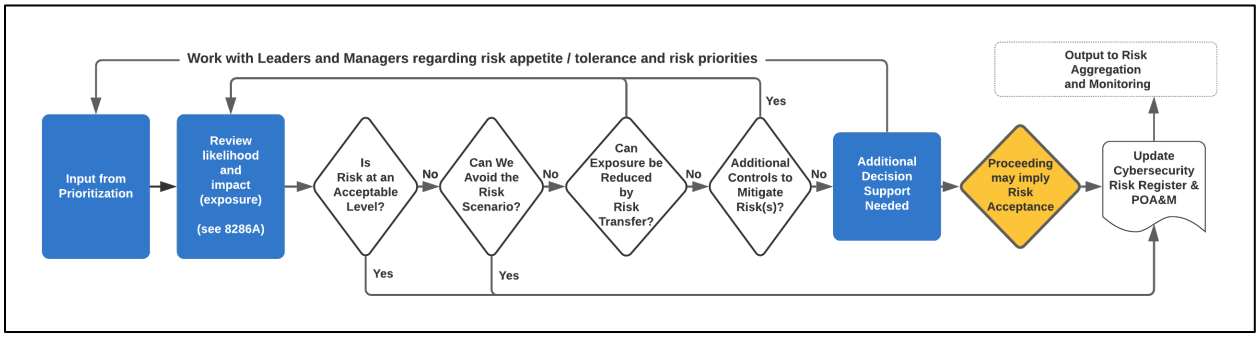
Similarly, while federal agencies may be permitted to use a POA&M describing future mitigation, such a condition is not permissible in private industry, and all risks must be fully disclosed, treated, and communicated. Corporate, shareholder, and regulatory stakeholders require comprehensive disclosure, so any planned future mitigation would need to be transliterated as "accepted" from the risk register and vice versa from the POA&M, depending on the date of mitigation. Doing so ensures that all residual risks will be included in the risk aggregation, correlation, and communication described throughout the NISTIR 8286 series. Including those risks in the POA&M, the CSRR, and – if applicable – the RDR ensures more complete communication and awareness of risks that have been identified but not yet treated.

Application of response methods does not need to be mutually exclusive. A risk owner is likely to apply a hybrid of multiple response methods to achieve the desired effect. Anyone who has driven an automobile has experienced this by both applying risk mitigation techniques (e.g., seat belts, airbags) and risk sharing methods (e.g., automobile insurance). The goal of the risk owner is to evaluate the options that will best achieve the balance among value, risk, and resources.

706 **Table 1: Response Types for Negative Cybersecurity Risks**

Type	Description
Accept	Accept cybersecurity risk within risk tolerance levels. No additional risk response action is needed except for monitoring.
Transfer	For cybersecurity risks that fall outside of tolerance levels, reduce them to an acceptable level by sharing a portion of the consequences with another party (e.g., cybersecurity insurance). While some of the financial consequences may be transferrable, there are often consequences that cannot be transferred, like the loss of customer trust. (Sometimes referenced as Sharing.)
Mitigate	Apply actions (e.g., security controls discussed in Section 3.5.1) that reduce the threats, vulnerabilities, and impacts of a given risk to an acceptable level. Responses could include those that help prevent a loss (i.e., reducing the probability of occurrence or the likelihood that a threat event materializes or succeeds) or that help limit such a loss by decreasing damage and liability.
Avoid	Apply responses to ensure that the risk does not occur. Avoiding a risk may be the best option if there is no cost-effective method for reducing the cybersecurity risk to an acceptable level. The cost of the lost opportunity associated with such a decision should be considered as well.

707 For each risk in the register, and considering the priority established above, the risk owner steps
708 through the decision points (in the listed order) illustrated in Figure 9 and considers methods and
709 options to bring the residual risk exposure to within an acceptable range. Details about each
710 response option are provided below.



711
712 **Figure 9: Risk Response Workflow**

713 When performing the risk decision workflow, remember that constraints (e.g., mandatory
714 regulatory requirements) may impact the decisions. For example, while a business unit manager
715 may wrongly decide that placing customer pharmaceutical records on an unencrypted laptop
716 represents an acceptable low risk, consumer protection and health information protection
717 regulations make that decision unsuitable. There may also be instances where a given risk
718 response has been pre-established, perhaps based on previous issues, stakeholder expectations, or
719 industry best practices.

720 Whichever method is selected for dealing with risks for which response resources are not
721 currently available, it is important to remember that "ignore risk" is not among the available
722 choices since that would represent passive acceptance of the risk. Even if all mitigation and
723 transfer options are not currently practical, there must be a clear plan for how that situation will
724 be remedied, and the residual risk must be included in enterprise risk reporting processes,
725 including the CSRR (and associated POA&M documents, if applicable).

As risk response decisions occur throughout the enterprise, reporting about performance and trends also takes place. Many cybersecurity incidents have become notorious because senior leaders were unaware that serious risks were being accepted by lower levels of management.

As response activities in the risk management life cycle occur, performance and trending metrics are collected and shared (including KPIs and KRIs) to help risk practitioners monitor the effects of these uncertainties on mission objectives. This information collection and sharing might be aided by the use of a GRC product. Monitoring and communication help to convey other information, such as an understanding of any risks that are outside of the risk tolerance range and yet are not treated to an acceptable level. By definition, someone has "accepted" such a risk, indicating either a need to adjust the tolerance or to take some action to offset the potential impact (e.g., setting aside reserve funding to deal with the implications should the risk scenario actually occur). Where decisions are being made based on previous iterations, performance results and ongoing risk trends may influence the next round through the workflow.

A key challenge with risk response is that one can often offset the financial impact of a risk, but other factors like reputation, regulatory compliance, or volatility might still have a significant impact on the enterprise. Cybersecurity insurance may reduce some financial costs of a ransomware attack, but the enterprise's reputation may still be tainted in customers' memories, potentially impacting shareholder sentiment and leading to stock volatility. Since downstream risk consequences can create combined enterprise impact, the use of risk treatment methods may also need to be combined to ensure that potential impacts are maintained at acceptable levels.

Figure 10 illustrates a number of risks shown in an excerpt of a CSRR. The sections below describe some of the considerations that led to the proposed responses and provide RDR excerpts with additional detail.

ID	Priority	Risk Description	Risk Category	Current Assessment			Risk Response Type	Risk Response Cost	Risk Response Description	Risk Owner	Status
				Likelihood	Impact	Exposure Rating					
17	L	Personal computer (PC) is stolen from the reception area.	Physical and Environmental Protection (PE)	75%	$2,000	$1,500	Accept	$0	No response required	Kira Caldwell	Open
25	H	Unauthorized connection to manufacturing plant, altering 3D plans, corrupts production goods.	Access Control (AC)	37%	$1M	$370K	Avoid	$0	No response required	Jemima Daugherty (Carly Hickman - backup)	Closed
21	M	A natural disaster disrupts communications circuits impeding customer access.	Contingency Planning (CP)	10%	$1.5M	$150K	Transfer	$150K	Purchase cybersecurity insurance to reimburse downtime	Mark Winters	Closed
8	M	A tornado disrupts headquarters communications circuits impeding e-commerce traffic.	Contingency Planning (CP)	10%	$1.5M	$150K	Mitigate	$250K	Move circuits into underground conduit. (See RDR notes for justification)	Mark Winters	Updated
11	H	Attacker exploits web server flaw, deploys a ransomware program on critical financial reporting system.	System and Information Integrity (SI)	90%	$4.1M	$3.7M	Mitigate	$1.9M	Re-engineer networks with separation; improve backups; improve patching; update policies	Jeffrey Contreras	Updated

Figure 10: Example Risk Responses in the CSRR

2.3.1 Risk Acceptance

The first risk response evaluation is to consider whether the exposure presented by the risk scenario is already at an acceptable level based on relevant risk tolerance statements. Notably, such a decision does not indicate that the risk is negligible or unimportant. The risk must be reported, monitored, and managed to ensure that risk conditions remain in an acceptable range as defined by risk tolerance. The risk owner might choose to accept the risk while applying a financial control to address a cybersecurity risk. In such a case, the risk reserves are not intended

to transfer risk impact or mitigate risk exposure but rather to provide resources that may be used as a counterbalance if risk factors change.

The figure below draws from NISTIR 8286, Figure 7, a notional CSRR with illustrative examples. Risk 1 of that example describes the loss of a computing device from the visitor reception area of a company. In this case, the owner of that endpoint confirms that there is no confidential or corporate information on the device. While a computer lock cable was added, the likelihood that the computer would be stolen from this area is still high since the reception area is often unattended, but the system owner accepts that risk and has updated the CSRR.

Risk Description	Personal computer (PC) is stolen from the reception area.	
Risk Category	Physical and Environmental Protection (PE).	
Current Risk Analysis		
Likelihood before controls (%): 75 %	**Impact before controls ($):** $2,000	**Exposure Rating before controls ($):** $1,500
Planned Risk Response	Select all that apply: ☑ **Accept** ☐ **Avoid** ☐ **Transfer** ☐ **Mitigate**	
Planned Risk Response Description	None required. See Decision Memo from Betsy Smith dated 05 May 2021.	
Resource Requirements for Planned Risk Response	None required.	
Planned Response Cost ($)	None required.	

Figure 11: RDR Excerpt – Example for an Acceptable Risk

2.3.2 Risk Avoidance

In some cases, if the risk exposure rating exceeds risk tolerance limits, the risk owner may determine that the best course of action is not to conduct the activity that results in the risk scenario. While it is rare that no combination of risk transfer and mitigation would bring the exposure to an acceptable level, there may be times when avoiding the risk is the wisest choice. This response type is exemplified by a manufacturer that has decided not to connect industrial control systems to the Internet, as shown in Figure 12. While such connectivity might bring some benefits, such as remote support and maintenance capabilities, the system owner may decide that the potential harmful impact may outweigh those benefits or that the cost of reaching an acceptable level of risk would not be a reasonable investment of resources.

Enterprise risk strategy may wish to declare the conditions under which a risk must be avoided. In other cases, the decision about whether to avoid a risk may occur after all other options have been exhausted. As with other risk considerations, this decision process may be cyclic.

Risk Description	An unauthorized external party connects to manufacturing control systems and alters 3D printing programming, corrupting a significant portion of manufactured goods.	
Risk Category	Access Control (AC).	
Current Risk Analysis		
Likelihood before controls (%): 37 %	**Impact before controls ($):** $1,000,000	**Exposure Rating before controls ($):** $370,000

Planned Risk Response	Select all that apply: ☐ **Accept** ☑ **Avoid** ☐ **Transfer** ☐ **Mitigate**
Planned Risk Response Description	While there might be corrective controls that could be applied, the CEO, guided by the governing body, has expressed zero risk appetite for any consequence that could jeopardize customer trust, as might occur with a breach of the manufacturing processes. To ensure that this risk does not occur, the board has determined to avoid this risk by prohibiting the interconnection of manufacturing systems to any other network, including other enterprise internetworks.
Resource Requirements for Planned Risk Response	None required.
Planned Response Cost ($)	None required.

Figure 12: RDR Excerpt – Example of Risk Avoidance

2.3.3 Risk Transfer

If a risk in the register cannot be accepted or fully avoided, another option would be to determine if some or all of the exposure could be transferred to (or shared with) another entity. The most frequent example of this activity is the use of an insurance provision that would help to offset the financial impact of a given risk scenario. Another common example of risk transfer is to outsource some risky activity, such as handling payment card transactions.

Figure 13 illustrates notional risk 3 from NISTIR 8286, Figure 7, that describes a condition where communications circuits are disrupted by a natural disaster. Because it would be rare for this enterprise to experience such a disaster, the risk owner has decided to purchase cybersecurity insurance that will reimburse the financial losses of such an outage. Note that, based on the discussion above, if the priority of this risk has been elevated (perhaps to meet a critical service-level agreement), then the potential impact may need to be reevaluated and the CSRR updated accordingly. In such a case, additional steps (such as mitigation, described below) may need to be added.

Risk Description	A natural disaster disrupts communications circuits impeding customer access.	
Risk Category	Contingency Planning (CP).	
Current Risk Analysis		
Likelihood before controls (%): 10 %	**Impact before controls ($):** $1,500,000	**Exposure Rating before controls ($):** $150,000
Planned Risk Response	Select all that apply: ☐ **Accept** ☐ **Avoid** ☑ **Transfer** ☐ **Mitigate**	
Planned Risk Response Description	Add additional coverage to enterprise disaster recovery policy to insure the direct losses caused by customer communication disruption from a covered event.	
Resource Requirements for Planned Risk Response	Existing disaster recovery/business continuity staff planning will address this risk. The cost to manage the restoration of services is already built into the incident response planning budget.	

	Public communications resources that are necessary to manage public announcements, periodic updates, and recovery communications are included in the Public Affairs budget.
Planned Response Cost ($)	Policy: $150,000 per year
Notes	All reviewers should keep in mind that this approach will provide direct reimbursement of some losses (TBD based upon policy specifics), but there will still be enterprise reputational consequences based on customer frustration, and there may be additional financial consequences if the outage results in a missed service-level agreement with a major customer. Additional research regarding this risk is necessary to ensure adequate treatment.

795 **Figure 13: RDR Excerpt – Example of Risk Transfer**

796 ### 2.3.4 Risk Mitigation

797 The most common method of responding to risk is to mitigate risk conditions, generally through
798 the application of various technical, managerial, and operational controls that reduce the
799 likelihood and impact of a risk occurrence. For many of the scenarios described in the CSRR,
800 mitigation occurs through the direct treatment of cybersecurity-related factors. In general, risk
801 managers apply combinations of internal and external human resources, enterprise processes, and
802 various types of information and technology to achieve an acceptable level of risk. Types of
803 controls include:

804 • **Preventative**: Reduce or eliminate specific instances of a vulnerability. Example:
805 network architects ensure physical or logical separation among network enclaves to help
806 isolate suspicious or malicious activities to the smallest area possible.

807 • **Deterrent**: Reduce the likelihood of a threat event by dissuading a threat actor. Example:
808 a warning banner that notifies a system user before they attempt to authenticate that the
809 system is closely monitored and that illicit activities may result in criminal prosecution.
810 The banner's key purpose is to dissuade unauthorized actions.

811 • **Detective**: Provide warning of a successful or attempted threat event. Example: an
812 intrusion detection system (IDS) alerts an operator in the Security Operations Center
813 (SOC) upon noticing that a network user has just downloaded an unapproved software
814 product.

815 • **Corrective**: Reduce exposure by offsetting the impact of consequences after a risk event.
816 Example: an anti-virus product quarantines a suspicious file that matches the signature of
817 malicious software.

818 • **Compensating**: Apply one or more cybersecurity controls to adjust for a weakness in
819 another control. Example: alarms on a server room door audibly notify nearby personnel
820 when an emergency exit push bar has been used, thereby compensating for a physical
821 access control that has been bypassed.

822 As mitigation techniques help to reduce the frequency or likelihood of a risk scenario (as in the
823 warning banner and anti-virus illustrations), the impact of a scenario (as in the network
824 segmentation example), or both, practitioners can iterate through the CSRR to bring the overall

risk level to within acceptable limits. Many sources of cybersecurity controls are available, such as those described in SP 800-53, *Security and Privacy Controls for Information Systems and Organizations* [5]. Based upon ERM roles, strategy, risk assessment, and prioritization direction, system owners and risk managers work to select, implement, and monitor various controls to ensure that risks remain within acceptable limits.

The application of cybersecurity controls should be evaluated by a competent assessor to confirm that the intended mitigation techniques are effective, optimize the use of resources, and achieve management direction regarding risk appetite and tolerance. Because this example includes several third-party supply chain partners, the assessment will likely include multiple parties. SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations*, provides detailed criteria for examining the application of controls and processes, testing control effectiveness, and conducting interviews to confirm that the mitigation techniques are likely to achieve their intended results [9]. The results of the application of those controls provide performance and risk metrics (including KPIs and KRIs) that may then be used to monitor the achievement of risk appetite and risk tolerance directives.

The cybersecurity control assessment also provides an opportunity to review and discuss the intended response. Consider the disaster recovery example above in Section 2.3.3. After calculating the annual cost of insurance combined with potential reputation and financial consequences, management might choose to seek an alternative risk response or at least consider other options. In this case, the system owner may have discussed the situation with their manager, who may have asked what the response might have been if they did not accept the risk. The manager may have also asked for estimated costs for the response, which could include:

- Moving overhead trunk lines underground to reduce susceptibility to windstorms
- Installing underground fiber-optic cabling between headquarters and the communications center below the frost line
- Funding the cost of the trench construction, conduit materials, new communications equipment, and time for the network staff to perform the necessary transitions

The final estimated cost of remediating this loss was calculated at $250,000, which exceeds a single year exposure but may make sense when considering annualized loss expectancy (ALE) over time. The manager might have also asked the system owner to review the risk analysis to confirm its reliability. If the 10 % likelihood were a guess and a subsequent simulation showed anything over 10 %, that exposure rating could be significantly higher, resulting in an unacceptable condition and leading the system owner to explore other risk response options. In this example, the risk analysis was reviewed by several knowledgeable experts and confirmed as a reasonable estimate, so the manager and system owner document that fact and decide that risk mitigation will provide a suitable solution.

Risk Description	A natural disaster disrupts communications circuits, impeding customer access.
Risk Category	Contingency Planning (CP).
Current Risk Analysis	

Likelihood before controls (%): 10 %	**Impact before controls ($):** $1,500,000	**Exposure Rating before controls ($):** $150,000
Planned Risk Response	Select all that apply: ☐ **Accept** ☐ **Avoid** ☐ **Transfer** ☑ **Mitigate**	
Planned Risk Response Description	Having identified that the key vulnerability is to overhead communications wiring, these circuits will be buried underground.	
Resource Requirements for Planned Risk Response	Network architecture staff will plan and design the new infrastructure (existing labor budget). A contract is made to install underground fiber-optic cabling between headquarters and the communications center, including necessary permits, trench construction, conduit materials, and new communications equipment.	
Planned Response Cost ($)	Construction, Equipment, and In-house Labor: $250,000	
Notes	While this response cost exceeds the impact of a single loss exposure, the cost to permanently mitigate this risk is a reasonable use of capital expenses.	

Figure 14: RDR Excerpt – Risk Mitigation

2.3.5 Relationship of Risk Response to Risk Strategy

Stakeholders monitoring risk management activities should be able to recognize the ways in which risk response will result in achieving risk direction in terms of previously provided risk appetite and risk tolerance statements. Consider an organization where the Chief Executive Officer has made the statements that the enterprise "has no appetite for any risk that results from a vulnerability for which a patch has been released" and that the enterprise "must prioritize any risk that would jeopardize the fulfillment of customer service-level agreements (SLAs)." Senior leaders might interpret those statements to define two risk tolerance statements:

1. All vendor-supplied security patches must be applied within 120 days of issue, with critical patches being tested and applied within 14 days.
2. The application of software patches will be conducted in a manner that minimizes downtime and does not result in service unavailability (of more than one hour for each occurrence) to more than 5 % of those customers with SLAs.

Based on risk tolerance, the risk owner must apply the guidance to achieve risk response through appropriate actions that balance availability and integrity requirements of the system. That response must consider ways in which software patch activities, which often result in system restarts and other disruption, might reduce functionality and uptime; it must also consider the fact that not patching will result in dangerous vulnerabilities remaining on critical systems.

Based on the facts above, the system owner has established a rule that all relevant security patches must be applied. The timeline for that application is based on the risk represented by the severity of the vulnerability, as assessed by the Common Vulnerability Scoring System (CVSS) in accordance with the following schedule:

- Critical severity: 14 days
- High severity: 30 days
- Medium severity: 90 days
- Low severity: 120 days

Because the rule, established as application of the risk tolerance statement, mandates the application of any relevant security patch, the choice of not applying the patch is not acceptable. The system owner eliminated avoidance and risk sharing for this situation. Therefore, the system owner must mitigate both risks. That system owner must work with the security team to develop and implement a plan for testing, staging, and applying the security patch in a way that does not cause disruption to the system.

To support the connection between risk response and overall risk strategy, practitioners may apply a monitor-evaluate-adjust (MEA) process (shown in Figure 15). Risk tolerance statements are translated into a triad of interrelated security mechanisms: security controls, KPIs, and KRIs. Extending the patch example above, one can decompose the elements into these parts:

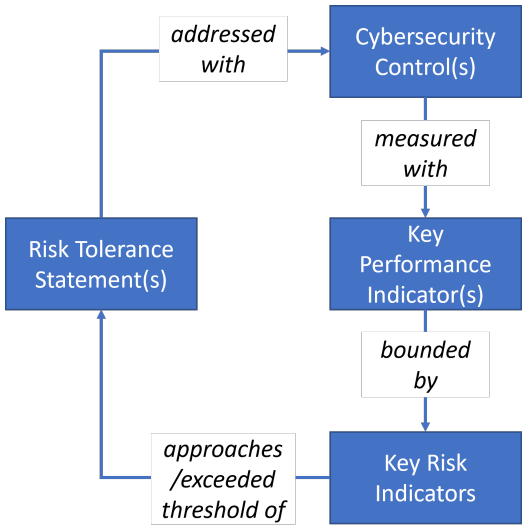


Figure 15: Monitor-Evaluate-Adjust Management Cycle

- Risk appetite: no appetite for any risk that results from a vulnerability for which a patch has been released; enterprise must prioritize any risk that would jeopardize the fulfillment of customer service-level agreements (SLAs)
- Risk tolerance: patches are applied within 120 days and critical within 14 days, all in a manner that minimizes downtime and supports customer SLAs
- Cybersecurity controls: flaw remediation; virtual test environment; continuous monitoring; security planning, policy, and procedures
- KPI: Mean-time-to-patch (MTTP) results (in days); availability metrics (in %); periodic SLA achievement results (in %); recovery time objective (RTO) achievement (in %)
- Leading KRI: critical patches taking 10 days or more; availability reports with cumulative downtime approaching unacceptable levels
- Lagging KRI: recoveries with missed RTOs; incident handling reports where an event occurred through a vulnerability that should have been mitigated

As the MEA cycle occurs as part of normal operations, the achievement of risk directives is tracked through performance and risk metrics, supporting evaluation of effectiveness and, if necessary, subsequent adjustment. The adjustment component of that process is important – if risk managers determine that there are compelling business objectives that necessitate delays in patching, and if organization leaders are aware of both the operational benefits of exceeding risk limits and the consequences of doing so, the appropriate parties may decide and document the conditions under which risk appetite and tolerance may be adjusted. These decisions must be well-communicated and approved by the appropriate stakeholders, who must accept the potential consequences of the risks undertaken.

Even if an exception were provided for a particular patch circumstance, risk managers might still continue to monitor KPIs and alert on the KRIs established. For example, given the deadlines described above, management may set "low-severity patches not applied within 90 days" as a KRI, whereby a system owner applying those within 30 days might be marked "green" and a system owner not yet patched after 100 days might be marked "red," possibly with required escalation to more senior management for immediate action.

Risk Description	An organized cyber-crime attacker exploits a known web server vulnerability to deploy a ransomware program, causing unavailability of the corporate financial reporting system.	
Risk Category	System and Information Integrity (SI).	
Current Risk Analysis		
Likelihood before controls (%): 90%	**Impact before controls ($):** 90%	**Exposure Rating before controls ($):** $2,900,000 - $3,700,000
Planned Risk Response	Select all that apply: ☐ **Accept** ☐ **Avoid** ☐ **Transfer** ☑ **Mitigate**	
Planned Risk Response Description	Better isolate networks containing critical financial systems from other networks supporting external facing applications; improve the diversity of backup solutions to minimize opportunities for adversaries to corrupt (or introduce vulnerabilities) to backup media; apply software patching methodologies to all enterprise systems in accordance with Vulnerability Management policy POL-VM-001 and as described in the financial systems' security plans.	
Resource Requirements for Planned Risk Response	Labor, network diagram updates, and testing resources will be needed for network segmentation activities. Existing staff will update backup process improvement, but additional disaster recovery and business continuity testing should be approved to ensure sufficient backup diversity and that participants understand how to apply various methods. The enterprise's threat intelligence service already provides information regarding new vulnerabilities, but external service support will be necessary to create and implement a sandbox for testing the impacts and efficacy of patches.	
Planned Response Cost ($)	$1,300,000 - $1,900,000	
Notes	Variance in response cost is partially based on network segmentation costs that are being updated based on results in other divisions. Initial isolation is through network virtualization using existing equipment, but tests are being performed to determine if physical isolation is recommended for critical networks.	

Figure 16: RDR Excerpt – Risk Mitigation (Example 2)

2.3.6 Implicit Acceptance

While a clear definition of risk response is the optimal method of communicating activity and status, there are likely to be times when a risk has been implicitly accepted. There may even be times when that acceptance has occurred without the full knowledge or understanding of all of the risk stakeholders involved. Examples of this implicit acceptance include:

- **Postponement due to conflict or resource constraints** – There may be cases where a risk owner has determined the actions that are necessary to reduce risk to an acceptable level yet does not have available time, funding, or other resources to accomplish that

mitigation. There may also be disagreement over specific risk tolerance interpretation since theoretical policy and declarations may be less clear in real-world applications. In cases like these, there should be collaboration between the risk owner, security team, and other enterprise personnel, including Level 1 and Level 2 security leaders. The team will need to realistically evaluate what actions may reasonably be taken and may decide that additional mitigation or transfer will take place in the future. If that is the case, those deadlines and activities should be recorded, including in the CSRR and RDR.

- **Future mitigation through a POA&M** – Federal agencies that apply the processes described in SP 800-37, Revision 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, record planned actions in a POA&M [11]. This document enables awareness of residual risk, ensures accountability, and highlights the need for particular risk scenarios to be closely monitored. A POA&M also enables the documentation of future plans for additional risk response. However, until that response occurs, the related risks should be recorded in the CSRR as a condition that is outside of risk tolerance parameters yet has not been accepted. The POA&M artifact is unique to federal agencies, and most non-federal enterprises use risk register entries (supported by details within the RDR) to document accepted risks for which future mitigation is planned.

- **Disclosure of future steps and forward-looking statements** – Enterprise leaders may document (i.e., for customers, shareholders, directors, or regulators) specific risk responses that will be performed in the future but have not yet taken place. For example, a publicly traded enterprise might be required (under Regulation S-K of the U.S. Securities Act) to provide qualitative disclosures of various risk factors that could influence investment decisions, including cybersecurity risk. These factors are included in the enterprise's annual or quarterly report (i.e., SEC Form 10-K or 10-Q, respectively) to enhance accountability to regulators and existing or prospective shareholders. The filing may include specific future steps to be taken that are intended to respond to that risk but would occur subsequent to the filing deadline. Filers may also include "forward-looking statements" that describe high-level risk considerations that are more general than the specific risk factors that must be disclosed.

- **Lack of transparency** – A dangerous example of implicit acceptance is one where future treatment is not even planned. Many historical cybersecurity incidents occurred because a risk owner chose to ignore known risks, either because they did not have resources to address them or because they felt that doing so would be costly or burdensome. It is important for enterprise risk managers to foster a risk-aware culture that promotes the need to properly respond to all risk scenarios and to work with risk management partners to address them. For example, it may be possible to revisit the prioritization and look for ways to reallocate resources from other risk decisions in the register. It may also be possible to gain additional resources to properly address the risk, perhaps by using the risk scenario to build a business case for a supplemental resource request.

These examples highlight the fact that all risks receive a response, even if a flawed one, such as ignoring the situation or burying it in a folder for future mitigation. Open and transparent recording and communication support an effective risk management life cycle.

2.3.7 Responding to Positive Risk Scenarios

As has been illustrated throughout the series (and as shown in Figure 7 and Figure 8), both negative and positive risks can be documented and should receive an appropriate response. Some enterprises maintain separate CSRRs and *opportunity* risk registers using both sets of information to evaluate potential impact (both harmful and beneficial) on mission and business objectives. Where positive risks are to be considered and included in risk registers, there are four response types that are generally applied, as described in Table 2.

Table 2: Response Types for Positive Cybersecurity Risks

Type	Description
Exploit	Eliminate uncertainty to make sure that the opportunity is actualized. **Example**: A manager learns that a well-qualified engineer has recently decided to seek new employment and arranges a generous signing bonus in order to ensure that she is able to entice the prospective employee to her team.
Share	Allocate ownership to another party that is better able to capture the opportunity. **Example**: A business unit leader would like to improve identity security through a privileged access management product but does not have a sufficient budget to purchase the tools and services in the current fiscal year. The leader works with a leader from a different business unit who will purchase and implement the tool as a pilot project with plans to later expand installation to support both business units.
Enhance	Increase the probability and positive impact of an opportunity (e.g., invest in or participate with a promising cybersecurity technology). **Example**: An employee has identified an opportunity to automate an existing business process, but it will require an investment in time and equipment to implement. Seeing the positive benefits of such a process, his manager approves overtime labor hours to develop the capability and repurposes existing hardware and software resources to enable to project to proceed.
Accept	Take advantage of opportunities that present themselves (e.g., hire key staff, embrace new cybersecurity technology). **Example**: A Division Chief learns that an employee in another division has developed a new application to automate what has previously been a tedious and manual endeavor and arranges to obtain a copy of the recently authorized internal product to gain a similar advantage.

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

2.4 Finalizing the Cybersecurity Risk Register

Having prioritized the various positive and negative risks based on enterprise drivers and risk factors, the remaining columns of the CSRR may be completed. As with other elements of the register, the enterprise risk strategy and supporting guidance (e.g., policies, procedures, and specific processes) will provide the specific methodologies to be used at each level of the enterprise but will generally follow the methods described below.

2.4.1 Risk Response Cost

Risk Response Type	Risk Response Cost	Risk Response Description	Risk Owner	Status
Accept	$0	No response required	Kira Caldwell	Open
Mitigate	$3.7M	Segment internal networks, Improve backup plans	Jemima Daugherty (Carly Hickman - backup)	Open
Transfer	$125,000	Purchase cybersecurity insurance to reimburse downtime	Mark Winters	Closed
Mitigate	$2M	Implement full-disk encryption of sensitive devices, implement remote tracking	Jeffrey Contreras	Updated

Figure 17: Notional CSRR Excerpt Showing Risk Response Cost Column

Figure 17 illustrates the Risk Response Cost column that contains an estimate of the anticipated cost of performing the selected response. This estimate, expressed in terms of direct financial expense, helps inform consumers of the risk register about the impact (in terms of capital and operating expenses) of performing the response. Inclusion of the anticipated cost enables comparison with the risk exposure rating value and supports a cost-benefit analysis. An estimation of the cost of response against the likely loss exposure had the response not occurred helps support risk decisions.

Since many risk prioritization and optimization activities will be based upon available resources, the risk response cost must be carefully and accurately determined. Many of the analysis techniques described in NISTIR 8286A may also be used to estimate the likely cost of risk treatment. For example:

- Three-point estimation might be used to determine the potential overall costs. Internal or external experts may be consulted to determine the optimistic (or best case) (O), most likely (M), and pessimistic (or worst-case) (P) cost estimates. The expected value of the response cost (EV) can be determined using a simple average of the three numbers ($EV = \frac{P+M+O}{3}$) or by using the *beta* distribution method ($EV = \frac{P+4M+O}{6}$), providing some confidence in the resulting estimate.

- An event tree analysis (ETA) might be used to evaluate the full cost of applying risk treatment. If an ETA was completed for the conditions that led to the risk described, then the subsequent treatment (and full life cycle costs of each) can be estimated more fully.

- A total cost of operations analysis might help avoid a situation where risk practitioners consider only the direct and immediate expense of treating a risk (or pursuing an opportunity). For example, a manager might list the direct cost of a network firewall appliance to mitigate the risk scenario of an external hacker exfiltrating corporate secrets through a web server vulnerability. The response costs should also include hardware and software maintenance of the device, installation, operational labor, and – eventually – secure disposal of that appliance.

The value(s) in the Risk Response column should be comparable to those in the risk assessment columns. For example, if the risk exposure is expressed as a financial range, the risk response cost should be similarly conveyed. The exposure rating value and risk response cost value should use a similar unit of measure. If the estimated impact has been summarized (as in an annualized loss expectancy, or ALE) then the cost should be estimated in similar terms. This consistency supports improved analysis of the cost to treat a given risk scenario against the benefit of doing so.

2.4.2 Risk Response Description

Risk Response Type	Risk Response Cost	Risk Response Description	Risk Owner	Status
Accept	$0	No response required	Kira Caldwell	Open
Mitigate	$3.7M	Segment internal networks, Improve backup plans	Jemima Daugherty (Carly Hickman - backup)	Open
Transfer	$125,000	Purchase cybersecurity insurance to reimburse downtime	Mark Winters	Closed
Mitigate	$2M	Implement full-disk encryption of sensitive devices, implement remote tracking	Jeffrey Contreras	Updated

Figure 18: Notional CSRR Excerpt Showing Risk Response Description Column

The next column in the CSRR, shown in Figure 18, enables a textual description of the response actions that will occur. The format of the text is at the user's discretion, but the explanation should be clear enough to support subsequent aggregation. If the response described explains a risk mitigation response, it may be helpful to convey the specific controls (e.g., from SP 800-53) or other information (e.g., NIST Cybersecurity Framework subcategory) that will be used to achieve that response. Expressing that risk response description in terms of the desired outcome may improve understanding and help to later confirm a successful risk response. For example, in the row describing a risk scenario where a laptop containing sensitive information is lost or stolen, the risk response description cell might state, "Implement full-disk encryption of sensitive devices (as approved by Chief Privacy Officer and Legal Department) to ensure that data on such devices cannot be viewed if the device is lost or stolen."[4]

[4] The risk description might also include references to the specific mechanisms to be used for risk response, such as SP 800-53 control SC-28 or an outcome listed in a profile for NIST Cybersecurity Framework subcategory PR.DS-1.

2.4.3 Risk Owner

Risk Response Type	Risk Response Cost	Risk Response Description	Risk Owner	Status
Accept	$0	No response required	Kira Caldwell	Open
Mitigate	$3.7M	Segment internal networks Improve backup plans	Jemima Daugherty (Carly Hickman - backup)	Open
Transfer	$125,000	Purchase cybersecurity insurance to reimburse downtime	Mark Winters	Closed
Mitigate	$2M	Implement full-disk encryption of sensitive devices, implement remote tracking	Jeffrey Contreras	Updated

Figure 19: Notional CSRR Excerpt Showing Risk Owner Column

The next column in the CSRR, shown in Figure 19, provides for the recording of the personnel and/or organizational element responsible for ensuring that the described risk response is implemented. The selection of who will constitute the risk owner (e.g., an individual, an individual and backup, a personal name and their organization name) is at the discretion of the enterprise but should be consistently used.

The CSRR will usually list the primary point of contact for the cybersecurity risk described, but additional stakeholders might be listed in the Notes section of the RDR, or additional fields could be added to the form itself. Two considerations that often support oversight and risk monitoring include risk escalation and elevation:

- Risk Escalation occurs when a particular threshold is reached, either based on a time frame or some other risk condition, thus requiring a higher level of attention. For example, a risk that has remained through more than two fiscal periods without adequate treatment might be flagged for additional scrutiny. Another condition for escalation might occur if, during risk monitoring, conditions indicate that the risk exposure rating will significantly exceed the initial estimates.

- Risk Elevation is the process of transferring the decisions on risk response to a more senior stakeholder when the factors involved (e.g., a regulatory compliance risk) are particularly sensitive or critical. For example, enterprise risk strategy might direct that any risk with more than $1 million exposure or risks related to a particularly important business application must be managed at a more senior level.

To ensure the consistent application of both types of risk owner transfer, ERM risk strategy should provide clear escalation and elevation criteria. Additional types of personnel (e.g., internal audit, Chief Risk Officer, legal or human relations staff) may have a stake in monitoring and managing each risk but would not be considered to be the risk owner and would likely not need to be listed in the CSRR or RDR.

2.4.4 Status

Risk Response Type	Risk Response Cost	Risk Response Description	Risk Owner	Status
Accept	$0	No response required	Kira Caldwell	Open
Mitigate	$3.7M	Segment internal networks, Improve backup plans	Jemima Daugherty (Carly Hickman - backup)	Open
Transfer	$125,000	Purchase cybersecurity insurance to reimburse downtime	Mark Winters	Closed
Mitigate	$2M	Implement full-disk encryption of sensitive devices, implement remote tracking	Jeffrey Contreras	Updated

Figure 20: Notional CSRR Excerpt Showing Risk Status Column

Status, the final column of the CSRR illustrated in Figure 20, provides an opportunity to record the current state of the risk response. As with other cells, the terms used are at the discretion of the organization, but the options available should be specified in the risk management policy and/or procedures to enable consistent review. For all cells in the CSRR, additional detail may be contained within the detailed risk record, described in NISTIR 8286A.

2.5 Conditioning Cybersecurity Risk Register for Enterprise Risk Rollup

Having completed a system level CSRR, whether through an initial review or a subsequent iteration, the final stage is to condition the entries to help support integration with other system level and organization level CSRRs. Since a key purpose of this artifact is to help organize and communicate information about risks that have been identified, assessed, and treated, that communication will be helped by maximizing the chances that the information can be effectively normalized, aggregated, and understood.

Conditioning actions enable the alignment of activity and reporting regarding CSRM activities. Another key element is the consideration of established enterprise-level criteria for risk reporting. For example, the risk ratings or exposure ratings may need to be transliterated as you move up the chain to allow comparability to other enterprise risks. Details regarding the aggregation and subsequent interpretation of enterprise CSRR information will be provided in NISTIR 8286C.

Conditioning actions also help provide an opportunity for CSRM practitioners to ensure that the information to be conveyed through the CSRR is accurate, complete, and thorough. In support of subsequent comparison to other CSRRs and integration at various levels, examples of alignment considerations for fields in the register include the following:

- Ensure that readers will be able to understand the **risk description** by using clear, concise terminology. For threat-based risks, use a brief and accurate description of the assets affected; threat actors, vectors, and events; vulnerabilities and pre-existing conditions exploited; and the resulting business-based adverse impacts. For positive risk scenarios, ensure that the reader is able to understand who will benefit from the

opportunity and that the CSRR entry describes the conditions necessary to enhance, accept, and realize that benefit.

- **Risk category** and **risk response type** entries should conform to guidance described in the enterprise risk strategy and be consistent with register entries from similar CSRRs at the same level of the enterprise.

- Likelihood, impact, and exposure rating entries within **current assessment** and **risk response** columns should use consistent units of measurement and be easily understood by the reader. If financial values are used, ensure that the currency used is consistent with those of other registers.

It may also be helpful to periodically review the risk detail record for each of the risks in the CSRR and ensure that information there is similarly and fully recorded. Because the RDR provides an opportunity to more fully convey the information that is summarized in the register, the RDR provides a meaningful and important reference to those who will subsequently be informed by it in support of organization and enterprise risk decisions.

Conclusion

As society's dependence on trustworthy information and technology increases, CSRM activities to properly treat security, privacy, supply chain, and other information-related risks remain critical considerations at all levels of the enterprise. Since resources are nearly always limited, it is vital that CSRM work at all levels is coordinated and prioritized to maximize effectiveness and ensure that the most critical needs are adequately addressed.

The activities described in the previous sections will help build on the risk strategy, identification, and analysis described in NISTIR 8286A. Risk prioritization, risk response, and risk aggregation will similarly support the normalization, aggregation, and optimization of risk information to help guide enterprise risk decision-making and ensure that key stakeholders are informed of known or potential risk factors.

The activities throughout this series are not intended to replace the extensive guidance provided by NIST and a large array of other risk management practitioners. Rather, the authors of this series hope to better amplify the benefits of CSRM work by supporting the consistent application of CSRM activities, enabling management and leadership understanding of the rationale and benefit of those activities, and supporting improved communications and measurement of the results of those activities.

For many years, NIST and other entities have encouraged senior leaders (in both public- and private-sector enterprises) to become more engaged with information- and technology-related risk management and for governing bodies to treat those risks in the same way they do other key components of their enterprises' risk universe. Because many leaders have answered that call to action, the cybersecurity community has an opportunity to show how CSRM activities help apply internal controls to continually achieve enterprise risk objectives. The integration and communication of risk information helps leaders effectively exploit opportunities and adeptly respond to unacceptable risks. Through effective prioritization and response based on detailed and accurate risk analysis, managers throughout the enterprise will be able to navigate a changing risk landscape and take advantage of new and exciting innovation.

References

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

[2] 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

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

[4] 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

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

[6] The Open Group (2020) Risk Analysis (O-RA), Version 2.0 (OpenFAIR). Available at https://publications.opengroup.org/standards/open-fair-standards/c20a.

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

[8] The European Union Agency for Cybersecurity (ENISA) Glossary of Risk Management Terms. Available at https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/glossary

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

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

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

1153

Appendix A—Acronyms

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

ALE	Annualized Loss Expectancy
CSRM	Cybersecurity Risk Management
CSRR	Cybersecurity Risk Register
CVSS	Common Vulnerability Scoring System
ERM	Enterprise Risk Management
ETA	Event Tree Analysis
GRC	Governance, Risk, and Compliance
I&T	Information and Technology
ISP	Internet Service Provider
ISRM	Information Security Risk Management
ITL	Information Technology Laboratory
KPI	Key Performance Indicator
KRI	Key Risk Indicator
MEA	Monitor-Evaluate-Adjust cycle
NIST	National Institute of Standards and Technology
NISTIR	NIST Interagency or Internal Report
OMB	Office of Management and Budget
OpenFAIR	Open Group Risk Analysis and Taxonomy based on the Factor Analysis of Information Risk (FAIR)
POA&M	Plan of Action and Milestones
RDR	Risk Detail Record
RTO	Recovery Time Objective
SLA	Service Level Agreement
SWOT	Strength, Weakness, Opportunity, and Threat Analysis