NISTIR 8286A

Identifying and Estimating Cybersecurity Risk for Enterprise Risk Management

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

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

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

NISTIR 8286A

Identifying and Estimating Cybersecurity Risk for Enterprise Risk Management

Stephen Quinn
Computer Security Division
Information Technology Laboratory

Matthew Barrett
CyberESI Consulting Group, Inc.
Baltimore, MD

Nahla Ivy
Enterprise Risk Management Office
Office of Financial Resource Management

Larry Feldman
Greg Witte
Huntington Ingalls Industries
Annapolis Junction, MD

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

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

November 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 8286A
61 pages (November 2021)

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

Comments on this publication may be submitted to:

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

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 supplements NIST Interagency or Internal Report 8286, *Integrating Cybersecurity and Enterprise Risk Management (ERM)*, by providing additional detail regarding risk guidance, identification, and analysis. This report offers examples and information to illustrate risk tolerance, risk appetite, and methods for determining risks in that context. To support the development of an Enterprise Risk Register, this report describes documentation of various scenarios based on the potential impact of threats and vulnerabilities on enterprise assets. Documenting the likelihood and impact of various threat events through cybersecurity risk registers integrated into an enterprise risk profile helps to later prioritize and communicate enterprise cybersecurity risk response and monitoring.

Keywords

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

Acknowledgments

The authors wish to thank all individuals, organizations, and enterprises that contributed to the creation of this document. This includes Lisa Carnahan, Amy Mahn, Chris Enloe, Santi Kiran, Matt Scholl, and Kevin Stine of NIST; Matthew Smith and Daniel Topper of Huntington Ingalls Industries; Mat Heyman of Impresa Management Solutions. Organizations and individuals who provided feedback on the public comment drafts include: David Austin of Bible.org; Julie Chua, Linda Esah, Elizabeth Flaim, Kim Isaac, Nnake Nweke, Brent Roddy, Nicole Rohloff, and Musarat Qadri Shaikh of the Cyber-ERM Community of Interest; Melanie Tiano of CTIA; Frederick Doyle of CubicPrism Analytics, Inc.; Alicia Jones of Entergy Services, Inc.; Luke Bader of FAIR Institute; Bernice Harvey of Harvey Consulting & Training LLC; Janet Anderson of the National Security Agency, Kelly Hood and Tom Conkle of Optic Cyber Solutions; Amy Hamilton of the U.S. Department of Energy; the Executive Secretariat of the U.S. Department of Energy; and the U.S. Department of Health and Human Services Team; individual contributors include Louise Dandonneau and Carmen Estigarribia.

Audience

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

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

This document begins with information generated at the Enterprise Level of the organization and frames the discussion and the response from the risk management practitioners. All readers are expected to gain an improved understanding of how cybersecurity risk management (CSRM) and ERM complement and relate to each other, as well as the benefits of integrating their use.

Document Conventions

For the purposes of this document, the terms "cybersecurity" and "information security" are used interchangeably, as are the terms Cybersecurity Risk Management (CSRM) and Information Security Risk Management (ISRM).

Patent Disclosure Notice

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

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

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

Executive Summary

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

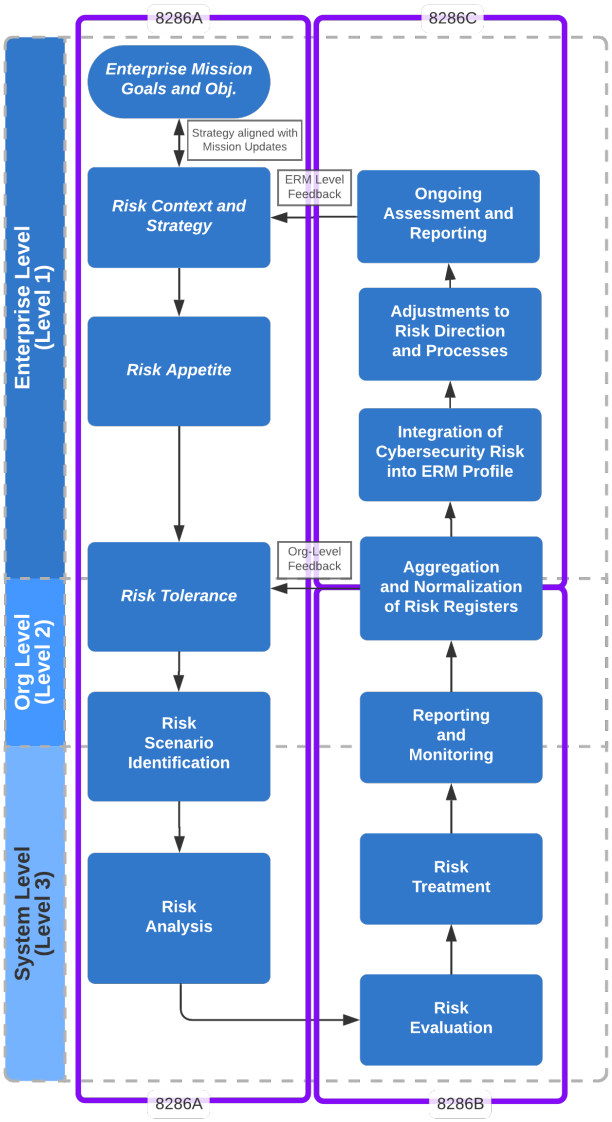

Figure 1: NISTIR 8286 Series Publications Describe Detailed CSRM/ERM Integration

This report highlights aspects of cybersecurity risk management (CSRM) inherent to enterprises, organizations, and systems. The terms *organization* and *enterprise* are often used interchangeably; however, without an understanding of organizational structure, effective risk management is impossible. For the purposes of this document, an *organization* is defined as an entity of any size, complexity, or position within a larger organizational structure. The *enterprise* exists at 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] This report describes CSRM activities at each level, as illustrated in Figure 1. Note that there may be iterative levels within the enterprise and that positions may be relative. For example, a given enterprise (e.g., a bureau or corporate division) may represent an organization to the overarching agency or corporation.

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

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

[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."

publication in the series, illustrated in Figure 1, provides additional detail and guidance to supplement topics in that document:

- NISTIR 8286A (this report) provides additional detail regarding risk context, scenario identification, and analysis of likelihood and impact. It also includes methods to convey risk information, such as through cybersecurity risk registers (CSRRs) and risk detail records (RDRs). Similar processes, and the general use of risk registers, are helpful to identify and manage other types of risk, including those for Cyber Supply Chain and Privacy.

- NISTIR 8286B describes ways to apply risk analysis to prioritize cybersecurity risk, evaluate and select appropriate risk response, 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 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 CSRM success factor is setting leadership expectations, such as through risk appetite and risk tolerance. Section 2.1 of this report provides examples of setting and communicating those expectations and provides input into Section 2.2, which describes methods for identifying CSRM scenarios. Each of the potential risk scenarios are analyzed, as described in Section 2.3, to consider specific likelihood and impact on the organization. Throughout these processes, risk data is developed and recorded in cybersecurity risk registers (and risk detail records) in support of ongoing risk communication. This information becomes the input to risk prioritization and response, which is described in NISTIR 8286B.

Table of Contents

List of Appendices

List of Figures

List of Tables

1 Introduction

This report provides guidance that supplements NIST Interagency/Internal Report (NISTIR) 8286, *Integrating Cybersecurity and Enterprise Risk Management (ERM)* [1]. This is the first 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.

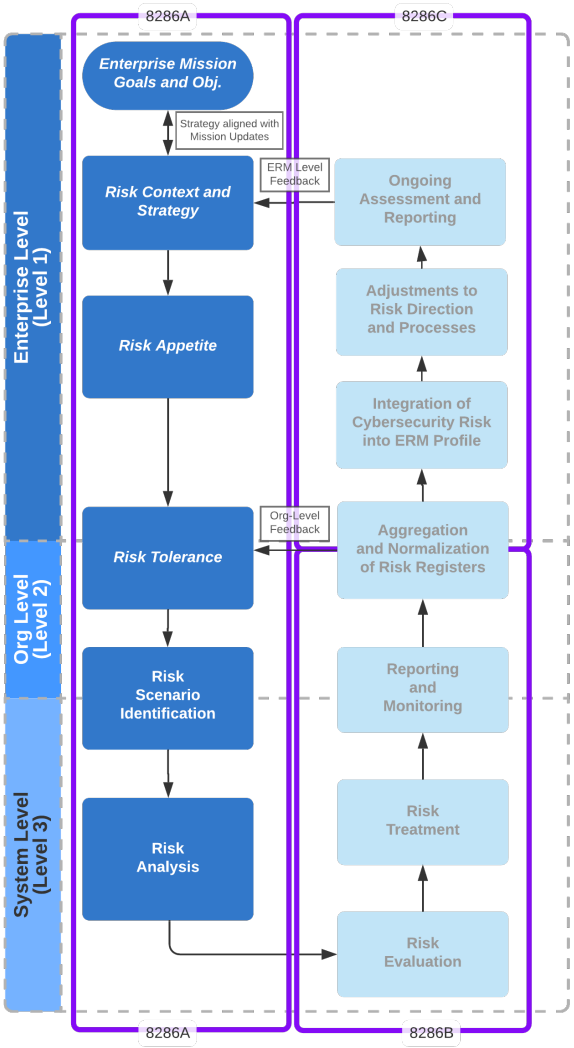

Figure 2: NISTIR 8286A Activities as Part of CSRM/ERM Integration

Each publication in the series, as illustrated in Figure 2, provides detailed guidance to supplement topics in the flagship document. Activities described in this report are shown in dark blue boxes; those in other documents are shown in light blue boxes. This report describes CSRM activities at each level, as illustrated in Figure 1. Note that there may be iterative levels within the enterprise and that positions may be relative. For example, a given enterprise (e.g., a bureau or corporate division) may represent an organization to the overarching agency or corporation.

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

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

- NISTIR 8286C 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,

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

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 an organization as an entity of any size, complexity, or position within a larger organizational structure (e.g., a federal agency or company). It defines an *enterprise* as having a structural hierarchy and senior leaders that bear fiduciary management and reporting responsibilities, including establishing risk strategy (e.g., risk appetite, methods).[3] Notably, government and private industry CSRM and ERM programs have different oversight and reporting requirements (e.g., accountability to the public versus accountability to shareholders), but the general needs and processes are quite similar.

1.1 Supporting CSRM as an Integrated Component of ERM

There are similarities and variances among approaches by public- and private-sector practices for ERM/CSRM coordination and interaction. Some entities incorrectly treat ERM and CSRM practices as separate stovepipes. The CSRM program is an integral part of the ERM portfolio, both taking its direction from ERM and informing it. The universe of risks facing an enterprise includes many factors, and risks to the enterprise's information and technology often rank high within that list. ERM strategy and CSRM strategy are not divergent; CSRM strategy should be a subset of ERM strategy with particular objectives, processes, and reporting. This

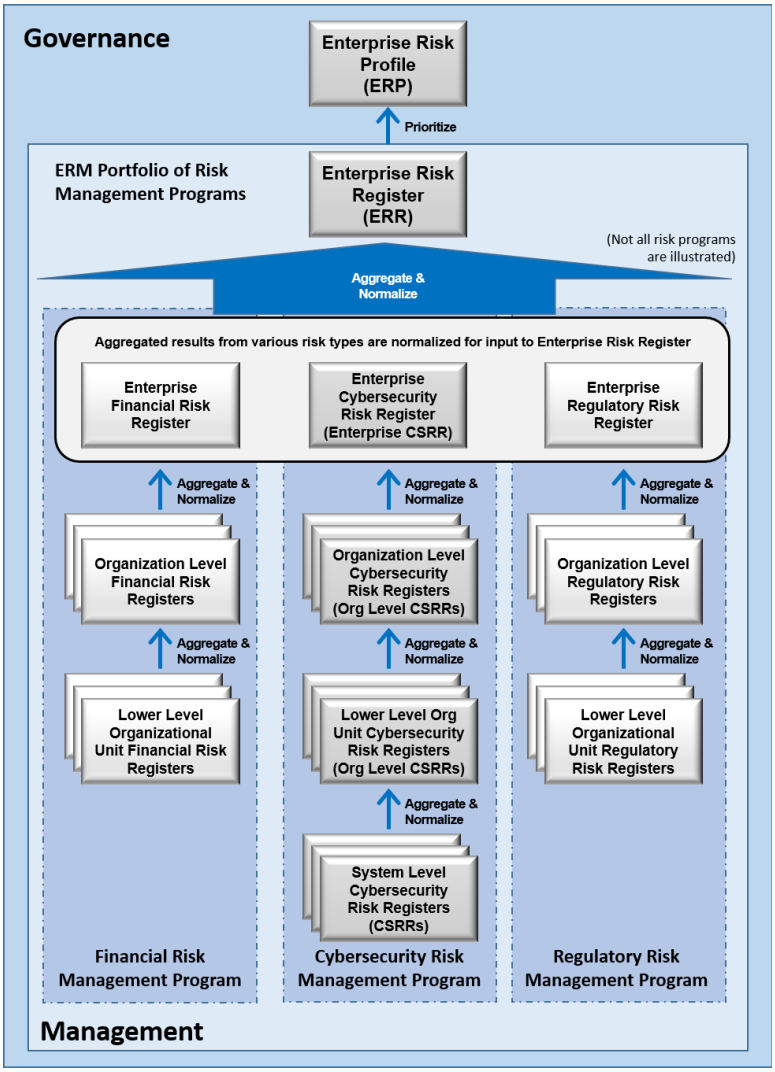

Figure 3: Integration of Various Risk Management Activities into the Enterprise Risk Register and Risk Profile

[3] This report refers to the term *enterprise* in two contexts, referencing both the top level of a hierarchical organization and also to represent the organization itself. Generally, the phrase *enterprise level* refers to governance and management activities at the most senior levels of that hierarchy (sometimes referenced as Level 1 in other NIST publications) while the phrase *the enterprise* references the entirety of the organization.

report and those in this series support improving ERM and CSRM coordination. As the risk management community continues that discussion, NIST will solicit and publish lessons learned and shared by that community.

Section 2 shows that enterprise governance activities direct the strategy and methods for risk management, including CSRM. Results of those activities are recorded in various risk registers. Cybersecurity risks, derived from system level assessments, are documented through cybersecurity risk registers (CSRRs) that are aggregated and used to create an *enterprise* cybersecurity risk register (Enterprise CSRR) that, in turn, becomes part of a broader Enterprise Risk Register (ERR), as depicted in Figure 3. The ERR, when prioritized by those with fiduciary and oversight responsibilities, represents an Enterprise Risk Profile. Figure 3 illustrates the integration of risk register information and demonstrates that ERM and CSRM are not separate processes, but CSRM represents an important subset of risk management under the broader umbrella of enterprise risk management.

The NISTIR 8286 series builds upon existing NIST frameworks by demonstrating methods for applying risk management processes at all enterprise levels and representing how the NIST frameworks are anchored in ERM. A key construct for performing that integration is the cybersecurity risk register (CSRR) described in NISTIR 8286.[4] As shown in Figure 3, the risk register is a key tool to document, communicate, and manage cybersecurity risk at each level of the enterprise.[5] Use of this process streamlines risk reporting, eliminates duplicate record keeping, and helps share CSRM knowledge across program areas.

NISTIR 8286A details methods for completing and maintaining that risk register by identifying threats and analyzing the likelihood of successful exploitation of certain conditions that result in threat events, the estimated impact on enterprise objectives, and whether estimates are within established risk tolerance parameters. This report focuses on the first three elements of the enterprise CSRM process: establishing scope, context, and criteria; identifying the cybersecurity-related risks that may affect an enterprise's ability to achieve its objectives; and calculating the likelihood and impact of such risks. Subsequent publications address methods for evaluating risk treatment options, selecting an appropriate treatment, communicating the plans and results of that treatment, and adhering to stakeholders' risk strategies.

1.2 Purpose and Scope

This document focuses on improving CSRM understanding and communications between and among cybersecurity professionals, high-level executives, and corporate officers to help ensure the effective integration of cybersecurity considerations as a critical subset of overarching enterprise risks. The processes that will be described support improved coordination among ERM champions and liaisons. The report recognizes that the risk management community has observed an opportunity for increased rigor in the manner in which cybersecurity risk

[4] Although this report is focused on CSRM as a function of ERM, future iterations of this report and documents in this series will address other risk management disciplines (e.g., Privacy RM, Supply Chain RM) using the risk register model.

[5] Figure 1 of NISTIR 8286 provides an illustration of the various levels of an entity including the enterprise, organization, and system levels. Activities at these levels are further described in this NISTIR 8286A report.

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:

- Help describe governance processes by which senior leaders build strategy and express expectations regarding CSRM as part of ERM and
- Provide guidance for CSRM practitioners in applying the risk direction received from senior leaders, communicating results, coordinating success, and integrating activities.

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 [2]. It builds upon concepts introduced in NISTIR 8286 and complements other documents in this series. It references some materials that are specifically intended for use by federal agencies and will be highlighted as such, but the concepts and approaches are intended to be useful for all enterprises.

1.3 Document Structure

This publication helps establish an enterprise strategy (Section 2.1) to identify cybersecurity risks to mission objectives (Section 2.2) and to analyze (Section 2.3) their likelihood and possible impacts. These sections describe ordinary methods in which that strategy is expressed through risk appetite and risk tolerance. The remainder of this document is organized into the following major sections:[6]

- Section 2 details CSRM considerations, including enterprise risk strategy for risk identification and risk analysis.
- Section 3 provides a short summary and conclusion.
- The References section provides links to external sites or publications that provide additional information.
- Appendix A contains acronyms used in the document.
- Appendix B provides a notional representation of a Risk Detail Record.

[6] An Informative Reference that crosswalks the contents of this document and the NIST Framework for Improving Critical Infrastructure Cybersecurity (the NIST Cybersecurity Framework) will be posted as part of the National Cybersecurity Online Informative References (OLIR) Program [3]. See https://www.nist.gov/cyberframework/informative-references for an overview of OLIR.

2 Cybersecurity Risk Considerations Throughout the ERM Process

Because digital information and technology are valuable enablers for enterprise success and growth, they must be sufficiently protected from various types of risk. Government entities for whom growth may not be a strategic objective are still likely to find value in dynamically adding or changing their services or offerings as their constituents' needs evolve. Thus, both private and public sector entities need to evaluate the role of information and technology in achieving enterprise objectives. This understanding enables a deeper consideration of the various uncertainties that jeopardize those objectives.

In the context of ERM, senior leaders must clearly express expectations regarding how risk should be managed. Those expectations provide CSRM practitioners with objectives for managing cybersecurity risks, including methods for reporting the extent to which risk management activities successfully achieve those objectives. The document for recording and sharing information about those risks is the cybersecurity risk register (CSRR).

NISTIR 8286 describes the use of risk registers, example fields for those registers, and the fact that prioritized risk register contents serve as the basis of a risk profile. That report also states that, while a risk register represents various risks at a single point in time, it is important for the enterprise to ensure that the model is used in a consistent and iterative way. As risks are identified (including calculation of likelihood and impact), the risk register will be populated with relevant information once decisions have been made. As risk responses are applied to each item in the risk register, the updated state of that risk will become the new current state in the next assessment cycle. Risk management policy designates which roles are appropriate for completing the CSRR at each level.

Figure 4 provides an example of a blank risk register. The red box shows fields that are relevant to the processes described in this report. The remaining columns are described in NISTIR 8286B. Note that, while prioritization is informed by some of the information recorded in these columns, risk priority is also discussed in NISTIR 8286B in support of Risk Evaluation and Risk Response activities. While the example illustrates a notional template for cybersecurity risks, a similar template could be used for any type of risk in the enterprise.

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

The risk register provides an easily consumed summary for understanding the risk landscape, but effective risk communication requires many additional details that would not fit into this compact table. The additional information should be recorded in a Risk Detail Record (RDR) and be readily available should the additional detail be required about a risk register entry. The RDR provides an opportunity to record historical risk-related information, detailed risk analysis data, and information about individual and organizational accountability. Appendix B of this document provides a notional example of such a record.

2.1 Risk Scope, Context, and Criteria

Effective management of risk throughout the enterprise depends upon collaboration and cooperation at each level. After senior leaders provide direction regarding how to manage risks (including cybersecurity risks), personnel at other levels use that direction to achieve, report, and monitor outcomes. This top-down, collaborative management approach helps ensure that CSRM strategy is formulated as a part of (and flows from) ERM strategy.

ISO 31000:2018 points out that there are three prerequisites for supporting a CSRM program as an input to ERM [4]:

- The *scope* of the CSRM activities should be defined;
- The internal and external *context* of the CSRM activities should be determined; and
- The criteria from enterprise stakeholders should be declared and documented through a comprehensive CSRM *strategy*.

The guidance in the NISTIR 8286 series relies upon these elements (scope, context, and strategy) being established. Senior leaders define the ERM scope, context, and strategy, which inform enterprise priorities, resource utilization criteria, and responsibilities for various enterprise roles. The ERM strategy helps define how various organizational systems, processes, and activities cooperate to achieve risk management goals, including those for CSRM, in alignment with mission objectives.

2.1.1 Risk Appetite and Risk Tolerance

CSRM, as an important component of ERM, helps assure that cybersecurity risks do not hinder established enterprise mission objectives. CSRM also helps ensure that exposure from cybersecurity risk remains within the limits assigned by enterprise leadership. Figure 5 illustrates the ongoing communications among ERM and CSRM stakeholders to set, achieve, and report on risk expectations throughout the enterprise. The diagram extends the Notional Information and Decision Flows figure from the NIST *Framework for Improving Critical Infrastructure Cybersecurity* (Cybersecurity Framework) by indicating risk appetite and risk tolerance definition, interpretation, and achievement [5].

The process described in Figure 5 illustrates that *risk appetite* regarding cybersecurity risks is declared at the Enterprise Level. Risk appetite provides a guidepost to the types and amount of risk, on a broad level, that senior leaders are willing to accept in pursuit of mission objectives

and enterprise value.[7] Risk appetite may be qualitative or quantitative. As leaders establish an organizational structure, business processes, and systems to accomplish enterprise mission objectives, the results define the structure and expectations for CSRM at all levels.[8] Based on these expectations, cybersecurity risks are identified, managed, and reported through risk registers and relevant metrics. The register then directly supports the refinement of risk strategy considering mission objectives.

Risk appetite can be interpreted by enterprise- and organization-level leaders to develop specific cybersecurity *risk tolerance*, which is defined by OMB as "the acceptable level of variance in performance relative to the achievement of objectives" [2]. Risk tolerance represents the specific level of performance risk deemed acceptable within the risk appetite set by senior leadership (while recognizing that such tolerance can be influenced by legal or regulatory requirements).[9] Risk tolerance can be defined at the executive level (e.g., at the department level for U.S. federal agencies), but OMB offers a bit of discretion to an organization, stating that risk tolerance is "generally established at the program, objective, or component level."[10]

Risk appetite and risk tolerance are related but distinct in a similar manner to the relationship between governance and management activities. Where risk appetite statements define the overarching risk guidance, risk tolerance statements define the specific application of that direction. This means risk tolerance statements are always more specific than the corresponding risk appetite statements. Together, these risk appetite and risk tolerance statements represent risk limits, help communicate risk expectations, and improve the focus of risk management efforts. They also help to address other factors such as findings from internal audits or external reports (e.g., an examination of corporate financial records by an independent audit firm, a review of a federal agency's improved IT management through the Federal Information Technology Acquisition Reform Act [FITARA]). The definition of these risk parameters places the enterprise in a better position to identify, prioritize, treat, and monitor risks that may lead to unacceptable loss. Risk tolerance should always stay within the boundaries established by senior leadership.

Achievement of defined expectations is conveyed through risk registers that document and communicate risk decisions. Risk assessment results and risk response actions at the system level are reflected in CSRRs. As CSRRs from multiple systems are collated and provided to higher level business managers at the organization level, those managers can evaluate results and refine risk tolerance criteria to optimize value delivery, resource utilization, and risk. The enterprise level aggregation of all of the various CSRRs enables senior leaders to monitor risk response

---

7 NISTIR 8286 supports the OMB Circular A-123 definition of risk appetite as "the broad-based amount of risk an organization is willing to accept in pursuit of its mission/vision. It is established by the organization's most senior level leadership and serves as the guidepost to set strategy and select objectives." [2]

8 The term "system" throughout this publication pertains to information systems, which are discrete sets of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information, whether such information is in digital or non-digital form.

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

10 Examples of the organization level include business units, company departments, or agency divisions.

considering the expectations set. Figure 2 illustrates the tight coupling of ERM, where senior leaders set enterprise risk strategy and make risk-informed decisions, and CSRM, where cybersecurity practitioners can best identify where cybersecurity risk is likely to occur. Table 1 provides examples of actionable, measurable risk tolerance that illustrates the application of risk appetite to specific contexts within the organization level structure.

Table 1: Notional Examples of Risk Appetite and Risk Tolerance

Example Enterprise Type	Example Risk Appetite Statement	Example Risk Tolerance Statement
Global Retail Firm	Our customers associate reliability with our company's performance, so service disruptions must be minimized for any customer-facing websites.	Regional managers may permit website outages lasting up to 4 hours for no more than 5 % of its customers.
Government Agency	Mission-critical systems must be protected from known cybersecurity vulnerabilities.	Systems designated as mission-critical must be patched against critical software vulnerabilities (severity score of 10) within 14 days of discovery.
Internet Service Provider	The company has a low risk appetite with regard to failure to meet customer service level agreements, including network availability and communication speeds.	Patches must be applied within deadlines to avoid attack-related outages but also must be well-tested and deployed in a manner that does not reduce availability below agreed-upon service levels.
Academic Institution	The institution understands that mobile computers are a necessary part of the daily life of students, and some loss is expected. The leadership, however, has no appetite for the loss of any sensitive data (as defined by the Data Classification Policy).	Because the cost of loss prevention for students' laptop workstations is likely to exceed the cost of the devices, it is acceptable for up to 10 % to be misplaced or stolen if and only if sensitive institution information is prohibited from being stored on students' devices.
Healthcare Provider	The Board of Directors has decided that the enterprise has a low risk appetite for any cybersecurity exposures caused by inadequate access control or authentication processes.	There will always be some devices that do not yet support advanced authentication, but 100 % of critical healthcare business applications must use multi-factor authentication.

These discussions may also help identify positive risks in the form of opportunities. From an opportunity standpoint, the risk appetite statements can identify areas where the organization needs to stretch further to reach goals and are expressed as those targeted areas where some loss is acceptable without crossing important lines of demarcation (e.g., innovative solutions should be pursued but not at the cost of life, safety, compliance with laws/regulations, or reputation). Understanding that private sector organizations pursue risk as part of their growth strategies and competitive advantage, this aspect should not be forgotten. Similarly, public sector agencies typically have stretch goals to keep up with industry needs, customer expectations, market demands, or other influences.

2.1.2 Enterprise Strategy for Cybersecurity Risk Coordination

Figures 5 and 6 provide simplified illustrations of risk integration and coordination activities. Each enterprise is unique, so enterprise leadership may wish to tailor the approach for those unique circumstances. For example, while risk appetite statements usually originate from the most senior leaders, those leaders may choose to delegate the creation of cybersecurity risk appetite statements to a senior cybersecurity risk official (e.g., Chief Information Security Officer, or CISO). Readers should note that the processes described are cyclical. Early iterations may include the definition of terms, strategies, and objectives. Subsequent iterations may focus on refining those objectives based on previous results, observations of the risk landscape, and changes within the enterprise.

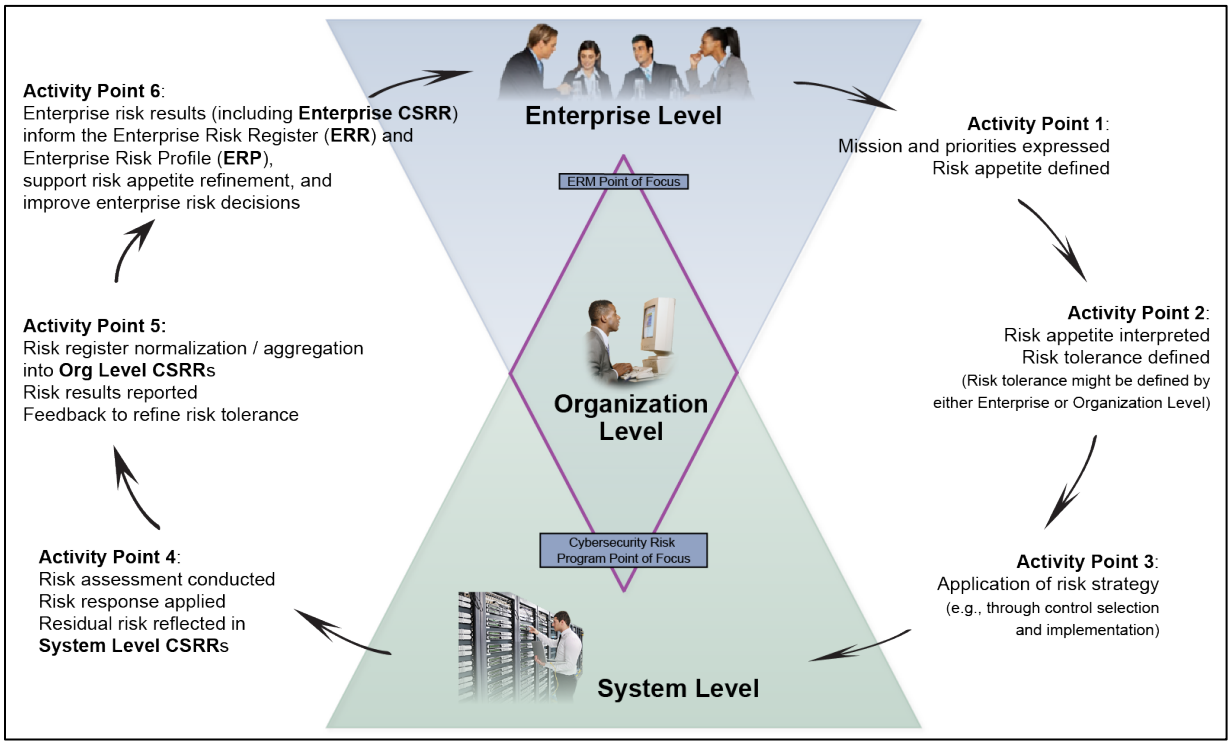

Figure 5: Illustration of Enterprise Risk and Coordination[11]

Table 2 describes the process by which senior leaders express strategy and expectations for managing cybersecurity risk throughout the enterprise. In general, NISTIR 8286A addresses activity points 1 to 3, and NISTIRs 8286B and 8286C address activity points 4 to 6.

[11] Figure 6 further decomposes the risk management cycle, information flow, and decision points illustrated in Figure 5, which provides a high-level understanding in the context of the organizational structure. Subsequent publications in this series provide additional information about the activities described in Figure 5 and Table 2.

Table 2: Inputs and Outputs for ERM Governance and Integrated CSRM

Activity Point	Inputs	Outputs
1. Setting risk expectations and priorities	Internal and external risk context; enterprise roles and responsibilities; governance framework and governance systems for managing risk for all types of risks	Documentation of enterprise priorities in light of mission objectives and stakeholder values; direction regarding budget (e.g., authorization for capital and operating expenditures); risk appetite statements pertaining to each risk management discipline, including cybersecurity
2. Interpreting risk appetite to define risk tolerance statements	Enterprise priorities in light of mission objectives and stakeholder values; direction regarding budget (e.g., authorization for capital and operating expenditures); risk appetite statements	Risk tolerance statements (and metrics) to apply risk appetite direction at the organization level; direction regarding methods to apply CSRM (e.g., centralized services, compliance/auditing methods, shared controls to be inherited and applied at the system level)
3. Applying risk tolerance statements to achieve system level CSRM	Risk tolerance statements; direction regarding shared services and controls; lessons learned from previous CSRM implementation (and those of peers)	Inputs to preparatory activities; system categorization; selection and implementation of system security controls
4. Assessing CSRM and reporting system level risk response through **CSRRs**	Security plans; risk response; system authorization (or denial of authorization with referral back for plan revision)	Risk assessment results; **CSRRs** describing residual risk and response actions taken; risk categorization and metrics that support ongoing assessment, authorization, and continuous monitoring
5. Aggregating **organization level CSRRs**	CSRRs showing system level risk decisions and metrics; internal reports from compliance/auditing processes to confirm alignment with enterprise risk strategy; observations regarding CSRM achievement in light of risk strategy	**CSRRs** aggregated and normalized based on enterprise-defined risk categories and measurement criteria; refinement of risk tolerance statements, if needed, to ensure balance among value, resources, and risk
6. Integrating CSRRs into **Enterprise CSRR**, Enterprise Risk Register **(ERR)**, and Enterprise Risk Profile (**ERP**)	Normalized and harmonized CSRRs from various organization level CSRM reports; compliance and audit reports; results from other (non-cybersecurity) risk management activities; observations regarding ERM and CSRM achievement	Aggregated and normalized **Enterprise CSRR**; integrated Enterprise Risk Register (**ERR**) aligning CSRM results with those of other risk categories; refinement of risk appetite tolerance statements and risk management direction to ensure balance among value, resources, and risk; Enterprise Risk Profile (**ERP**) for monitoring and reporting overall risk management activities and results

Figure 6 illustrates a more detailed information flow of inputs and outputs. Senior leaders and business managers define risk tolerance direction that is applied at the system level. System level practitioners interpret those risk tolerance statements and apply CSRM activities to achieve risk management objectives. The results are then reviewed to confirm effectiveness, highlight opportunities for improvement, and identify important trends that might require organization or

enterprise level action. The specific process activities will be based on the risk management methods applied but will generally include those below.

The process described in Figure 6 highlights the integration of ERM and CSRM, achieving the high-level process from Figure 5 above, where cybersecurity risks are documented through CSRRs, aggregated at appropriate levels, then used to create an enterprise cybersecurity risk register, which provides input into the broader Enterprise Risk Register (ERR). This integration is described in more detail in NISTIR 8286C.

2.1.3 Detailed Risk Integration Strategy

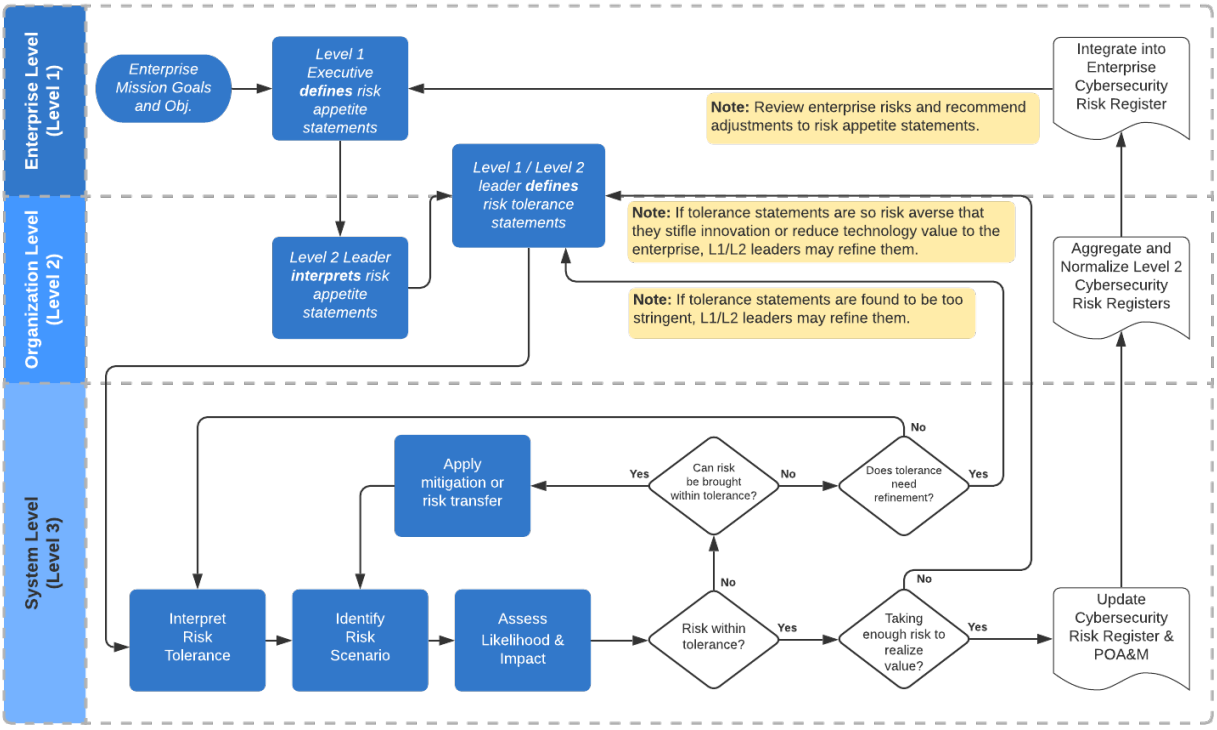

Figure 6: Continuous Interaction Between ERM and CSRM Using the Risk Register[12]

The activities in Figure 6 are listed below.[13]

Risk Context and Strategy Activities

- As described in earlier portions of this section, leaders at Levels 1 and 2 define specific and measurable risk appetite and risk tolerance statements that reinforce enterprise mission objectives and organization goals.

[12] Figure 6 demonstrates select communications, processes, and decisions germane to the risk appetite, risk tolerance, and risk register interactions among the three levels of an enterprise addressed by this report and is not intended to be exhaustive.

[13] For those topics that are addressed in NISTIR 8286A, a pointer to the relevant section is included. NISTIR 8286B describes how to apply risk analysis to prioritize risks and implement appropriate responses. NISTIR 8286C provides guidance regarding aggregation of risks into the Enterprise CSRR and subsequent risk monitoring and communications, including adjustments to risk appetite and risk tolerance based upon previous results and the evolving risk landscape.

- At Level 3, practitioners interpret the risk tolerance statements for the information and technology assets, processes, and activities which may support mission-essential delivery operations. Those in various roles (e.g., system owners, security officers) work together to derive system level requirements for confidentiality, integrity, and availability.

Risk Identification Activities

- The value of each asset of a given system (e.g., information type, technical component, personnel, service provider) is appraised to determine how critical or sensitive it is to the operation of the system (see Section 2.2.1). Subsequent risk decisions depend on an accurate understanding of the importance of each resource to the system.

- For each of these components, the practitioner identifies threat sources that might have a harmful effect (see Section 2.2.2) and the vulnerabilities or conditions that might enable such an effect (see Section 2.2.3). To complete development of the risk scenario, the practitioner determines the adverse effect of the threat source exploiting the vulnerable conditions. The scenario is recorded in the CSRR as the "Risk Description" (see Section 2.2.5). The category for the scenario will be recorded in the "Risk Category" column based on enterprise criteria to support risk correlation, aggregation, and reporting.

Risk Analysis Activities

- The practitioner performs risk analysis (see Section 2.3) to determine the likelihood that the threat events and vulnerable conditions would result in harmful impacts to the system asset. Similarly, the practitioner analyzes the impact value and calculates the risk exposure using the methodology defined in the enterprise risk strategy (e.g., as the product of [risk likelihood] x [risk impact].) The results of these analyses are recorded in the CSRR's "Current Assessment" column as "Likelihood," "Impact," and "Exposure."

Risk Response Activities

- The determined exposure is compared with the risk tolerance.
    - If exposure is within risk tolerance limits, the risk may be "**accepted**."
- If exposure exceeds tolerable levels of risk, practitioners can consider whether they can achieve risk tolerance through other forms of risk response.
    - In many cases, security controls may be applied to **mitigate** risk by reducing the likelihood or impact of a risk to a tolerable level. Controls should be implemented with a corresponding performance scale (i.e., key performance indicator, or KPI) which is used as the basis for key risk indicators (KRIs).
    - Risk response may also include risk **transfer**, also known as risk sharing. For example, an organization might hire an external organization to process sensitive transactions (e.g., payment card transactions), thus reducing the likelihood that

such sensitive data would be processed by an in-house system. Another common risk transfer method involves the use of cybersecurity insurance policies that can help reduce the economic impact if a risk event occurs.

- In some cases, it might be determined that the exposure exceeds risk tolerance and cannot be brought within limits through any combination of mitigation or risk transfer. In this case, practitioners (e.g., the system owner) may need to work with Level 2 leaders to revisit the risk tolerance itself. This negotiation presents an opportunity for the Level 2 and Level 3 managers to determine the best course of action to refine risk direction in light of mission objectives (e.g., through an exception process, an adjustment to the risk tolerance statement, or increased security requirements for the relevant system). In any case, stakeholders will have applied a proactive approach to balancing risk and value.

- If an unacceptable cybersecurity risk cannot be adequately treated in a cost-effective manner, that risk must be **avoided**. Such a condition may require significant redesign of the system or service. These circumstances should be rare, and they highlight the value of CSRM coordination early in the system engineering process. Notably, risk avoidance is not the same as ignoring a risk.

Risk Monitoring and Communication Activities

- KRIs inform organizations whether controls are adequately addressing risk and whether risks are changing over time. When KRIs fall outside of pre-established thresholds, this indicates a risk response is beyond acceptable levels. In this case, organizations should evaluate risks and make any necessary adjustments to controls.

- Results of risk activities and decisions are recorded in the CSRR and, if applicable, in a documented Plan of Actions & Milestones (POA&M)[14] that records agreed-upon future risk activities.

- It is important for enterprise processes to ensure adequate communication of risk that has been accepted (or risk that is implicitly accepted, such as through the exception example above). A key purpose of the various risk registers and reporting methods is to ensure that adequate governance information is available to monitor enterprise risk decisions.

- Risk activities may also be informed through the integration of relevant internal and external audit findings. Significant audit findings often have enterprise level impacts; however, lower severity findings may, if not addressed adequately, spread through multiple systems to create risk in aggregate. The coordination of audit findings may span multiple levels of the enterprise. For example, as operational teams at the system level

[14] Federal agencies are required by OMB to develop a plan of action and milestones (POA&M) for each system. The plan includes a listing of unaccepted risks and associated plans to mitigate the risks. However, the time horizon to resolve outstanding risks may exceed the current reporting cycle. Through regulation, many private industry enterprises are also required to document this type of risk in similar ways (e.g., quarterly SEC Form Q-10 filings, a prospectus). POA&Ms will be addressed in greater detail later in this series when risk mitigation strategies are discussed.

address shortcomings or system deficiencies, key findings might be communicated and tracked by an audit committee (organization level). As responses to findings occur and are documented (such as through a corrective action plan, or CAP), they assist in the planning of subsequent enterprise risk management.

- The process continues until all information and technology assets and processes have been evaluated for risk from currently understood threats and vulnerabilities. For some enterprises, the composite set of system risks (as recorded in the CSRR), risk responses applied, agreements regarding additional CSRM actions to be taken (e.g., as recorded in the POA&M), and other relevant artifacts will be reviewed by a senior official to confirm that risk decisions and risk responses align with risk tolerance and risk appetite directives. For federal government agencies, this represents the system authorization process.

- Subsequently, CSRRs from throughout the business level are normalized and aggregated to provide a composite view of the risk posture and decisions for that organization. As Level 2 managers consider feedback from system CSRM activities, they may decide to refine risk tolerance levels. It may be that the aggregate risk across multiple systems represents too great an exposure and needs to be reduced. In other cases, based on successful risk management results, stakeholders may be able to permit a little more risk in some areas if such a decision would support mission objectives and potentially save resources or allow them to be directed to areas that require additional resources in order to meet expected risk tolerances.
- Similar reviews and refinement occur at Level 1 to support enterprise governance and risk management decisions. Some types of enterprises may be required to formally disclose risk factors (e.g., through annual reports), and this aggregate understanding of cybersecurity risks and risk decisions can support their fiduciary responsibilities. These activities may also help others, such as federal government agencies, to help comply with mandatory requirements, such as those established by OMB.

Interpreting risk tolerance at Level 3, practitioners develop requirements and apply security controls to achieve an acceptable level of risk. This process helps to ensure that CSRM occurs in a cost-effective way. As an example, consider the global retail firm described in the first row of Table 1. The system owner of the customer website will select controls that will ensure adherence to availability service levels. In deciding which controls to apply, the system owner collaborates with a security team to consider methods to meet service level objectives. The team can contact the local power utility supplier to determine electrical availability history and gather other information regarding the likelihood of a loss of power to the important website. This additional information might help the system owner decide whether to invest in a backup generator to ensure sufficient power availability.

Results from previous assessments can be useful for estimating the likelihood of achieving risk goals in the future (this topic is described in Section 2.3.2.1.) The team would then move to the next risk scenario (e.g., perhaps an internet service outage) and review the history and reliability of the organization's telecommunications provider to ascertain the likelihood and impact of a loss of service. Iterating through each potential risk, as described in Figure 6, practitioners can

develop a risk-based approach to fulfilling CSRM objectives in light of risk appetite and risk tolerance. This, in turn, helps CSRM practitioners demonstrate how their actions directly support mission objectives and enterprise success.

2.1.4 Enterprise Strategy for Cybersecurity Risk Reporting

The enterprise strategy for cybersecurity risk management and monitoring includes common definitions for how and when assessment, response, and monitoring should take place. Notably, ERM monitoring is for communication and coordination regarding overall risk and should not be confused with system level monitoring (or continuous monitoring.)

Direction from senior leaders provides risk guidance – including advice regarding mission priority, risk appetite and tolerance, and capital and operating expenses to manage known risks – to the organizations within their purview. There are some details that need to be defined at the enterprise level so that information can be combined and compared effectively, including the ability to communicate about risks through the various types of risk registers.

While many of these details will be delegated to organization level processes, several key factors should be defined at the enterprise level, including:

- Criteria regarding risk category selection that enables risk register entries from various risk management domains to be consolidated and compared;
- Direction regarding the classification and valuation of enterprise assets, including approved methods for business impact analysis (described in Section 2.2.1.1);
- Assessment methodologies, including direction regarding analysis techniques and the appropriate scales to be applied;
- Frequency of assessment, reporting, and potential escalation;
- Methods for tracking, managing, and reporting risks; and,
- Resources available for risk treatment, including common baselines, common controls, and supply chain considerations.

As cybersecurity risks are recorded, tracked, and reassessed throughout the risk life cycle and aggregated within the enterprise cybersecurity risk register, this guidance ensures that risk will be consistently communicated, managed, and potentially escalated. Strategic guidance from enterprise stakeholders should also include:

- Definition of the organizational boundaries to which CSRM activities will apply; documentation that the scope for cybersecurity objectives supports alignment among enterprise, business and mission objectives, and operational achievements
- Direction regarding specific roles for managing, communicating, and integrating risks throughout the enterprise; defining the types of stakeholders (by role) will support risk communication and timely decision-making

- Determination of KRIs and KPIs that will support the management and monitoring of the extent to which risk response remains within acceptable levels

Through the processes described above, senior leaders express risk limits and expectations as risk appetite statements. That risk appetite is then interpreted through risk tolerance and applied at the system level. The subsections below describe how feedback is provided using the risk register to identify and document risk, analysis, and results.

2.2 Risk Identification

This section describes notional methods for identifying and documenting sources and their potential consequences (recorded in the Risk Description column of the CSRR, as shown by the red border in Figure 7.) [15] The CSRR provides a concise synopsis of identified risks, supplemented by additional detail as recorded in the Risk Detail Record (RDR). A notional example of an RDR is provided in Appendix B.[16]

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		Parts A, B, C, and D (described below)									
2											
3											
4											
5											
Continually Communicate, Learn, and Update											

Figure 7: CSRR Highlighting Risk Description Column

Risk identification represents a critical activity for determining the uncertainty that can impact mission objectives. NISTIR 8286A primarily focuses on negative risks (i.e., threats and vulnerabilities that lead to harmful consequences), but positive risks represent a significant opportunity and should be documented and reviewed as well. Consideration and details regarding positive risks will be addressed in subsequent publications. Through the activities in the following sections, risk practitioners determine and record events that could enhance or impede objectives, including the risk of failing to pursue opportunities.

[15] The CSRR template is available in the Open Risk Register Format (ORRF) format, an automated JavaScript Object Notation (JSON) for organizations maintaining automated applications that provide detailed tracking and reporting. The CSRR template is also available in comma-separated value (CSV) format at the same link.

[16] The focus of the NISTIR 8286 series is populating and communicating the risk register; however, many of the activities (such as those described in section 2.2) will generate supporting risk data that should be recorded in a Risk Detail Record (RDR) and be readily available should the additional detail be required about a risk register entry.

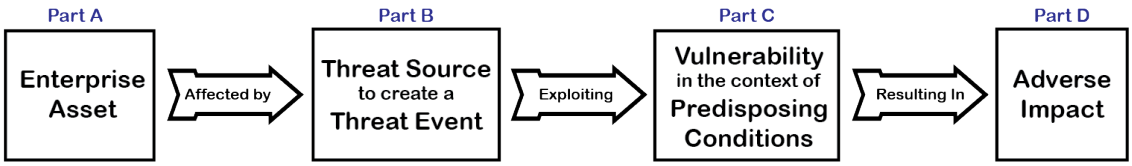

Figure 8: Inputs to Risk Scenario Identification[17]

As shown in Figure 8, which is derived from the Generic Risk Model in NIST SP 800-30, Revision 1, *Guide for Conducting Risk Assessments*, cybersecurity risk identification is composed of four necessary inputs – parts A through D – in the Risk Description cell of the cybersecurity risk register [6]. Combining these elements into a risk scenario helps to provide the full context of a potential loss event. The use of this scenario-based approach helps ensure comprehensive risk identification by considering many types of physical and logical events that might occur. The scope of cybersecurity has expanded from its original boundaries of adversarial digital attacks and encompasses all types of uncertainty that can impact any form of information and technology. Accordingly, the risks to be identified and registered are much broader as well.

The completion of the Risk Description column is composed of four activities that are detailed in Subsections 2.2.1 through 2.2.4. The activities include:

- Part A – Identification of the organization's relevant assets and their valuation
- Part B – Determination of potential threats that might jeopardize the confidentiality, integrity, and availability of those assets
- Part C – Consideration of vulnerabilities or other predisposing conditions of assets that make a threat event possible
- Part D – High-level evaluation of the potential consequences if the threat source (part B) exploits the weakness (part C) against the organizational asset (part A)

The integration of those elements enables the practitioner to record each scenario in the CSRR as a description of cybersecurity risk. The quantity and level of detail of the risks identified should be in accordance with the risk strategy.

Enterprises that are just beginning to integrate the cybersecurity risk register results into broader ERM activities will benefit from focusing on an initial and limited number of top risks. Those creating a risk management program for the first time should not wait until the risk register is completed before addressing extraordinary issues. However, over time, the risk register should become the ordinary means of communicating risk information.

[17] The consideration of positive risks involves a similar process through which an enterprise asset is considered as contributory to an opportunity, supporting activities to take advantage of a new or preexisting condition, thus resulting in a positive impact (benefit) to the enterprise.

2.2.1 Inventory and Valuation of Assets

The first prerequisite for risk identification is the determination of enterprise assets that could be affected by risk (part A in Figure 8). Assets are not limited to technology; they include any resource that helps to achieve mission objectives (e.g., people, facilities, critical data, intellectual property, and services). For assets that record or store or process data, the relevant data types (e.g., contractual, business sensitive, student records, intellectual property, privacy-related) have a significant bearing on the valuation of an asset and subsequent risk analysis.

Enterprises may benefit from applying a comprehensive method to inventory and monitor enterprise assets, such as the use of a *configuration management database (CMDB)* or an *information technology asset management (ITAM)* system. These management tools help to record and track the extent to which various assets contribute to the enterprise's mission. They can also help track enterprise resources throughout their own life cycle. For example, as the use of mobile devices (including personal devices) expands, there are commercial products that can help maintain inventory to support ongoing risk identification, analysis, and monitoring.

2.2.1.1 Business Impact Analysis

Risk managers can benefit by using a business impact analysis (BIA) (sometimes called a business impact assessment) process to consistently evaluate, record, and monitor the criticality and sensitivity of enterprise assets. The BIA categorization can, in turn, inform the establishment of risk tolerance levels.

A BIA can help document many aspects of the value of an asset that may extend well beyond replacement costs. For example, while one can calculate the direct cost of research and development underlying a new product offering, the long-term losses of the potential theft of that intellectual property could have more far-reaching impacts, including future revenue, share prices, enterprise reputation, and competitive advantage. That is among the reasons why it is beneficial to gain the guidance of senior leadership regarding the determination of assets that are critical or sensitive. The relative importance of each enterprise asset will be a necessary input for considering the impact portion of the Risk Description (part D) in the cybersecurity risk register. Considerations include:

- Would loss or theft of the resource compromise customer or enterprise private information?
- Would disclosure of an asset's information trigger legal or regulatory fines or actions?
- Would a lack of availability of the asset interrupt the enterprise's ability to fulfill its mission or result in costly downtime?
- Would the lack of confidentiality, integrity, or availability of the asset undermine public or consumer confidence or trust in the enterprise?
- Do internal or external critical resources depend on this asset to operate?
- For government systems, would loss or theft of the resource or information cause grave damage to national security?

As the organization reviews the results of previous system level categorization decisions and monitors risk assessment findings, practitioners can use that information to review system prioritization as an input into the BIA.

2.2.1.2 Determination of High-Value Assets

An example of asset valuation is the U.S. Government's designation of "high-value assets," or HVAs,[18] described in OMB Memorandum M-19-03 as representing agency resources that have been deemed highly sensitive or critical to achieving the business mission [7]. While not all critical federal assets will be characterized as HVAs, OMB M-19-03 represents an example of an enterprise approach to valuation since the memorandum defines the specific categories for consistent designation (i.e., information value, role in Mission Essential Function support, and role in support for Federal Civilian Essential Functions) yet permits each agency to determine which assets meet those criteria. Other common industry examples include the use of specific classifications to reflect the sensitivity and criticality of technology and information, including "Company Confidential" or "Business Sensitive."

2.2.1.3 Automation Support for Inventory Accuracy

Accurate and complete asset inventory is an important element of CSRM, and the measurement of that accuracy is often a key performance measurement for CSRM reporting. To illustrate that importance, federal agencies must report how completely their hardware and software asset management inventories reflect what is actually installed on agency networks as part of their annual reporting metrics.

Automated tools can aid in discovering and monitoring various technical components used by the enterprise. For example, a use case described by the NIST Security Content Automation Protocol (SCAP) specification is *inventory scanning*. Products that have been successfully reviewed as part of the SCAP Validation Program help maintain a comprehensive and accurate inventory of digital assets [8]. Valuation information recorded in that inventory can, in turn, help maintain a comprehensive view of the enterprise assets for which cybersecurity risks should be identified, analyzed, treated, and monitored. The use of automation helps to ensure that enterprise asset inventory is current, accurate, and complete.

The integration of asset inventory management processes throughout the enterprise can help to ensure a complete and accurate repository. For example, harmonizing acquisition, project management, business operations, IT operations, and security as part of an overarching ITAM process will support transparency and real-time data to effectively track and monitor assets.

2.2.2 Determination of Potential Threats

The enumeration of potential threat sources and the threat events that those sources could initiate is the second prerequisite for the identification of potential risk scenarios. Figure 9

[18] Federal Binding Operational Directive (BOD) 18-02 describes specific actions that federal agencies must complete to ensure effective identification and timely remediation of major and critical weaknesses to HVA systems [8].

represents part B of the Risk Description cell of the CSRR. Because information and technology exist in many forms, this threat-informed risk management approach combines data-driven processes (awareness of threats) and sound business judgment (consideration of mission impact) to support comprehensive risk identification.

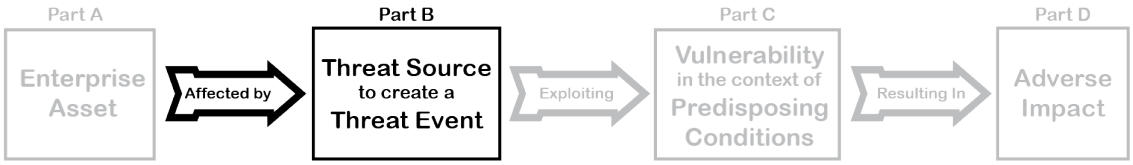

Figure 9: Threats as an Input to Risk Scenario Identification (Part B)

2.2.2.1 Threat Enumeration

Many public- and private-sector processes are available to help enumerate threats. One example is the OCTAVE Allegro method from Carnegie Mellon University's Software Engineering Institute [9]. That model includes identification of areas of concern – a process for determining the "possible conditions or situations that can threaten an organization's information asset." The OCTAVE Allegro approach describes a process where risk managers create a tree diagram of various threats based on:

- Human actors using technical means;
- Human actors using physical methods;
- Technical problems, such as hardware and software defects, malicious code (e.g., viruses), and other system-related problems; and
- Other problems that are outside of the control of an organization (e.g., natural disasters, unavailability of critical infrastructures).

Enumeration of threats can be performed as a "top-down" analysis that considers important assets that might be threatened or as a "bottom-up" analysis that considers what an unknown threat might attempt to accomplish. Table 3 provides an example excerpt of a threat analysis.

Table 3: Example Threat Modeling Analysis

Source Type	Motivation	Threat Action	Assets Affected
Insider	Accidental, Intentional	Disclosure	Legal documents related to an upcoming merger, sales records, designs from the research and development division
Insider	Intentional	Disclosure	Physical files from the personnel department, physical design drawings from manufacturing
Insider	Intentional	Modification	Financial transactions diverted for personal gain through a privilege escalation attack
External	Accidental	Disclosure	Remote access account information for maintenance service staff
External	Intentional	Destruction	Student record database
External	Intentional	Disclosure	Patient medical records database (e.g., ransomware)

Software Defects	n/a	Modification	Financial transaction database (corruption)
Software Defects	n/a	Interruption	Financial transaction database (outage)
System Crashes	n/a	Interruption	Retail e-commerce site, payroll processing system, manufacturing automation
Utility Outage	n/a	Disclosure	Enterprise network connections, e-commerce data center
Natural Disaster	n/a	Interruption	Enterprise network connections, e-commerce data center

The list above includes physical security considerations. Numerous physical issues (e.g., theft, mechanical failures) can affect digital and logical devices, so both logical and physical threat sources should be considered. Threat enumeration should also consider potential motivations or intents. Accidental and intentional threat activity can each have significant impacts, but the evaluation, treatment, and monitoring of each type of activity will vary based on the motivation. Motivation will also have some bearing on the likelihood calculation (as described in subsequent sections).

Practitioners consider various factors for each threat source based on an understanding of valuable enterprise assets, as determined in Section 2.2.1. Example considerations include:

- What might a human actor accidentally disclose, modify, or destroy?
- Are there critical or sensitive data types stored or processed by the assets at risk?
- What information or technology might a person (e.g., a disgruntled employee) *intentionally* disclose, interrupt, or delete?
- Are there threat conditions that might be introduced by supply chain partners, such as external service providers?
- Are any cyber-physical systems or other operational technology (OT) subject to an attack that might impact safety or otherwise affect enterprise operations?
- What similar considerations might apply to accidents or intentional actions from an external source using technical means?
- What technical flaws or malicious code might affect valuable systems and lead to adverse impacts on enterprise objectives?
- What natural disasters or utility outages might have harmful effects?

Risk managers should develop a reasonable list of potential threats based on practical and imaginative scenarios, particularly in light of the assets identified in earlier processes. The extent of this list depends on the direction of senior leaders. While some stakeholders may prefer fewer risks in the register, it is important to remember that any risks that are not identified at this stage will not be part of the subsequent risk analysis and may introduce an unforeseen vulnerability.

2.2.2.2 Reducing Unwanted Bias in Threat Considerations

While cybersecurity threat discussions often focus on the intentional and adversarial digital attack, it is important that all risk practitioners consider a broad array of threat sources and events. In addition, while highly unlikely scenarios might not need to be listed (e.g., a meteorite

crashing into the data center), risk managers should avoid dismissing threats prematurely. For these reasons, practitioners will benefit from identifying and overcoming bias factors in enumerating potential threat sources and the events they might cause. Consideration of these factors will also help reconcile reactionary thinking with analytical reasoning. An intentional approach to enumerate threats without bias helps to avoid complacency before an incident and supports a proactive evaluation based on relevant data, trends, and current events.

Table 4 describes some of these bias issues as well as methods for addressing them.

Table 4: Example Bias Issues to Avoid in Risk Management

Bias Type	Description	Example	Countermeasure
Overconfidence	The tendency to be overly optimistic about either the potential benefits of an opportunity or the ability to handle a threat	Notion that "our users are too smart to fall for a phishing attack"	Detailed and realistic risk analysis (see Section 2.4) helps to evaluate the true probability of threats
Group Think	A rationalized desire to miscalculate risk factors based on a desire for conformity with other members of a group or team	A group member may not want to be the only one to express concern about a given threat or opportunity	Use of individual input and subject matter expert judgement (e.g., Delphi Technique) helps avoid the risk that group-based threat discussions might discourage brainstorming
Following Trends	Over- or under-valuation of threats due to an irrational consideration of recent hype that can result in inappropriate risk response	Assuming that *any* digital challenge can be addressed and solved through the application of "machine learning" and "artificial intelligence"	Staying informed about the details of current threat patterns and considering input from subject matter experts helps avoid "following the herd" to unreasonable conclusions
Availability	Tendency to over-focus on opportunities or issues that come readily to mind because one has recently heard or read about them	Concern that VPN confidentiality is insecure because quantum computing will make modern encryption obsolete and unreliable	Detailed and realistic risk analysis (Section 2.3) helps to evaluate the true probability of threats

2.2.2.3 Threat Enumeration Through SWOT Analysis

While it is critical that enterprises address potential negative impacts on mission and business objectives, it is equally important (and required for federal agencies) that enterprises also plan for success. OMB states in Circular A-123 that "the profile must identify sources of uncertainty, both positive (opportunities) and negative (threats)" [2].

One method for identifying potential positive and negative risks is through the use of a SWOT (strength, weakness, opportunity, threat) analysis. Because effective risk management is achieved by balancing potential benefits against negative consequences, a SWOT analysis provides a visual method for considering these factors. Table 5 provides an example of an overarching SWOT analysis. A similar exercise could be performed at any level of the enterprise, including for an information system or cyber-physical system.

Table 5: Example SWOT Analysis

Strengths	**Weaknesses**
Effective communication among a small office with co-located staff Online email and financial applications mean no local servers to support and protect Modernized office desktop equipment with current operating systems and connectivity	Few dedicated IT and information security employees Many endpoints are laptops that could be lost or stolen Office laptops do not employ full-disk encryption
Opportunities	**Threats**
A newly awarded contract will significantly increase revenue and reputation Expansion of services into software development and remote administration services will enable company growth Funds have been allocated for cybersecurity improvement Third-party partners may help quickly ramp up new service offerings	Visibility from contract announcement may cause adversaries to target the enterprise Information security requirements included in the terms and conditions of the new contract increase the criticality of cybersecurity improvement Additional service offerings (e.g., development and remote administration) increase cybersecurity risks Supply chain partners may bring additional security risks to be considered and managed

2.2.2.4 Use of Gap Analysis to Identify Threats

As part of the threat modeling exercise, practitioners can benefit from evaluating a comparison of current conditions to more desirable conditions and then analyzing any gaps between those to identify potential improvements. This process can be iterative in that the organization may not know the current state until after several rounds of risk management activities. Similarly, practitioners may not fully know the desired state until after several iterations of identifying, assessing, analyzing, and responding to risks. Despite this challenge, gap analysis can be a useful tool to include as part of a broad methodology.

NISTIR 8286 provides an example of the process described by the NIST Cybersecurity Framework [5], which includes a set of activities that consider the five functions:

1. **Identify** what assets are important for achieving enterprise objectives.
2. **Protect** those assets from known threats and vulnerabilities.
3. **Detect** risk events on those assets in an efficient and effective manner.
4. **Respond** to such risk events rapidly and effectively.
5. **Recover** from any disruptions in accordance with enterprise strategy.

The framework decomposes the functions into categories, each of which is further described in terms of strategic and tactical outcomes (subcategories). For each subcategory, the framework recommends the creation of profile artifacts that document the *current* and *desired* (or target) policies, processes, and practices. By documenting the "as-is" outcomes, organizations can consider potential risk implications, including potential threat events. That information will later help develop target state profiles for managing risk as directed by risk appetite and risk tolerance statements. More detail about this process is described in NISTIR 8286C. Table 6 provides an example excerpt from a current profile with example threat considerations.

Table 6: Cybersecurity Framework Current State Profiles Help Consider Threats

ID	Category	Current State	Threat Considerations
ID.AM	Asset Management	• Hardware and software are tracked, but inventory is not always accurate. • Network flows are not mapped. • Asset classification is performed and effective. • Internal security roles are defined but not those of supply chain partners.	• **Internal user** (adds a non-compliant device; because a device is not in inventory, scans may miss it as a host so vulnerabilities may go undetected) • **External adversary** (could gain network access, and activities might not be distinguished from unmapped, typical traffic patterns) • **External partner** (may not fulfill responsibilities for protecting, detecting, or responding to incidents)
ID.BE	Business Environment	• Priorities and responsibilities based on the Commercial Facilities Sector. • Dependencies and resilience requirements are anecdotally understood but not more formally recorded.	• **Power failure** (causes customers [e.g., emergency services, hospitals] with critical dependencies to experience an extended loss of internet service due to a lack of service level agreements and documented resilience requirements)
PR.AT	Awareness and Training	• All staff have been trained in physical and information security practices during onboarding.	• **Internal user** (may fall victim to an email phishing attack due to a lack of sufficient training)
PR.DS	Data Security	• Inbound and outbound remote connections are encrypted. • Laptops with proprietary facility information do not have full-disk encryption. • Email systems are configured to provide limited data loss prevention.	• **External adversary** (who has gained network access may quickly recognize and exfiltrate unencrypted, sensitive information in databases or within cleartext network traffic) • **Internal user** (may unintentionally send sensitive records without encryption, while data loss prevention tools might impede that error)
DE.CM	Security Continuous Monitoring	• Physical security is monitored through cameras and access log reviews. • Information security logs are aggregated and stored securely. • Intrusion Detection products monitor for risks.	• **Internal User** (steals valuable equipment due to a lack of diligent video and log monitoring) • **External User** (is not quickly detected and thwarted due to ineffective monitoring)
RS.RP	Response Planning	• Response processes and procedures are executed and maintained. • Supply chain partners have not been included in planning or exercises.	• **Supply Chain Partner** (is not able to provide the Security Operations Center with system log information and is unable to restore data to a known-good recovery point)
RC.RP	Recovery Planning	• Incident recovery processes are included in response plans. • Lack of recovery objectives and metrics impedes the ability to confirm that risks are treated in accordance with risk appetite and risk tolerance.	• **Software failure** (could cause an outage in an essential business application that exceeds organizational directives regarding maximum tolerable downtime)

Another source of ideas for threat modeling is NIST SP 800-53, *Security and Privacy Controls for Information Systems and Organizations*, which provides a catalog of security and privacy controls[19] [10]. A companion document, SP 800-53A, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans*, documents methods for assessing the effectiveness and suitability of those controls for various purposes [11]. Through the examination of controls and assessment methods, practitioners can observe conditions that align with enterprise situations, sparking discussions about potential threats. For example:

> A practitioner can consider control AC-17, Remote Access, which states, "The use of encrypted VPNs provides sufficient assurance to the organization that it can effectively treat such connections as internal networks if the cryptographic mechanisms used are implemented in accordance with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines." The practitioner should then consider the threat conditions that would make encryption necessary (e.g., preventing eavesdropping, ensuring authorization) and perhaps identify regulatory compliance requirements.

Considering controls and their assessments can inspire the imagination and support effective threat modeling.

As noted in NISTIR 8286, "organizations should not wait until the risk register is completed before addressing obvious issues," such as those issues that arise from the threat modeling exercises. CSRM practitioners, in collaboration with ERM stakeholders, will need to continually define and refine the timing of various risk identification processes. An organization that delays risk management until the end of a detailed and exhaustive risk identification activity may find that many risks become realized while the practitioners are still working. At the other extreme, immediately beginning risk management when only a few risks have been catalogued can hamper prioritization or cause a continual recalculation of risk importance as new loss event types are identified and added. Threat identification methods may also discover quick wins (e.g., changing default passwords for devices and applications, enabling cryptography settings, locking file cabinets) that can be efficiently resolved, immediately addressed, and documented in the risk register while other risk identification activities continue.

2.2.2.5 Technical Threat Enumeration

While threat sources include many factors because cybersecurity risks are so closely associated with information and technology, technical threats are likely to comprise the majority of those enumerated. The complexity and rapid evolution of technical threats make it particularly worthwhile to gain insights from reputable partners regarding how to prepare for, recognize, and respond to these threat sources. These insights also help achieve a proactive threat management stance rather than a reactive approach.

[19] NIST provides a set of Online Informative References Validation Tool and Focal Document Templates, including those for SP 800-53, that assist with aligning and comparing various information security models. The templates are available at https://www.nist.gov/cyberframework/informative-references/validation-tool-templates.

To be successful in protecting information and technology and to rapidly detect, respond, and recover from threat events, the organization may choose to apply an intelligence-driven approach, commonly referenced as Cyber Threat Intelligence (CTI). Using sources of information and data, such as those described in Table 7, practitioners will gain insight into adversaries' tactics, techniques, and procedures (TTPs) as well as other information about how to prepare and what conditions to monitor.

Industry-based threat intelligence-sharing organizations are available for the exchange of CTI among members or subscribers. For example, DoD-Defense Industrial Base Collaborative Information Sharing Environment (DCISE) is a government program that facilitates CTI sharing between its Defense Industrial Base (DIB) members and participants. Another example is that of information sharing analysis centers (ISACs) and organizations (ISAOs). Using intelligence provided by such sources, risk practitioners can make threat-informed decisions regarding defensive capabilities, threat detection techniques, and mitigation strategies. By correlating and analyzing cyber threat information from multiple sources, an organization can also enrich existing information and make it more actionable.[20]

Table 7: Example Sources of Threat Information

Commercial Threat Intelligence sources	Various commercial organizations provide subscription-based services that supply enterprise intelligence regarding potential threat actors and events. Often, these intelligence providers maintain an understanding of enterprise asset types; the commercial provider then provides information about what actions specific threat sources have conducted against similar assets elsewhere. Example: Gartner Inc. Reviews for Security Threat Intelligence Products and Services https://www.gartner.com/reviews/market/security-threat-intelligence-services
Automated Indicator Sharing (AIS) feeds	Both public- and private-sector organizations (e.g., DHS, FS-ISAC) provide automated data feeds with information about existing or imminent threats, as well as vulnerabilities being exploited by those threats. Example: DHS Cybersecurity and Infrastructure Security Agency (CISA) https://us-cert.cisa.gov/ais, https://www.cisa.gov/ciscp
Information Sharing and Analysis Centers and Organizations (ISACs and ISAOs)	Many industries, including critical infrastructure sectors, experience sector-specific threat types. Information Sharing and Analysis Centers (ISACs) provide members with support and information to help conduct risk assessments and maintain risk awareness. Some ISACs offer in-house applications for sharing indicators of compromise (IoC) and other threat-based alerts. Example: National Council of ISACs (https://www.nationalisacs.org/)
Technical Threat Category Models	Many industry models are available for performing technical threat modeling, particularly in a software development context. Like the threat trees described in Section 2.2.2, such models help guide collaboration and brainstorming activities to consider what-if scenarios, including threats, vulnerabilities, and their impacts.

[20] Cybersecurity information sharing is discussed in detail in NIST SP 800-150, *Guide to Cyber Threat Information Sharing*, which is available at https://doi.org/10.6028/NIST.SP.800-150.

MITRE ATT&CK®	This is a knowledge base of adversary tactics and techniques based on real-world observations, is used as a foundation for the development of specific threat models and methods, and helps enterprise risk practitioners consider the threat conditions that an adversary might apply and the events that adversary might seek to cause. The recent addition of pre-attack indicators and methods can help prepare for and detect signs of an impending event. https://attack.mitre.org/
NSA/CSS Technical Cyber Threat Framework (NTCTF) v2	While this model does not help identify sources, it provides a broad list of the types of events that a threat source might attempt to initiate, particularly a motivated human adversary. By defining the actions such an adversary might desire to perform, the NTCTF supports an imaginative approach to enterprise threat modeling. https://www.nsa.gov/Portals/70/documents/what-we-do/cybersecurity/professional-resources/ctr-nsa-css-technical-cyber-threat-framework.pdf

By understanding typical attack patterns, enterprises can mount defenses to improve resilience. For example, understanding the methods of various attackers in privilege escalation or lateral movement will help risk managers plan effective preventive and detective controls. Because technical attacks can move rapidly, preparation is paramount. Updated, rapid sharing of indicators of compromise (such as those provided through Structured Threat Information Expression [STIX]) helps enterprise practitioners better detect and respond to emerging threats.[21]

Because of the time-critical nature of cybersecurity risks, the use of automation in threat intelligence analysis enables an enterprise to reduce the potential delays and errors that a human-only approach can introduce. While automated information sharing will not entirely eliminate threats, it can help an organization stay aware of and prepared for new and evolving types of attacks. One example of an AIS is that offered by the U.S. Department of Homeland Security (DHS) in accordance with the U.S. Cybersecurity Information Sharing Act of 2015. The DHS AIS site includes the following information:

> The free (DHS) AIS capability enables the exchange of cyber threat indicators between the Federal Government and the private sector at machine speed. Threat indicators are pieces of information like malicious IP addresses or the sender address of a phishing email (although they can also be much more complicated).
>
> AIS participants connect to the "CISA Central" service that allows bidirectional sharing of cyber threat indicators. A server housed at each participant's location allows them to exchange indicators with CISA. Participants will not only receive DHS-developed indicators but can share indicators they have observed in their own network defense efforts, which DHS will then share back out to all AIS participants.[22]

An analysis of network packet capture data can help identify potential threats based on observed traffic. Armed with understanding from CTI sources regarding TTPs and IoCs, practitioners will be able to observe potential indicators and likely attack paths. In conjunction with past and

[21] STIX is one of several data exchange specifications for cybersecurity information sharing. More information is available at https://oasis-open.github.io/cti-documentation.

[22] CISA Central (formerly the National Cybersecurity and Communications Integration Center, or NCCIC) is part of the Cyber Information Sharing and Collaboration Program (CISCP) and is available at www.cisa.gov/central.

existing cyber incident information, organizations can use CTI to support internal risk communication and risk analysis and to improve risk scenario development. In addition to the technical advisories, the alerts and analysis reports at the DHS National Cyber Alert System provide information about recent TTPs and how they have affected various enterprises.

2.2.3 Vulnerability Identification

For any of the various threat conditions described above to result in an impactful risk, each needs a vulnerable or predisposing condition that can be exploited. The identification of vulnerabilities or conditions that a threat source would use to cause impact is an important component of risk identification and represents part C (Figure 10) of the CSRM risk scenario. As demonstrated in examples throughout this series, threats and vulnerabilities are not limited to the routine vulnerability management of software flaws, patching and network ports, but encompass a more full range of considerations that NIST Special Publication (SP) 800-53 addresses in the form of controls.

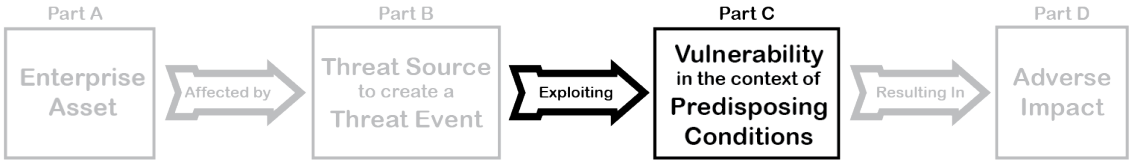

Figure 10: Vulnerability Inputs to Risk Scenario Identification (Part C)

2.2.3.1 Determination of Vulnerabilities and Predisposing Conditions

While it is necessary to review threats and vulnerabilities as unique elements, they are often considered at the same time. Many organizations will consider a given loss scenario and evaluate both. What threat sources might initiate which threat events? What vulnerabilities or predisposing conditions might those threat sources exploit to cause a loss event?[23] Much of the information provided through CTI will also inform an understanding of vulnerability. For example, analysis of the infamous 2017 WannaCry ransomware attack includes understanding the threat source and motive (a known and capable cybercrime group seeking financial gain), the intended threat event (deliberate modification, interruption, and potential destruction of key enterprise information assets), and the vulnerability to be exploited by the adversary (CVE-2017-0144).

Practitioners should (within the scope agreed upon in activities described in Section 2.1) systematically consider the potential physical and logical vulnerabilities and predisposing conditions that can be exploited by a threat source. This consideration can be facilitated by many of the methods described in Table 7, including:

[23] There are many similarities among threat identification and vulnerability identification activities. These may seem redundant, but it is important to understand both the sources of potential harm (threats) and the conditions that those threat sources might exploit (vulnerabilities).

- The use of commercial intelligence sources can provide threat and vulnerability information. Many providers will take note of a customer's enterprise information and technology (e.g., hardware, software, and operating systems in use) to alert the organization to any vulnerabilities in those platforms that are known to be targeted by existing threat sources.

- The integration of AIS feeds may include automated alerts regarding known vulnerabilities. Many security incident event monitoring (SIEM) products and intrusion detection systems (IDS) can help enterprises associate asset inventory information with AIS alerts to support incident reporting and monitoring.

- A threat tree model (e.g., the diagram in the OCTAVE ALLEGRO guidance) can consider various human factors, technical defects, software flaws, physical entry points, utility dependencies, and supply chain vulnerabilities that present vulnerabilities.

- A review of the various threat categorization models (e.g., MITRE ATT&CK®) can inspire internal discussions, such as "What vulnerabilities might enable execution of malicious code?" or "What predisposing conditions foster lateral movement within the enterprise?"

As with threat modeling, practitioners will also benefit from applying known risk management frameworks as a tool for vulnerability discovery. For example, a review of the controls catalog in SP 800-53 may lead to consideration of control MP-3, Media Marking, which can then inspire discussion regarding potential vulnerabilities that might result from unmarked (or improperly marked) system media.

Notably, the enterprise will benefit from the advice of external specialists with expertise in identifying and categorizing various types of vulnerabilities. Some entities, such as those operating moderate- and high-impact federal information systems, require formal penetration testing to identify potential vulnerabilities and the exploitability of those conditions. In addition to some government and law enforcement agencies that are able to assist enterprises with evaluating physical and technical vulnerabilities, many commercial organizations offer these services.

2.2.3.2 System Complexity as a Vulnerability

NISTIR 8286 states that additional risks can result from the dynamic complexity of enterprise information and technology. In fact, that complexity is itself a vulnerability to be considered and documented. Evaluation of "what-if" scenarios regarding potential vulnerabilities, especially those affecting critical assets, should include the determination of critical dependencies on other resources. Because risk identification and risk analysis are iterative, risk analysis methods (such as the Event Tree Analysis described in Section 2.3.2.2) will help determine those dependencies. Having made that determination, those critical dependencies can be recorded in the BIA (described in Section 2.2.1.1). Risk identification then includes scenario discussions that evaluate complex or cascading events as vulnerabilities to be identified.

For example, the 2003 Northeast Power Grid interruption demonstrated how several moderate risk events cascaded into a national emergency.[24] Another example of systemic risk are the financial institutions that were impacted by cascading risk in 2008.[25] In that case, large enterprises experienced catastrophic events because they had interdependencies with other banks, insurance companies, and customers. When identifying and recording risks in the register, such emerging risk conditions created by the interdependence of systems and counterparty risk must also be identified, tracked, and managed using the same methods described for more straightforward scenarios.

As with other CSRM components, vulnerability identification can be considered through either qualitative or quantitative means. An organization might determine that it has a large number of high severity vulnerabilities based on an internal review. A qualitative review might result from a gap analysis between NIST Cybersecurity Framework Current State and Target State profiles since such an analysis is intended to foster discussion and communication regarding risks but will not likely produce a highly specific quantitative result.

More quantitative vulnerability identification results from a formal testing approach that examines a discrete set of enterprise resources for a specified set of known vulnerabilities. Particular vulnerability assessments (e.g., software code review or simulated phishing attack) can provide quantitative results. Results of a formal assessment might include a specific number of identified issues, which can be used to help complete the likelihood column of the risk register.

2.2.3.3 Vulnerability Identification Automation

The complexity and interconnection of technology results in many thousands of potential vulnerabilities. Because of this broad scale combined with a rapidly evolving technical landscape, automation can improve the enterprise's ability to manage relevant vulnerabilities. Automation also enables a timelier monitoring of risk as well as adaptation to changing risk scenarios.

Hardware and software products are significant sources of vulnerabilities for any enterprise, whether through inherent flaws in those products or through errors in product implementation or application. To help support the consistent identification and monitoring of these vulnerabilities, security organizations have developed broad clearinghouses of vulnerability information. For example, NIST operates the National Vulnerability Database (NVD) and the National Checklist Program (NCP) to support vulnerability and security configuration management via catalogs of:

- Configuration checklists for securing key information technologies,

[24] For more information about the 2003 power blackout, please see https://www.nerc.com/pa/rrm/ea/August%2014%202003%20Blackout%20Investigation%20DL/ISPE%20Annual%20Conf%20-%20August%2014%20Blackout%20EPA%20of%202005.pdf

[25] For more information about the 2008 global banking crisis, please see the report Risk Management Lessons from the Global Banking Crisis of 2008, https://www.sec.gov/news/press/2009/report102109.pdf

- Information about secure configuration settings (with associated SP 800-53 security controls),
- Vulnerabilities (with associated severity scores),
- Standardized security checklists for automated security configuration scanning (e.g., security checklists in Security Content Automation Protocol format[26]), and
- Products that use standards to identify and report vulnerabilities.

Automated data feeds, such as those described above, enable enterprise monitoring tools to ingest information about known vulnerabilities in near-real time and compare them with the asset inventory. A key factor in that data feed is information regarding the date that a vulnerability was publicly disclosed. The severity of a given vulnerability increases exponentially after it becomes publicly known, so it is important that practitioners prioritize remediation of flaws. The risk of the vulnerability must be balanced with the risk of implementing a fix for that issue too quickly. Automated tools can help monitor and maintain that balance through specific reports regarding severe vulnerabilities that have not been patched within a reasonable time. An example of this is the DHS AWARE (Agency-Wide Adaptive Risk Enumeration) scoring methodology used by the DHS Continuous Diagnostics and Mitigation (CDM) risk management dashboard. AWARE is not intended to identify all issues, but the scoring methodology helps to highlight and prioritize cybersecurity risks that are likely to exceed allowable risk tolerance (e.g., known software vulnerabilities on critical assets that are not mitigated within a designated grace period).[27]

2.2.4 Determining Potential Impact

The final prerequisite for creating a practical list of risk scenarios for the risk register is the determination of the potential impact of the threats and vulnerabilities described above. The section below describes the completion of part D of the CSRM Risk Description column (Figure 11.)

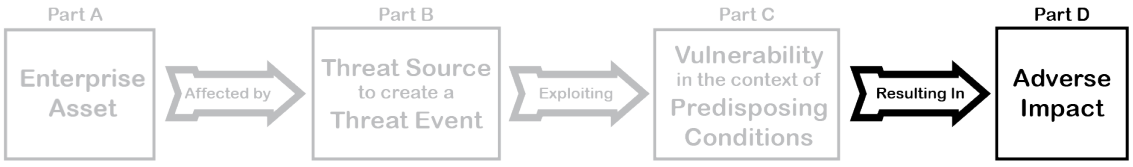

Figure 11: Adverse Impact Inclusion in Risk Scenario Identification (Part D)

Discovery activities throughout Section 2.2 may have already highlighted potential adverse impacts to explore. Description of the impact is a key element for enterprise stakeholders and represents the connection between cybersecurity risks and the enterprise objectives that would be affected by those risks. Reviewing the key enterprise objectives, as identified in scoping, and

[26] Information about the NIST SCAP is available at https://csrc.nist.gov/projects/security-content-automation-protocol/.

[27] More information about the DHS AWARE scoring method is available at https://www.cisa.gov/cdm-training.

armed with a broad list of potential threats and vulnerabilities, personnel can develop a list of realistic scenarios.

While some types of impact may not be immediately apparent, the long-term effects can be significant. For example, consider a situation where a criminal has gained unauthorized access to an enterprise system and has exfiltrated a large amount of confidential data. If that criminal is cautious, there may not be any disruption of operations. In fact, sometimes cyber criminals actually try to *improve* the health of a victim's technology to ensure that it will be available for their malicious activity. In this case, the system may seem to be working fine – even better than ever – and then later, the enterprise realizes that a catastrophic loss has occurred.

Notably, impact scenarios can be considered as a continuum rather than as a binary state. Many impacts will cause mission degradation or reduced performance and may not exhibit themselves as a full interruption of service or capability. This consideration should be factored into risk prioritization and analysis.

Risk scenarios should be assessed in terms of both initial impact and downstream consequences. Factors to consider include:

- Primary impact – The initial impact following a negative cybersecurity event, such as the downtime when a website is unavailable to customers
- Secondary impact – A loss event that occurs subsequent to the primary impact as a downstream or cascading impact to the enterprise

For example, consider a large enterprise that experiences a breach of confidential customer data. In this example, an external attacker with criminal intent might attack a highly critical and sensitive customer database through a software vulnerability in the internet-facing website. The initial impact may be minimal since exfiltration is not disruptive, and the company may not even detect an issue. Once the problem has been discovered, there may be primary impacts, such as:

- Cost of a focused investigation into the breach
- Price of restitution for customer losses (e.g., credit monitoring services)
- The expense of third-party specialists to provide forensic expertise and to ensure adequate mitigation of the cybersecurity incident
- Cost of immediate capital investment to address cybersecurity issues that contributed to the breach

Long-term or secondary effects may be more impactful. They can include:

- Loss of market share due to eroded trust in the company's reputation
- Reduction or cessation of funding for a government agency or program
- Revenue losses from organizations that choose not to renew contracts
- Fines and penalties from regulators

When considering the impact component of risk scenarios, it is important to consider the frequency of potential consequences. A risk event of moderate impact that occurs weekly may, over time, represent a higher risk than that of a major event that occurs infrequently. Such temporal factors may be valuable for stakeholders' understanding and reporting of risks. For example, senior leaders may wish to see the impact of a risk expressed as the loss for each occurrence (the *single loss expectancy,* or *SLE*), or they might prefer to see the total loss for that risk over an annual period (the *annualized loss expectancy,* or *ALE*). Consistent documentation of impact frequency is also important for supporting the integration and aggregation of risk registers.

As with other risk components, impact considerations may be either qualitative or quantitative, as illustrated by the examples in Table 8.

Table 8: Example Negative and Positive Impact Scenarios

Description of negative consequences (qualitative)	A software flaw results in a significant issue with the integrity of enterprise financial systems, necessitating a major outage and extended rework to validate existing records and verify proper operation.
Description of negative consequences (quantitative)	A ransomware attack has performed unauthorized encryption of 112,000 patient records. Remediation and repair of the affected health information system are likely to disrupt operations for 48 hours, resulting in a $1.14 million primary loss.
Description of positive impact (qualitative)	New machine learning technology would significantly increase the throughput of the enterprise research team and could lead to expansion into new marketing areas.
Description of positive impact (quantitative)	The addition of high-availability services for the enterprise web server will improve availability from 93.4 % to 99.1 % over the next year and will also improve market share by 3 % due to improved customer satisfaction and resulting reviews.

2.2.5 Recording Identified Risks

Using the four elements described in earlier subsections (i.e., key assets, threats, vulnerabilities, and impacts), practitioners can complete the risk description column in the risk register. As previously stated, the CSRR provides a brief synopsis of each identified risk and the RDR provides for recording and managing many of the specific details developed above.

ID	Priority	Risk Description	Risk Category	Current Assessment		
				Likelihood	Impact	Exposure Rating
1	TBD	External criminal attacker exploits a software vulnerability in the internet-facing customer data site, resulting in "significant" customer confidential data exfiltration with revenue, reputation, and regulatory implications.				
2	TBD	A flood event enters the first-floor data center, causing water damage to several critical servers and interrupting service to more than 10% of customers.				

Figure 12: Example Risk Register with Sample Risk Descriptions

The use of detailed risk scenarios helps ensure that all understand the risks being considered and the impacts on organizational objectives. The risk description (illustrated in Figure 12) need not be exhaustive but should include sufficient information to support subsequent analysis, evaluation, treatment, and monitoring. Use of a cause-and-effect format clarifies the event or scenario under consideration and its specific impacts. An example risk description based on the data breach illustration above might say:

> External criminal attacker exploits a software vulnerability in the internet-facing customer data site, resulting in "significant" customer confidential data exfiltration with revenue, reputation, and regulatory implications.

In support of ERM, practitioners need to continually balance an understanding of what mission objectives can be affected by various threats (a top-down consideration) and how various threats can impact enterprise objectives (a bottom-up consideration). Both sets of conditions are continually changing, so CSRM is an iterative activity of ongoing discovery, communication, response, and monitoring. In addition to the known risks that are already being monitored, there may also be developing or *emergent risks* that are yet to be fully defined but might disrupt enterprise objectives in the future.

Each of the activities in Section 2.2 is iterative and supports the top-down/bottom-up approach described above. An if/then scenario analysis can be developed and used to consider threats and vulnerabilities, which may lead to the discovery of additional risk scenarios to be considered. This iterative process can be adjusted and tailored to develop and maintain a practical and manageable set of risks.

As an example, consider some high-value assets that are important to a local hospital and issues that could jeopardize those assets. Some top-down considerations may include:

- Patient record database – A ransomware attack could encrypt critical records; a network outage could disrupt availability; an authentication issue could hamper the ability to log in; a software upgrade could inadvertently corrupt the data.
- Pharmaceutical system provided by a third party – A malicious (or tricked) insider could alter pharmacy records, resulting in incorrect medication being given to a patient; the malicious external party could break in and disclose or destroy pharmacy records; a construction incident could sever network communications to the service.
- Point of care (PoC) terminals – Authentication system failure could disrupt the ability to provide patient care; user data error could result in inaccurate and potentially unsafe patient conditions; an improperly tested software patch could render terminals unusable.

Bottom-up considerations start with threats and vulnerabilities and consider where those can lead:

- Ransomware attack through a social engineering attack (e.g., web-based malware drive-by attack, email phishing attack) – An attack could render many systems unreadable, including patient care databases, pharmacy records, billing systems, and payroll.
- Network outage due to a firewall malfunction – An internal failure of a major switch or router could result in localized failures of PoC terminals, patient in-processing, and medical care services (e.g., review of radiology reports). External connectivity failure would disrupt electronic mail, clinical professional services, pharmaceutical processing, some laboratory results.
- Physical hardware malfunction through a failed component – Technical equipment (e.g., televisions) could be rendered unavailable with few consequences, and technology (e.g., patient scanners) malfunctions could fail to provide timely and accurate patient results. Awaiting replacement systems could lead to potential injuries (e.g., through fire or electrical shock) or delays in patient care.

Thorough risk identification in realistic and mission-oriented scenarios help to communicate the connection between various uncertainties and the mission objectives that might be affected.

2.2.6 Risk Categorization

Each risk in the CSRR should also indicate the relevant risk category (indicated by the yellow dashed box in Figure 13) based on the risk strategy guidance described in Section 2.1. Categories could be any taxonomy that helps aggregate risk information and supports the integration of cybersecurity risk registers for ERM decision support. Example risk categories include:

- Risk framework groupings, such as by security and privacy control families (e.g., Access Control, Supply Chain Risk Management, such as those recorded in NIST SP 800-53)
- Threat types, such as intentional disclosures, unintended modifications, system failures, or natural disasters
- Impact considerations based on business units affected or information systems impacted

Consistent risk categorization supports the effective integration of cybersecurity risks throughout the enterprise and aggregation into an enterprise cybersecurity risk register. That information ultimately becomes part of the overall Enterprise Risk Register and the Enterprise Risk Profile.

2.3 Detailed Risk Analysis

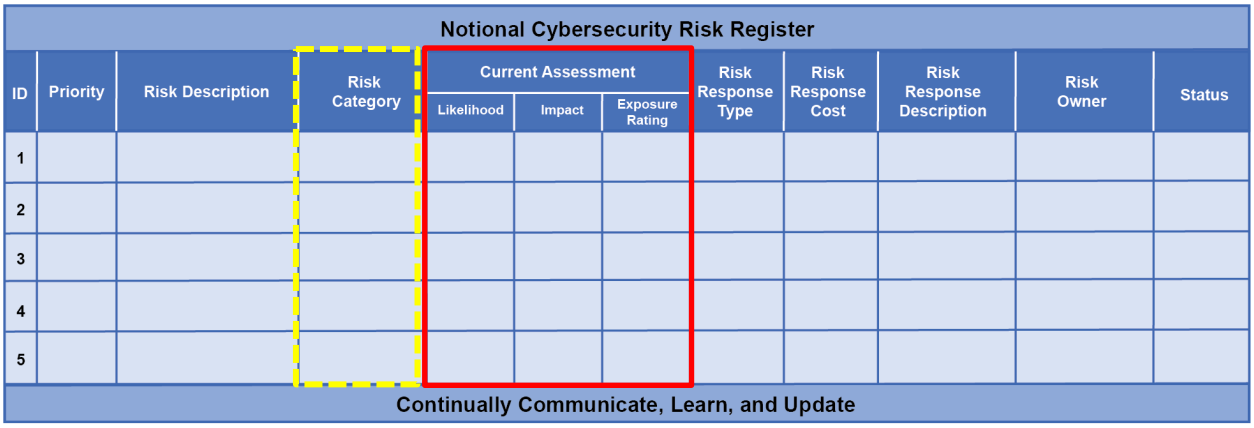

Figure 13: CSRR Highlighting Risk Category and Current Assessment Columns

Risk analysis enables the determination of the likelihood of impact and priority of treatment. This section helps to complete the likelihood and impact columns of the cybersecurity risk register and the exposure column that represents the product of those two values. These columns are illustrated by the solid red box in Figure 13.

Because cybersecurity risk reflects the effect of uncertainty on or within a digital component that supports enterprise objectives, risk analysis helps to measure both the level of uncertainty entailed by the risk scenario and the extent of the uncertain effect upon enterprise objectives. Deterministic models can provide a detailed analysis of likelihood and impact where sufficient information is available for such a determination. In other cases, the randomness of uncertainty and the many factors involved in complex information and technology better support a probabilistic (or stochastic) methodology.

2.3.1 Selecting Risk Analysis Methodologies

International Electrotechnical Commission (IEC) standard 31010:2019, *Risk management — Risk assessment techniques*, provides a comprehensive list of risk analysis techniques. The standard states,

> In deciding whether a qualitative or quantitative technique is more appropriate, the main criteria to consider are the form of output of most use to stakeholders and the availability and reliability of data. Quantitative techniques generally require high quality data if they are to provide meaningful results. However, in some cases where data is not sufficient, the rigor needed to apply a quantitative technique can provide an improved understanding of the risk, even though the result of the calculation might be uncertain [12].

The Open Group Standard for Risk Taxonomy (O-RT) Version 2.0, part of the OpenFAIR series of documents, supports the assertion that quantitative risk analysis can provide an improved understanding of risk [13].[28] It points out,

> While there's nothing inherently wrong with a qualitative approach in many circumstances, a quantitative approach provides better clarity and is more useful to most decision-makers – even if it's imprecise. For example, [one] may not have years of empirical data documenting how frequently cleaning crew employees abuse usernames and passwords on sticky-notes, but [we] can make a reasonable estimate using ranges, particularly if [we] have been trained in how to make estimates effectively.

Analysis considerations are often provided in a qualitative way, such as, "The patient database is at high risk of unauthorized disclosure because we have learned that hackers are targeting health information systems with ransomware, and we have determined that there are numerous vulnerabilities in our health information system."

In other cases, the analysis can be quantitative, such as in the example below:

> The health information system contains about 12,000 records. A successful ransomware breach could cost approximately $1.3 million if the data is destroyed or $2.5 million dollars if the breach results in a disclosure. We know that the Arctic Zebra APT team has been targeting similar databases; through our understanding of their techniques and those of others, we believe that there is a 70 % chance they will target us and a 30 % chance (based on internal testing and network scans) that it would be successful. Based on that data, we believe that there is a 21 % chance of single loss exposure, or between $273,000 and $525,000. This exposure calculation does not consider additional secondary losses, such as lost revenue due to customer erosion from loss of trust or personal lawsuits against the firm.

As shown by the referenced standards and examples in this section, there are benefits to both qualitative and quantitative risk analysis methodologies and even the use of multiple methodologies, based on enterprise strategy, organization preference, and data availability. Regardless of the methodologies being applied, it is important to consider as many data points as needed to render a judgement regarding likelihood and impact values. Unfortunately, without supporting data, well-intentioned but misguided methods of risk analysis amount to little more than a guess. In many cases, the application of even a moderate amount of deductive reasoning, combined with various analysis techniques, can render a more accurate and reliable risk analysis. Quantitatively informed qualitative decision-making should be the objective in the absence of purely quantitative-driven decisions.

[28] OpenFAIR also highlights the importance of determining and quantifying the probable frequency of future loss, including the need to determine Threat Event Frequency (TEF) and Loss Event Frequency (LEF) values. Agencies have pointed out that accurate calibrated ranges, such as for TEF and LEF, can lead to more accurate calculations for Annualized Loss Exposure (ALE). Details regarding the OpenFAIR taxonomy and analysis are available at the reference provided. [14]

Because CSRM is intended to inform ERM activities, the selection and application of risk analysis methods must be aligned. The enterprise CSRM strategy should inform risk analysis methodologies, support coordination, and direct the consistent use of available data. As with many risk management elements, the strategy should help consider the methods available and provide for a tailored approach that results in effective risk management.

When selecting a risk assessment technique, organizations should consider the analysis costs in light of the desired outcome to help determine the most cost-effective technique. Inexpensive but accurate qualitative analysis that identifies the most risks and leads to best mitigating those risks may be the right move for a particular organization. For others, a highly detailed quantitative risk assessment may require more resources than a qualitative approach but may also provide specific and actionable information that helps to focus attention on important threat scenarios.

2.3.2 Techniques for Estimating Likelihood and Impact

NISTIR 8286 highlights the need for improved risk analysis when estimating and recording the likelihood and impact of cybersecurity events and monitoring to ensure that risks remain within acceptable parameters.[29] To improve enterprise risk estimation accuracy and consistency, CSRM practitioners are encouraged to explore the use of tools and processes that support measurable and meaningful risk analysis and reporting.

Some analysis techniques are based on estimates from subject matter experts' (SMEs) experience and knowledge. Some methods, such as this SME estimation, can be subjective. Other methods are more objective and based on analytical considerations, statistical analysis, and scenario modeling, as well as potentially drawing on knowledge of previous events.

Understanding the intended purpose of the analysis can help one decide which techniques to use. For example, a detailed and quantified approach may be valuable as a basis for a comprehensive review or update of the enterprise cybersecurity approach. Detailed evaluation helps to reinforce defense measures and increase resilience, as in the following example:

> Enterprise leaders have learned through an InfraGard alert that there is a high probability that companies in its sector will be targeted by a particular APT group. Because internal cybersecurity risk managers have performed threat modeling based on the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK®) and Pre-ATT&CK frameworks, the company was able to quickly consider high-value assets that would most likely be at risk.
>
> A key TTP of this attack is "password spraying" brute force login attempts. Several critical systems have not yet been updated to support multi-factor authentication and would be vulnerable to such an attack. A poll of the security leaders (using a Delphi exercise) determined that there is a 50-70 % chance that the payroll system will be attacked (the mean value was 60 %). A successful attack on that system would have

[29] It is the intention of this document to introduce the reader to commonly used estimation techniques. The authors defer to other industry resources for comprehensive details regarding how to perform such analyses.

direct and indirect financial impacts of between $1.7 million and $2.4 million USD with the most likely impact being $2.0 million. Therefore, the risk exposure value for this row of the risk register was established at $1.2 million (based on .6 x $2 million).

Notably, the example above provides several ranges of estimates. Some industry specialists have indicated that a range of possible values is more helpful and likely more accurate than a single "point estimate." Additionally, while this example uses the mean values of those ranges to identify the likelihood and potential impact, the ranges themselves are often recorded in the risk register. In this instance, given a possible impact of "between $1.7 million and $2.4 million," the exposure may have been presented as "$1.02 million to $1.44 million."

2.3.2.1 Improving Estimation Based on Knowledge of Prior Events

Information about previous risk events may be helpful when estimating the likelihood and impact of those in the future. For example, practitioners should consult industry literature, their current power companies, or internet service providers for descriptions of loss events within a given sector or over a particular time frame. To determine the likelihood of a utility outage, the utility provider can be asked to provide details regarding previous disruptions and their duration.

As an example, consider the example organization in the first row in Table 1: Examples of Risk Appetite and Risk Tolerance. It describes a global retail firm at which a senior leader has expressed the risk tolerance statement that "any outage that exceeds four hours for any customer requires significant corrective action." Risk practitioners can review the actual availability of that website for the previous year (using a table similar to Table 9).

Table 9: Example Risk Tolerance Results Assessment

Month	Total Hours in the Month	# of Hours Unavailable	Outage (Customer %)	Available Hours	Tolerance Limit (Total - 4 hrs.)	Avail % (Avail. Hrs. ÷ Total Hrs.)
Jan	744	1	2.4	743	740	99.87 %
Feb	672			672	668	100.00 %
Mar	744			744	740	100.00 %
Apr	720	1.5	4.5	718.5	716	99.797 %
May	744			744	740	100.00 %
Jun	720			720	716	100.00 %
Jul	744			744	740	100.00 %
Aug	744			744	740	100.00 %
Sep	720	2	0.5	718	716	99.72 %
Oct	744			744	740	100.00 %
Nov	720	3	1.5	717	716	99.58 %
Dec	744			744	740	100.00 %
Yearly	**8760**	**7.5**	**-**	**8752.5**	**8704.5**	**99.91 %**

In this case, the system did not exceed the risk tolerance since no single outage exceeded four hours, nor did any outage impact more than 5 % of customers. While past performance is not a guarantee of future probability, it provides some information that helps inform likelihood estimates. The impact of an outage is likely similar to that in previous iterations. Understanding the probability of an outage given what is known about prior disruption helps organizations consider likely exposure in the future.

When considering each risk in the risk register, practitioners will analyze the likelihood that any risk would result in an impact that would exceed the risk tolerance. That consideration provides a basis for risk treatment decisions, either to ensure sufficient security controls or to review risk tolerance statements to ensure that they represent reasonable and practical expectations.

2.3.2.2 Three-Point Estimation

One method for considering the likelihood or impact of a risk event is three-point estimation. This method,[30] illustrated in Figure 14, is useful because it considers the judgement of available subject matter experts (SMEs). For example, to determine the impact[31] of a successful phishing attack, the risk estimator could poll an SME regarding:

- The most optimistic (or best case) estimate (O),
- A most likely estimate (M), and
- A pessimistic (or worst-case) estimate (P).

Figure 14 illustrates the result of an SME estimating a $80,000 revenue loss due to an attack that would be successful if employees are not properly trained. This first estimate represents a worst-case scenario (pessimistic). The same estimator may suggest that only a $35,000 impact is likely (optimistic) if the attack were successful but limited in spread. Finally, the SME may suggest that the most likely impact of recovering from such a successful phishing attack would be $50,000. Each of these data points can be used to calculate the expected value (also known as EV, expectation, average, or mean value).

[30] For better estimates of O, M, and P and to eliminate bias, the estimator should poll multiple SMEs and determine the average of individual O values, M values, and P values before proceeding with the three-point estimate.

[31] Although impact was used in this example, three-point estimating can also be used in determining likelihood.

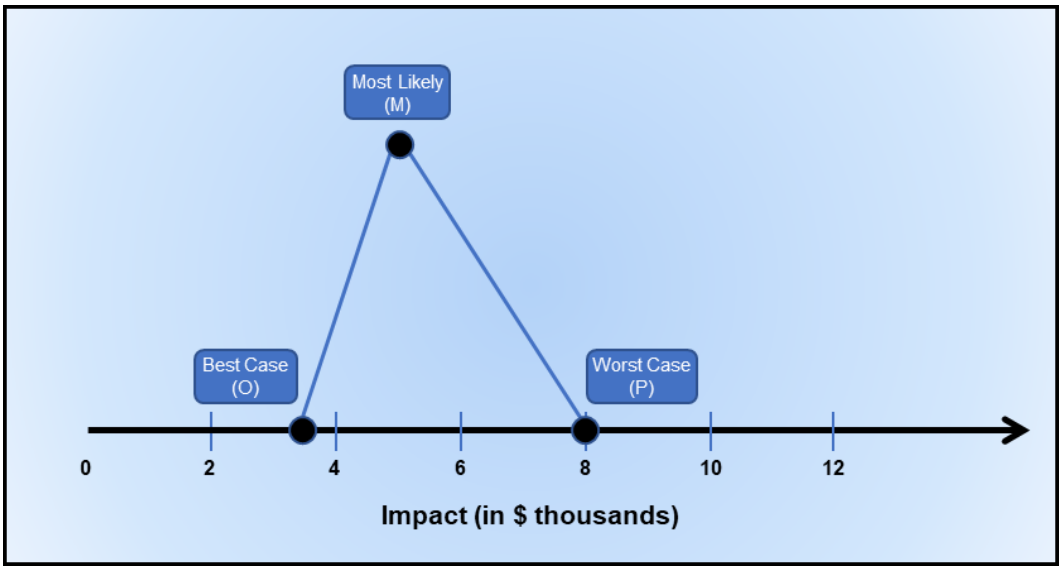

Figure 14: Example Three-Point Estimate Graph (Triangle Distribution)

The three datapoints can be categorized as **O**ptimistic ($35,000), **P**essimistic ($80,000), and **M**ost likely ($50,000). A simple average of the three numbers (called a *Triangular Distribution*) is:

$$EV = \frac{P+M+O}{3} = \$55{,}000 \text{ in this example, where O=\$35,000, P=\$80,000, and M=\$50,000}$$

In this phishing attack scenario, perhaps the estimator believes that the pessimistic and optimistic values are too different and that the "most likely" estimate is a better predictor. The estimator can give greater weight (perhaps four times as much) to the "most likely" value using the following standard formula (called the *Average for a Beta Distribution*):

$$EV = \frac{P+4M+O}{6} = \$52{,}5000 \text{ in this example, where O=\$35,000, P=\$80,000, and M=\$50,000}$$

The next question is, "How confident is the estimator regarding this estimated impact of a successful phishing attack?" In three-point estimating, confidence (referred to as *sigma,* or σ) in the estimated value can be predicted by calculating the standard deviations from the mean. A useful model for determining sigma is $\sigma = \frac{P-O}{6}$.

Figure 15 illustrates these values graphically. Statistical models have demonstrated that one can determine the level of confidence (or confidence interval [CI][32]) in the financial estimates given the mean (EV) and standard deviation. For the example above, the estimator will have a 68.27 % confidence that the financial impact of a successful phishing attack will result in a loss between $39,000 and $66,000. The estimator will have approximately a 95 % confidence that the loss will be between $25,500 and $79,500 and a nearly 100 % confidence in the $12,000 to $93,000

[32] The NIST Engineering Statistics Handbook points out that a confidence interval generates a lower and upper limit for the mean instead of a single estimate. The interval gives an indication of how much uncertainty there is in the estimate of the true mean. The narrower the interval, the more precise the estimate. (See https://itl.nist.gov/div898/handbook.)

estimate. This application of CI is useful for each of the analysis methods in this section and helps to represent the level of uncertainty in each of the estimates.

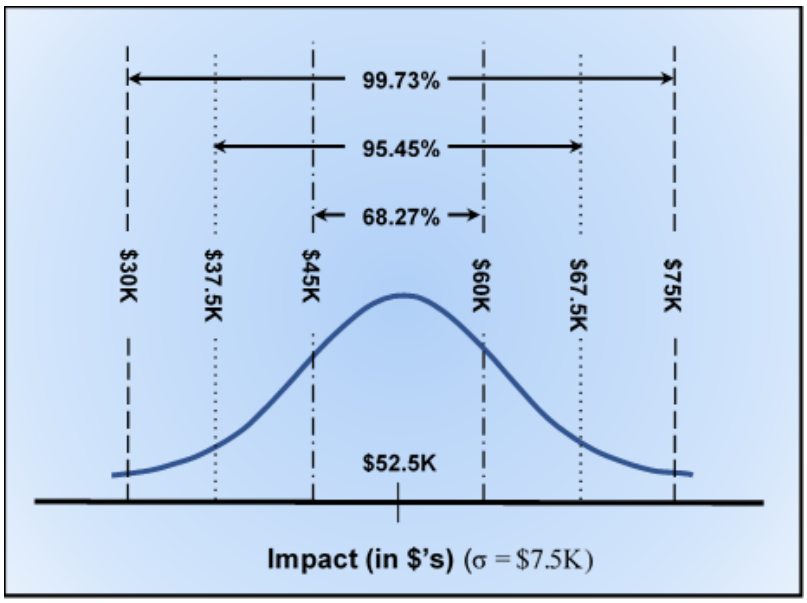

Figure 15: Example Three-Point Estimate Graph (Normal Distribution)

Confidence requirements and standardized methods of calculation should be included in senior leaders' ERM strategy as part of enterprise risk management policy. This directive helps all risk practitioners in the enterprise consider risk in a similar manner and may help to improve the reliability of likelihood and impact estimates. Additionally, as more information becomes available regarding previous risk results and those of external organizations, this information can be included in the estimation models and used to reduce uncertainty.

Notably, the level of effort for estimating risk factors increases with the required level of rigor. An estimate with very low CI might be simple to develop (perhaps as simple as flipping a coin) but likely offers little value. A CI of 99 % may be important in some situations, but the work to develop a more precise estimate can cost significantly more than that required for a 90 % CI. Because the appropriate levels of accuracy and precision for cybersecurity risk analysis will vary based on enterprise needs, the techniques and expectations should be clearly defined as part of the enterprise's risk management guidance.

It is critical that the risk practitioner consider the accuracy of the SME estimates over time to determine who or what source is more accurate and then consider that expert judgement more prominently in calculations for the ongoing risk management cycles. Experts who are overly optimistic or pessimistic create a broad range. However, when accuracy is required, especially when calculating likelihood, knowing who the best estimators are in the organization is vitally important.

2.3.2.3 Event Tree Analysis

Event Tree Analysis (ETA) is a graphical technique that helps practitioners evaluate the downstream impact of a given scenario (as determined in Section 2.2.4.) In the same way that a Root Cause Analysis helps consider previous events that have already led to an event, ETA helps consider the potential consequences of future events. The exercise helps document a sequence of outcomes that could arise following an initiating threat event (e.g., a particular TTP, as described in Section 2.2.2). By iterating through a series of what-if scenarios, the practitioner can analyze each set of circumstances and determine the likelihood that the results would occur.

Figure 16 demonstrates the layered defense that an organization employs to prevent malicious code from being used to exfiltrate data. For each condition, the analyst considers a Boolean (i.e., true or false) answer. The analyst then follows through each iterative outcome until an end result is reached. This analysis can be performed in a qualitative way (using the yes or no conditions), or a probability could be calculated for each scenario. In Figure 16, the probability is calculated based on whether the attack was prevented (Yes) or if the attack was successful (No). Since each branch of the tree represents a binary option, the sum of the two probabilities is always equal to 100 % (or 1.00 in decimal format). In this example, the calculated probabilities provide information about the potential success (or failure) of risk response. The resulting probability (*Pr* values in the example below) is multiplied by the anticipated financial loss of the scenario. In the tree below, if the anticipated loss of sensitive data being exfiltrated is $1.4 million, then there is a $205,100 risk exposure ($1.4 million x.1463).

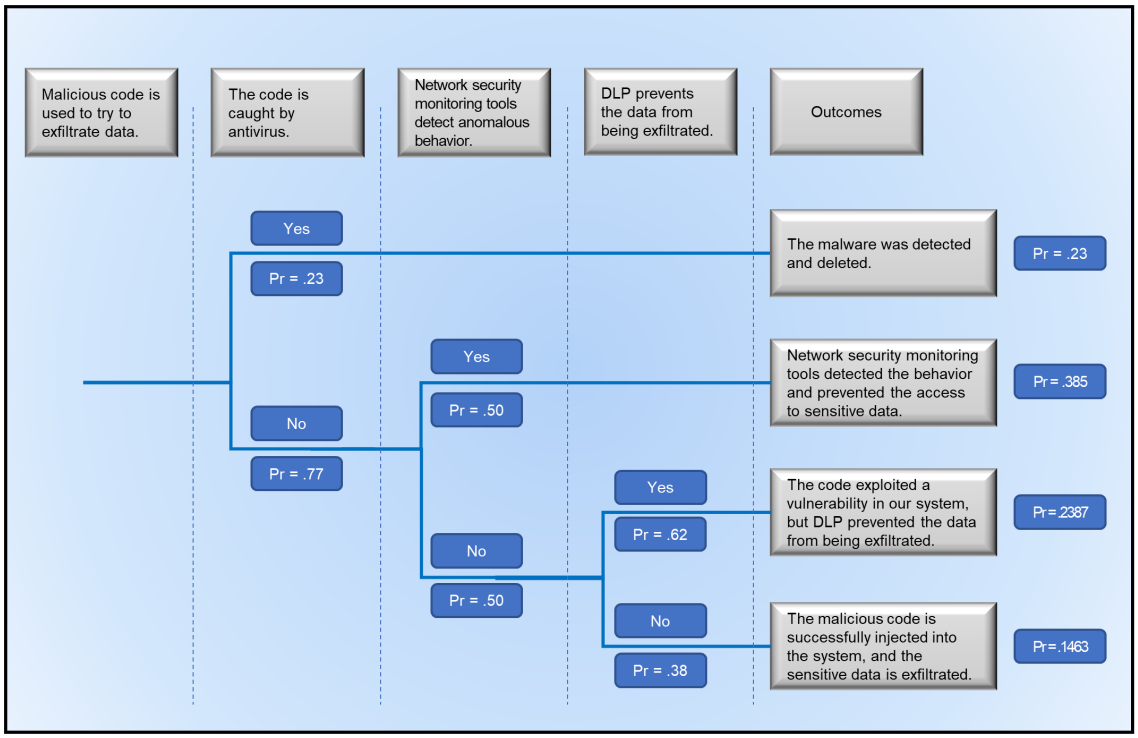

Figure 16: Example Event Tree Analysis

In the above example, the Event Tree Analysis of the cascading events illustrates the various countermeasures available and the calculated percentage of the success of each defense. A qualitative approach would still describe the Yes/No conditions and outcomes but would not include specific probabilities of each branch. While such an analysis might be less helpful than a quantitative approach, it would still provide meaningful information about potential harmful impacts to the organization and the sequence of events leading to those consequences.

2.3.2.4 Monte Carlo Simulation

While expert judgement is valuable in estimating risk parameters, one way to reduce subjectivity is to supplement that judgement using simulation models. For example, using the Monte Carlo method, the above parameters could be modeled repeatedly (perhaps several hundred thousand cycles) to help account for the many random variables inherent in cybersecurity risks. Simulation is not always necessary, but with the variables for considering likelihood and impact values (based on the factors described in Section 2.2), randomly sampled probabilities can help identify a range of possible values.[33] The results of such a simulation can be plotted on a graph or distribution to facilitate a visual understanding, such as shown in Figure 17.

For example, when calculating the financial impact of the attack on the payroll system (from the example above), practitioners can use a simulation model to consider the most likely range between the low value ($1.7 million) and the high value ($2.4 million). The result of this simulation could be recorded as a histogram that records the frequency at which certain random values occurred, in this case resulting in a simulated estimated impact of $2 million.

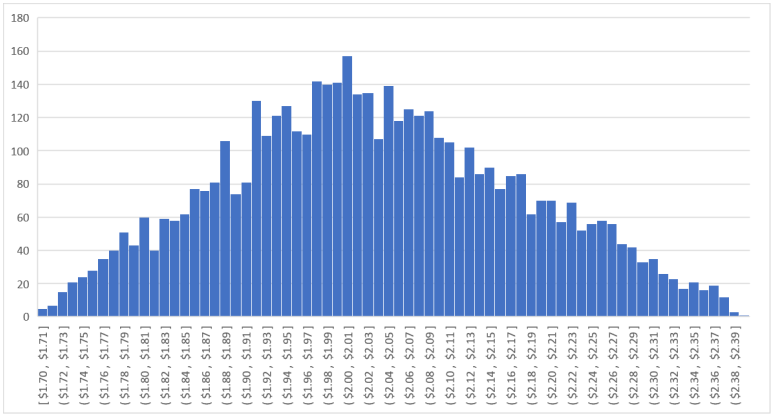

Figure 17: Illustration of a Histogram from a Monte Carlo Estimation Simulation

2.3.2.5 Bayesian Analysis

While there is value in using expert judgement to help estimate risk parameters, it might be improved based on information known from prior events, and the results may represent a more objective determination. For example, if the organization has identified that several critical software vulnerabilities have remained uncorrected, there is an increased likelihood that a threat

[33] An example implementation of a Monte Carlo analysis is available from NIST's Engineering Lab at https://www.nist.gov/services-resources/software/monte-carlo-tool.

actor will be able to exploit a software vulnerability to successfully gain access to the enterprise and exfiltrate valuable data. Bayesian analysis describes methods for considering conditional probability – applying a distribution model and a set of known prior data to help estimate the probability of a future outcome.[34]

While an SME might render an opinion regarding how likely a breach might be, that opinion can be improved by what the enterprise risk managers already know about the success of previous attempts by others or about the success of adversaries in similar enterprises. Prior knowledge, drawn from internal observations and events at similar organizations can be of significant value for improving the accuracy and reliability of estimates, such as those for determining the likelihood of an impactful event or for estimating the impact of that uncertainty on the enterprise objectives. Similar methods can be used to estimate whether several conditions might occur (joint probability) or that certain conditions would occur given other external variables (marginal probability).

2.4 Determination and Documentation of Risk Exposure

Once the probability that an impactful event will occur has been determined and the most probable impact of such an occurrence has been calculated, the information is recorded in the risk register. Figure 18 shows how an organization can record this information.

ID	Priority	Risk Description	Risk Category	Current Assessment		
				Likelihood	Impact	Exposure Rating
1	TBD	An outsider using an APT breaches the organization's network, remains undetected for months, and exfiltrates much of the organization's critical and prioprietary intellectual property by employing a Privilege Escalation attack.	Access Control (AC)	.6	$2,000,000	$1,200,000

Figure 18: Example Quantitative Analysis Results

[34] Application and usage of Bayesian analysis is outside of the scope of this document but is included here as a valid quantitative means for performing risk analysis estimation.

Figure 19 provides an illustration of similar information in a qualitative manner.

ID	Priority	Risk Description	Risk Category	Current Assessment		
				Likelihood	Impact	Exposure Rating
5	TBD	Criminals are able to infiltrate our customers' mobile banking application due to endpoint user validation or an encryption issue, fraudulently causing customer funds to be transferred to an unauthorized location.	System & Information Integrity (SI) / System & Comms Protection (SC)	H	H	H

Figure 19: Example Qualitative Analysis Results

In this example, internal SMEs feel that the likelihood of an attack on the organization's mobile banking application is high. A survey of the SMEs reflects their determination that the impact to the organization if customers experience such an event would be high based on customers' perception that the application lacked sufficient security protections. In this case, the practitioner would use the enterprise assessment scale for determining qualitative risk, such as the application of Table I-2, *Assessment Scale – Level of Risk (Combination of Likelihood and Impact)*, from SP 800-30, Revision 1. Based on that table, an event with a high likelihood and high impact would be ranked as a high exposure. As an example, this decision would help inform the selection of strong user authentication and encryption controls.

Risk priority is described in NISTIR 8286B and will be determined based on mission objectives, enterprise strategy, and the results of comprehensive risk identification and analysis activities.

3 Conclusion

The use of the methods and templates described in this report supports effective communication and coordination of ERM and CSRM activities. As described in NISTIR 8286, understanding the expectations of senior leaders and business managers regarding risk is a key input for managing cybersecurity risk at the business and system levels. This is reflected by including the determination of enterprise risk appetite and organizational risk tolerance among the first tasks in both the Cybersecurity Framework and the NIST Risk Management Framework.

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 20: Use of a Cybersecurity Risk Register Improves Risk Communications

Once these expectations have been defined and communicated, practitioners can use various methods to ensure that risk is managed to stay within the limits articulated. They do this by identifying potential risks (as described in Section 2.2), estimating the probability that an impactful event will occur, calculating the potential harm to the enterprise after such an event, and analyzing the actual risk exposure (the product of likelihood and impact).

Industry practitioners have demonstrated that applying risk analysis techniques like those described in Section 2.3 can be helpful for identifying, responding to, and monitoring enterprise cybersecurity risk. While statistical analysis has been available for hundreds of years, many within the CSRM community have only recently recognized the value of applying a more quantitative approach to risk estimation. It seems likely that those in the CSRM domain will continue to develop and improve statistical methods to estimate risk and include guidance regarding the application of various statistical distribution models.

Responses to previous requests for information have indicated that enterprise risk managers desire increased rigor in the manner in which risk identification, analysis, and reporting are performed. This publication is designed to provide guidance and to further conversations regarding ways to improve CSRM and the coordination of CSRM with ERM. Subsequent publications in this series will describe improvements to the manner in which risk scenarios are prioritized, treated, and reported. Through the NISTIR 8286 series publications, NIST will continue to collaborate with public- and private-sector communities to address methods for improving the integration and coordination of ERM and CSRM.

References

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

[2] Office of Management and Budget (2016) 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

[3] National Institute of Standards and Technology (2020) *Online Informative References*. Available at https://www.nist.gov/cyberframework/informative-references

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

[5] 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

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

[7] Office of Management and Budget (2019) OMB Memorandum M-19-03, Strengthening the Cybersecurity of Federal Agencies by enhancing the High Value Asset Program. (The White House, Washington, DC), OMB Memorandum M-19-03, December 10, 2018. Available at https://www.whitehouse.gov/wp-content/uploads/2018/12/M-19-03.pdf

[8] National Institute of Standards and Technology (2020) *Security Content Automation Protocol*. Available at https://csrc.nist.gov/projects/security-content-automation-protocol

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

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

[11] 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

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

[13] The Open Group (2013) Risk Taxonomy (O-RT), Version 2.0 (OpenFAIR). Available at https://publications.opengroup.org/standards/open-fair-standards/c13k

Appendix A—Acronyms

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

AIS	Automated Indicator Sharing
ALE	Annualized Loss Expectancy
APT	Advanced Persistent Threat
AWARE	Agency-Wide Adaptive Risk Enumeration
BIA	Business Impact Analysis
CCE	Common Configuration Enumeration
CDM	Continuous Diagnostics and Mitigation
CI	Confidence Interval
CMDB	Configuration Management Database
CPE	Common Platform Enumeration
CSRM	Cybersecurity Risk Management
CSRR	Cybersecurity risk register
CTI	Cyber Threat Intelligence
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
DIB	Defense Industrial Base
DCISE	DoD-Defense Industrial Base Collaborative Information Sharing Environment
ERM	Enterprise Risk Management
ERP	Enterprise Risk Profile
ERR	Enterprise Risk Register
ETA	Event Tree Analysis
EV	Expected Value

HVA	High-Value Asset
IDS	Intrusion Detection Systems
IEC	International Electrotechnical Commission
IoC	Indicators of Compromise
ISAC	Information Sharing Analysis Center
ISAO	Information Sharing and Analysis Organization
ITAM	Information Technology Asset Management
ITL	Information Technology Laboratory
KPI	Key performance indicator
KRI	Key risk indicator
NCCIC	National Cybersecurity and Communications Integration Center
NCP	National Checklist Program
NTCTF	NSA/CSS Technical Cyber Threat Framework
NVD	National Vulnerability Database
OLIR	Online Informative References
OT	Operational technology
OVAL	Open Vulnerability Assessment Language
POA&M	Plan of Actions & Milestones
RDR	Risk Detail Record
SCAP	Security Content Automation Protocol
SIEM	Security Incident Event Monitoring
SWOT	Strength, Weakness, Opportunity, and Threat Analysis
TTP	Tactics, Techniques, and Procedures

Appendix B—Notional Example of a Risk Detail Record (RDR)

NISTIR 8286 recommends use of a *risk detail record*, or RDR. As shown in the following notional example, an RDR may help provide information regarding each risk, relevant stakeholders, date and schedule considerations, and planned activities.

Notional Risk Detail Record		
Risk ID Number(s)		
System Affected:		
Organization or business unit:		
Risk Scenario Description		
Asset(s) Affected		
Threat Source(s) / Actor(s) (with intent? with motivation?)		
Threat Vector(s)		
Threat Event(s)		
Vulnerability / Predisposing Conditions		
Primary Adverse Impact (be sure to reconcile impact vs consequences)		
Secondary Adverse Impact(s)		
Other scenario details		
Risk Category		
Current Risk Analysis		
Likelihood before controls (%):	**Impact before controls ($):**	**Exposure Rating before controls ($):**
Planned Residual Risk Response	Select all that apply: □ **Accept** □ **Avoid** □ **Transfer** □ **Mitigate**	
Planned Risk Response Description		
Resource Requirements for Planned Risk Response		
Planned Response Cost ($)		
Likelihood after controls will be (%):	**Impact ($)**:	**Expected Exposure Rating ($)**:
Residual Risk Response as Implemented	**Actual Response Cost ($)**:	
After controls are in place, measured Likelihood is (%):	**Impact ($)**:	**Final Exposure Rating ($)**:
Risk owner / point of contact		
Date of risk identification		
Source of risk information		
Current status date		
Dependencies		
Follow-up date		
Comments		

Figure 21: Notional Risk Detail Record

JSON-based digital expressions of the CSRR and RDR notional template, with examples, are available from the NIST Computer Security Resource Center.