Identifying and Estimating Cybersecurity Risk for Enterprise Risk Management (ERM)

Kevin Stine
Stephen Quinn
Nahla Ivy
Larry Feldman
Greg Witte
R. K. Gardner

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

Identifying and Estimating Cybersecurity Risk for Enterprise Risk Management (ERM)

26 Kevin Stine
27 *Applied Cybersecurity Division*
28 *Information Technology Laboratory*

Larry Feldman
Greg Witte
Huntington Ingalls Industries
Annapolis Junction, MD

31 Stephen Quinn
32 *Computer Security Division*
33 *Information Technology Laboratory*

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

35 Nahla Ivy
36 *Enterprise Risk Management Office*
37 *Office of Financial Resource Management*

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

Note to Reviewers

In the development of this second public draft, it has become clear that there is some variance in
how common terms are applied across government, commercial, and other types of enterprises.
Keeping in mind that all comments are publicly available and should contain no confidential or
proprietary information, it will be helpful for commenters to include information about how risk
direction (i.e., risk appetite, risk tolerance, risk boundaries) are used within their organizations.

Acknowledgments

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).

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

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

119   **Document Conventions**

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

123   **Call for Patent Claims**

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

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

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

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

137   under reasonable terms and conditions that are demonstrably free of any unfair
138   discrimination; or

139   without compensation and under reasonable terms and conditions that are demonstrably
140   free of any unfair discrimination.

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

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

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

Executive Summary

150 All organizations face a broad array of risks, including cyber security risk. For federal agencies,
151 the Office of Management and Budget (OMB) Circular A-11 defines risk as "the effect of
152 uncertainty on objectives." An organization's mission and business objectives can be impacted
153 by such effects and must be managed at various levels within the organization.
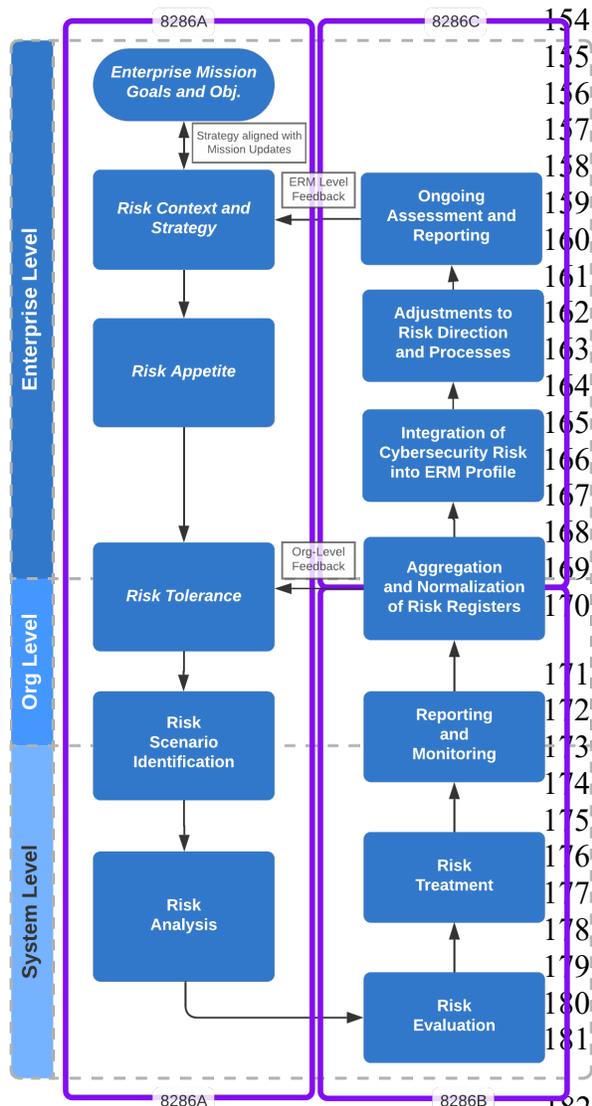
Figure 1: NISTIR 8286 Series Publications Describe Detailed CSRM/ERM Integration

154 This report highlights aspects of cybersecurity
155 risk management (CSRM) inherent to
156 enterprises, organizations, and systems. The
157 terms *organization* and *enterprise* are often
158 used interchangeably; however, without an
159 understanding of organizational structure,
160 effective risk management is impossible. For
161 the purposes of this document, an
162 *organization* is defined as an entity of any
163 size, complexity, or position within a larger
164 organizational structure. The *enterprise* exists
165 at the top level of the hierarchy where senior
166 leaders have unique risk governance
167 responsibilities. Each enterprise, such as a
168 corporation or government agency, is
169 comprised of *organizations* supported by
170 *systems*.[1]

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

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

---

[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."

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

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

195 • NISTIR 8286B describes ways to apply risk analysis to prioritize cybersecurity risk,
196 evaluate and select appropriate risk response, and communicate risk activities as part of
197 an enterprise CSRM strategy.

198 • NISTIR 8286C describes processes for aggregating information from CSRM activities
199 throughout the enterprise. As that information is integrated and harmonized,
200 organizational and enterprise leaders monitor achievement of risk objectives, consider
201 any changes to risk strategy, and use the combined information to maintain awareness of
202 risk factors and positive risks (or opportunities).

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

211   **Table of Contents**

236   **List of Appendices**

239   **List of Figures**

262   **List of Tables**

272

1   Introduction

274   This report provides guidance that supplements NIST Interagency/Internal Report (NISTIR)
275   8286, *Integrating Cybersecurity and Enterprise Risk Management (ERM)* [1]. This is the first of
276   a series of companion publications that provide guidance for implementing, monitoring, and
277   maintaining an enterprise approach designed to integrate cybersecurity risk management
278   (CSRM) into ERM.[2] Readers of this report will benefit from reviewing the foundation document,
279   NISTIR 8286, since many of the concepts described in this report are based upon practices and
280   definitions established in that NISTIR.

281   Each publication in the series, as illustrated in
282   Figure 2, provides detailed guidance to
283   supplement topics in the flagship document.
284   Activities described in this report are shown in
285   dark blue; those in other documents are shown in
286   a lighter shade.

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

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

298   • NISTIR 8286C describes processes for
299   aggregating information from CSRM activities
300   throughout the enterprise. As that information is
301   integrated and harmonized, organizational and
302   enterprise leaders monitor achievement of risk
303   objectives, consider any changes to risk strategy,
304   and use the combined information to maintain
305   awareness of risk factors and positive risks (or
306   opportunities).

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

A key point established by NISTIR 8286 is that
308   the terms *organization* and *enterprise* are often used interchangeably. That report defines an
309   organization as an entity of any size, complexity, or position within a larger organizational
310   structure (e.g., a federal agency or company). It defines an *enterprise* as having a structural

---

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

311   hierarchy and senior leaders that bear fiduciary management and reporting responsibilities,
312   including establishing risk strategy (e.g., risk appetite, methods).[3] Notably, government and
313   private industry CSRM and ERM programs have different oversight and reporting requirements
314   (e.g., accountability to the public versus accountability to shareholders), but the general needs
315   and processes are quite similar.

1.1   Supporting CSRM as an Integrated Component of ERM

317   There are similarities and variances
318   among approaches by public- and
319   private-sector practices for
320   ERM/CSRM coordination and
321   interaction. Some entities
322   incorrectly treat ERM and CSRM
323   practices as separate stovepipes.
324   The CSRM program is an integral
325   part of the ERM portfolio, both
326   taking its direction from ERM and
327   informing it. The universe of risks
328   facing an enterprise includes many
329   factors, and risks to the enterprise's
330   information and technology often
331   rank high within that list. ERM
332   strategy and CSRM strategy are
333   not divergent; CSRM strategy
334   should be a subset of ERM strategy
335   with particular objectives,
336   processes, and reporting. This
337   report and those in this series
338   support improving ERM and
339   CSRM coordination. As the risk
340   management community continues
341   that discussion, NIST will solicit
342   and publish lessons learned and
343   shared by that community.

344   Section 2 shows that enterprise
345   governance activities direct the
346   strategy and methods for risk
347   management, including CSRM.
348   Results of those activities are
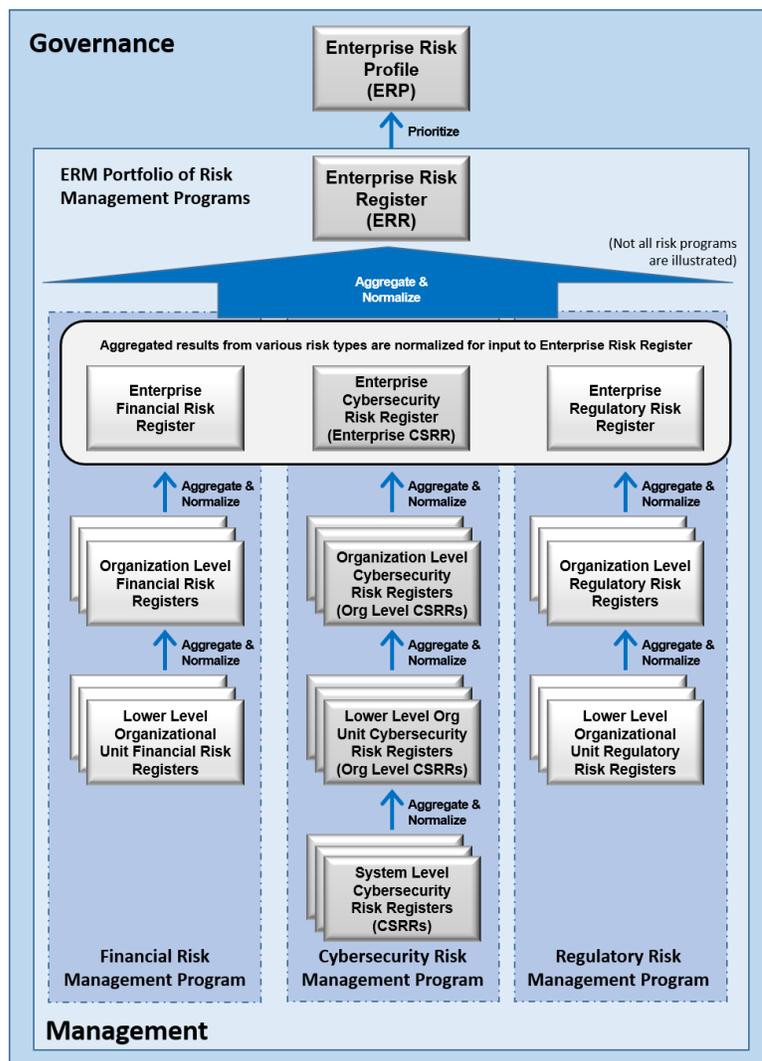
Figure 3: Integration of Various Risk Management Activities into the Enterprise Risk Register and Risk Profile

---

[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 entirety of entity 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 organizational structure and composition.

349 recorded in various risk registers. Cybersecurity risks, derived from system level assessments,
350 are documented through cybersecurity risk registers (CSRRs) that are aggregated and used to
351 create an *enterprise* cybersecurity risk register (Enterprise CSRR) that, in turn, becomes part of a
352 broader Enterprise Risk Register (ERR), as depicted in Figure 3. The ERR, when prioritized by
353 those with fiduciary and oversight responsibilities, represents an Enterprise Risk Profile. Figure 3
354 illustrates the integration of risk register information and demonstrates that ERM and CSRM are
355 not separate processes, but CSRM represents an important subset of risk management under the
356 broader umbrella of enterprise risk management.

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

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

1.2 Purpose and Scope

374 This document focuses on improving CSRM understanding and communications between and
375 among cybersecurity professionals, high-level executives, and corporate officers to help ensure
376 the effective integration of cybersecurity considerations as a critical subset of overarching
377 enterprise risks. The processes that will be described support improved coordination among
378 ERM champions and liaisons. The report recognizes that the risk management community has
379 observed an opportunity for increased rigor in the manner in which cybersecurity risk
380 identification, analysis, and reporting are performed at all levels of the enterprise. This
381 publication is designed to provide guidance and to further conversations regarding ways to
382 improve CSRM and the coordination of CSRM with ERM.

---

[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.

383   The goals of this document are to:

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

388   This document continues the discussion to bridge existing private industry risk management
389   processes with government-mandated federal agency enterprise and cybersecurity risk
390   requirements derived from OMB Circulars A-123 and A-130 [2]. It builds upon concepts
391   introduced in NISTIR 8286 and complements other documents in this series. It references some
392   materials that are specifically intended for use by federal agencies and will be highlighted as
393   such, but the concepts and approaches are intended to be useful for all enterprises.

1.3   Document Structure

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

400   • Section 2 details CSRM considerations, including enterprise risk strategy for risk
401   identification and risk analysis.

402   • Section 3 provides a short summary and conclusion.

403   • The References section provides links to external sites or publications that provide
404   additional information.

405   • Appendix A contains acronyms used in the document.

406   • 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. That risk condition, after the agreed-upon risk response has been applied, becomes the current risk state in the next assessment cycle.

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 will be described in a subsequent publication. Note that, while prioritization is informed by some of the information recorded in these columns, risk priority will be discussed in that future publication as part of Risk Evaluation and Risk Response activities. While the example illustrates a 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

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

2.1   Risk Scope, Context, and Criteria

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

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

449   • The *scope* of the CSRM activities should be defined;

450   • The internal and external *context* of the CSRM activities should be determined; and

451   • The criteria from enterprise stakeholders should be declared and documented through a
452   comprehensive CSRM *strategy*.

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

2.1.1   Risk Appetite and Risk Tolerance

460 CSRM, as an important component of ERM, helps assure that cybersecurity risks do not hinder
461 established enterprise mission objectives. CSRM also helps ensure that exposure from
462 cybersecurity risk remains within the limits assigned by enterprise leadership. Figure 5 illustrates
463 the ongoing communications among ERM and CSRM stakeholders to set, achieve, and report on
464 risk expectations throughout the enterprise. This illustration builds upon the well-known levels
465 of the Organization-Wide Risk Management Approach described in NIST Special Publication
466 (SP) 800-37, Revision 2 [5]. The diagram extends the Notional Information and Decision Flows
467 figure from the NIST *Framework for Improving Critical Infrastructure Cybersecurity*
468 (Cybersecurity Framework) by indicating risk appetite and risk tolerance definition,
469 interpretation, and achievement [6].

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

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

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

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

499 Achievement of defined expectations is conveyed through risk registers that document and
500 communicate risk decisions. Risk assessment results and risk response actions at the system level
501 are reflected in CSRRs. As CSRRs from multiple systems are collated and provided to higher
502 level business managers at the organization level, those managers can evaluate results and refine
503 risk tolerance criteria to optimize value delivery, resource utilization, and risk. The enterprise
504 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.

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

510   **Table 1: 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 2 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 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.

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

520   **2.1.2   Enterprise Strategy for Cybersecurity Risk Coordination**

521   Figures 5 and 6 provide simplified illustrations of risk integration and coordination activities.
522   Each enterprise is unique, so enterprise leadership may wish to tailor the approach for those
523   unique circumstances. For example, while risk appetite statements usually originate from the
524   most senior leaders, those leaders may choose to delegate the creation of cybersecurity risk
525   appetite statements to a senior cybersecurity risk official (e.g., Chief Information Security
526   Officer, or CISO). Readers should note that the processes described are cyclical. Early iterations
527   may include the definition of terms, strategies, and objectives. Subsequent iterations may focus
528   on refining those objectives based on previous results, observations of the risk landscape, and
529   changes within the enterprise.
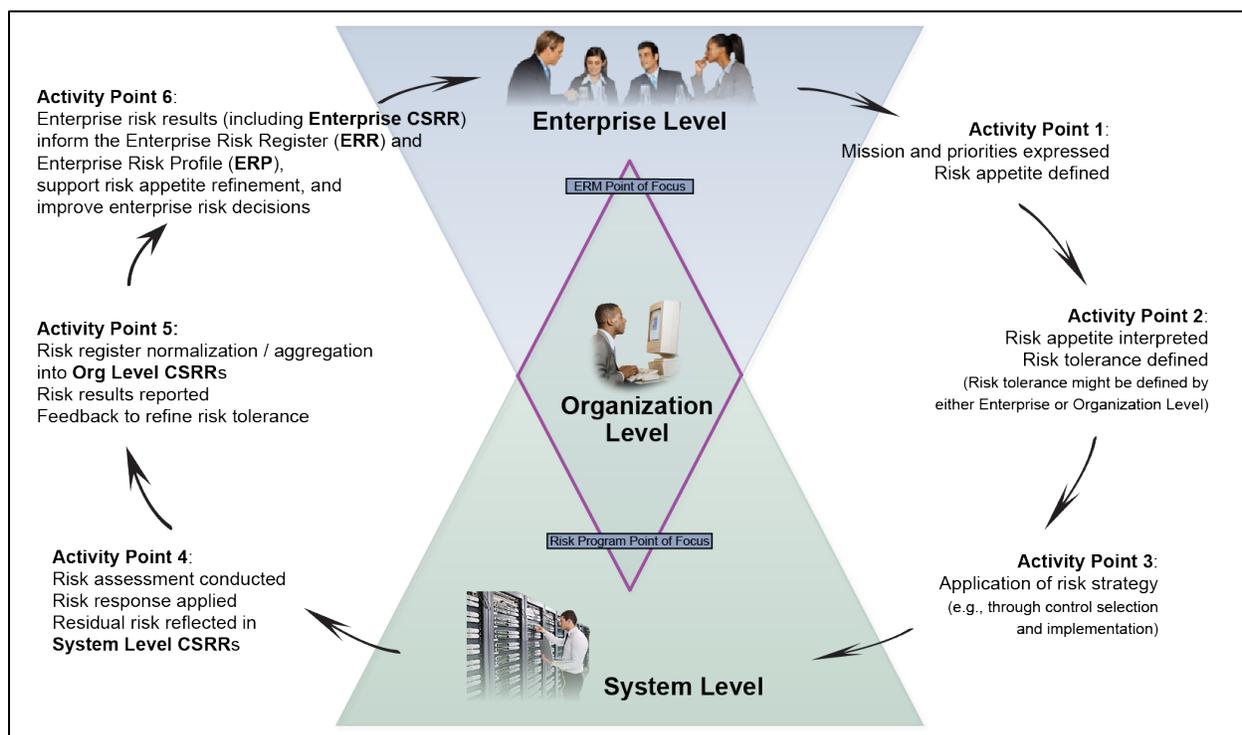
530

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

532   Table 2 describes the process by which senior leaders express strategy and expectations for
533   managing cybersecurity risk throughout the enterprise. In general, NISTIR 8286A addresses
534   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 will
        provide additional information about the activities described in Figure 5 and Table 2.

535　　　**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 (e.g., NIST Risk Management Framework, or RMF, Prepare step); 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

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

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

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

548   ### 2.1.3 Detailed Risk Integration Strategy
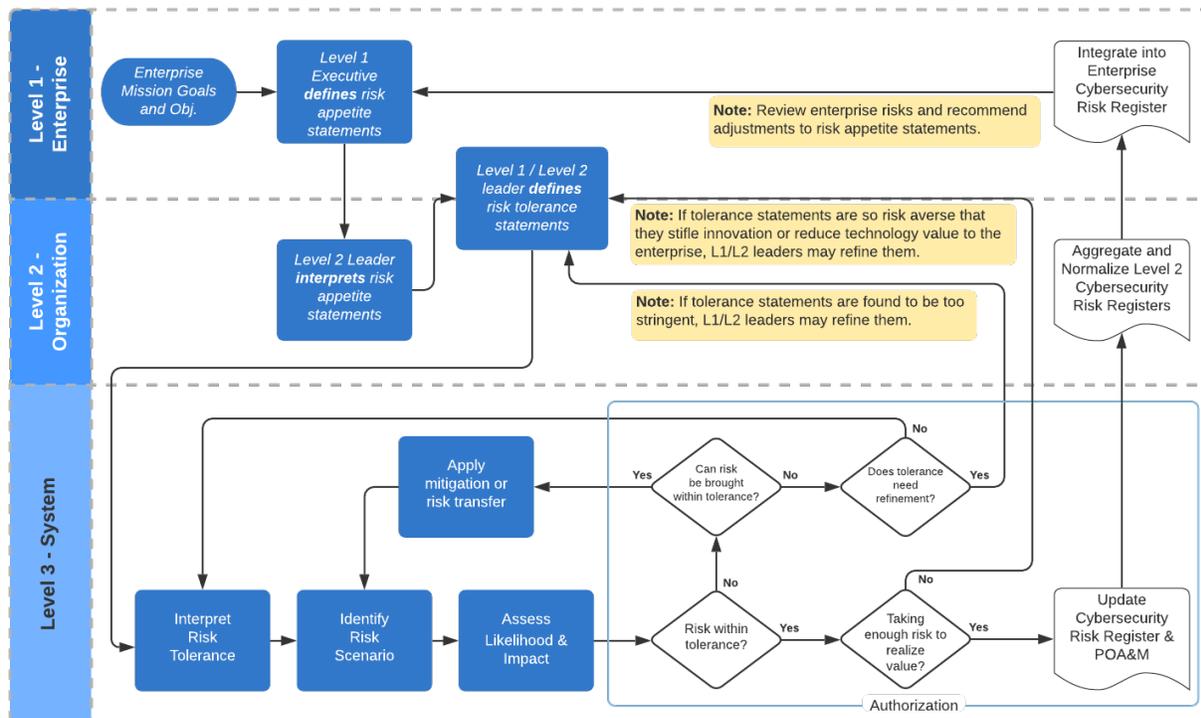
549   **Figure 6: Continuous Interaction Between ERM and CSRM Using the Risk Register**[12]

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

551   **Risk Context and Strategy Activities**

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

---

[12]   Figure 3 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 will
        describe how to apply risk analysis to prioritize risks and implement appropriate responses. NISTIR 8286C will provide
        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.

555   • At Level 3, practitioners interpret the risk tolerance statements for the specific systems
556   that operate to provide business (or agency) benefits. Those in various roles (e.g., system
557   owners, security officers) work together to derive system level requirements for
558   confidentiality, integrity, and availability.

559   **Risk Identification Activities**

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

564   • For each of these components, the practitioner identifies threat sources that might have a
565   harmful effect (see Section 2.2.2) and the vulnerabilities or conditions that might enable
566   such an effect (see Section 2.2.3). To complete development of the risk scenario, the
567   practitioner determines the adverse effect of the threat source exploiting the vulnerable
568   conditions. The scenario is recorded in the CSRR as the "Risk Description" (see Section
569   2.2.5). The category for the scenario will be recorded in the "Risk Category" column
570   based on enterprise criteria to support risk correlation, aggregation, and reporting.

571   **Risk Analysis Activities**

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

578   **Risk Response Activities**

579   • The determined exposure is compared with the risk tolerance.

580   o If exposure is within risk tolerance limits, the risk may be "**accepted**."

581   • If exposure exceeds tolerable levels of risk, practitioners can consider whether they can
582   achieve risk tolerance through other forms of risk response.

583   o In many cases, security controls may be applied to **mitigate** risk by reducing the
584   likelihood or impact of a risk to a tolerable level. Controls should be implemented
585   with a corresponding performance scale (i.e., KPI) which is used as the basis for
586   KRIs.

587   o Risk response may also include risk **transfer**, also known as risk sharing. For
588   example, an organization might hire an external organization to process sensitive
589   transactions (e.g., payment card transactions), thus reducing the likelihood that

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

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

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

Risk Monitoring and Communication Activities

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

612   • Results of risk activities and decisions are recorded in the CSRR and, if applicable, in a
613   documented Plan of Actions & Milestones (POA&M)[14] that records funded future
614   agreed-upon risk activities that will transpire over time.

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

619   • Risk activities may also be informed through the integration of relevant internal and
620   external audit findings. Significant audit findings often have enterprise level impacts;
621   however, lower severity findings may, if not addressed adequately, spread through
622   multiple systems to create risk in aggregate. The coordination of audit findings may span
623   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. Private industry is 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.

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

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

635 • Subsequently, CSRRs from throughout the business level are normalized and aggregated
636   to provide a composite view of the risk posture and decisions for that organization. As
637   Level 2 managers consider feedback from system CSRM activities, they may decide to
638   refine risk tolerance levels. It may be that the aggregate risk across multiple systems
639   represents too great an exposure and needs to be reduced. In other cases, based on
640   successful risk management results, stakeholders may be able to permit a little more risk
641   in some areas if such a decision would support mission objectives and potentially save
642   resources or allow them to be directed to areas that require additional resources in order
643   to meet expected risk tolerances.

644 • Similar reviews and refinement occur at Level 1 to support enterprise governance and
645   risk management decisions. Some types of enterprises may be required to formally
646   disclose risk factors (e.g., through annual reports), and this aggregate understanding of
647   cybersecurity risks and risk decisions can support their fiduciary responsibilities. These
648   activities may also help others, such as federal government agencies, to help comply with
649   mandatory requirements, such as those established by OMB.

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

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

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

2.1.4 Enterprise Strategy for Cybersecurity Risk Reporting

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

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

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

680 • Criteria regarding risk category selection that enables risk register entries from various
681   risk management domains to be consolidated and compared;

682 • Direction regarding the classification and valuation of enterprise assets, including
683   approved methods for business impact analysis (described in Section 2.2.1.1);

684 • Assessment methodologies, including direction regarding analysis techniques and the
685   appropriate scales to be applied;

686 • Frequency of assessment, reporting, and potential escalation;

687 • Methods for tracking, managing, and reporting risks; and,

688 • Resources available for risk treatment, including common baselines, common controls,
689   and supply chain considerations.

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

694 • Definition of the organizational boundaries to which CSRM activities will apply;
695   documentation that the scope for cybersecurity objectives supports alignment among
696   enterprise, business and mission objectives, and operational achievements

697 • Direction regarding specific roles for managing, communicating, and integrating risks
698   throughout the enterprise; defining the types of stakeholders (by role) will support risk
699   communication and timely decision-making

700   •   Determination of key risk indicators (KRIs) and key performance indicators (KPIs) that
701   will support the management and monitoring of the extent to which risk response remains
702   within acceptable levels

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

2.2   Risk Identification

708 This section describes methods for identifying and documenting sources and their potential
709 consequences (recorded in the Risk Description column of the CSRR, as shown by the red border
710 in Figure 7.) [15]

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											

711

Figure 7: CSRR Highlighting Risk Description Column

713 Risk identification represents a critical activity for determining the uncertainty that can impact
714 mission objectives. NISTIR 8286A primarily focuses on negative risks (i.e., threats and
715 vulnerabilities that lead to harmful consequences), but positive risks represent a significant
716 opportunity and should be documented and reviewed as well. Consideration and details
717 regarding positive risks will be addressed in subsequent publications. Through the activities in
718 the following sections, risk practitioners determine and record events that could enhance or
719 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.
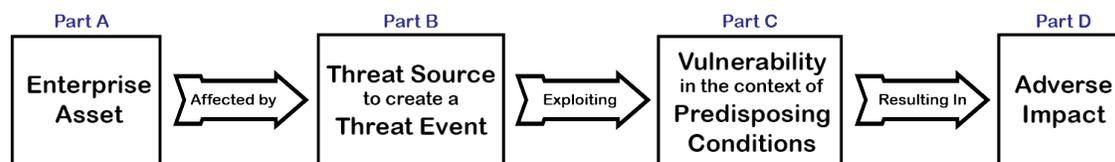
720

721   **Figure 8: Inputs to Risk Scenario Identification[16]**

722   As shown in Figure 8, which is derived from the Generic Risk Model in NIST SP 800-30,
723   Revision 1, *Guide for Conducting Risk Assessments*, cybersecurity risk identification is
724   composed of four necessary inputs – parts A through D – in the Risk Description cell of the
725   cybersecurity risk register [7]. Combining these elements into a risk scenario helps to provide the
726   full context of a potential loss event. The use of this scenario-based approach helps ensure
727   comprehensive risk identification by considering many types of physical and logical events that
728   might occur. The scope of cybersecurity has expanded from its original boundaries of adversarial
729   digital attacks and encompasses all types of uncertainty that can impact any form of information
730   and technology. Accordingly, the risks to be identified and registered are much broader as well.

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

733   • Part A – Identification of the organization's relevant assets and their valuation

734   • Part B – Determination of potential threats that might jeopardize the confidentiality,
735   integrity, and availability of those assets

736   • Part C – Consideration of vulnerabilities or other predisposing conditions of assets that
737   make a threat event possible

738   • Part D – High-level evaluation of the potential consequences if the threat source (part B)
739   exploits the weakness (part C) against the organizational asset (part A)

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

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

748   **2.2.1   Inventory and Valuation of Assets**

749   The first prerequisite for risk identification is the determination of enterprise assets that could be
750   affected by risk (part A in Figure 8). Assets are not limited to technology; they include any

---

16   Positive risks apply a similar process through which an enterprise asset considers an opportunity that takes advantage of a
     new or preexisting condition that results in a positive impact (benefit) to the enterprise.

751   resource that helps to achieve mission objectives (e.g., people, facilities, critical data, intellectual
752   property, and services).[17]

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

2.2.1.1   Business Impact Analysis

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

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

774   • Would loss or theft of the resource compromise customer or enterprise private
775   information?

776   • Would disclosure of an asset's information trigger legal or regulatory fines or actions?

777   • Would a lack of availability of the asset interrupt the enterprise's ability to fulfill its
778   mission or result in costly downtime?

779   • Would the lack of confidentiality, integrity, or availability of the asset undermine public
780   or consumer confidence or trust in the enterprise?

781   • Do internal or external critical resources depend on this asset to operate?

782   • For government systems, would loss or theft of the resource or information cause grave
783   damage to national security?

---

[17]   NIST SP 800-37, Revision 2, points out that risk could impact "organizational operations (including mission, functions,
        image, or reputation), organizational assets, or individuals."

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

787   ### 2.2.1.2   Determination of High-Value Assets

788   An example of asset valuation is the U.S. Government's designation of "high-value assets," or
789   HVAs,[18] described in OMB Memorandum M-19-03 as representing agency resources that have
790   been deemed highly sensitive or critical to achieving the business mission [8]. While not all
791   critical federal assets will be characterized as HVAs, OMB M-19-03 represents an example of an
792   enterprise approach to valuation since the memorandum defines the specific categories for
793   consistent designation (i.e., information value, role in Mission Essential Function support, and
794   role in support for Federal Civilian Essential Functions) yet permits each agency to determine
795   which assets meet those criteria. Other common industry examples include the use of specific
796   classifications to reflect the sensitivity and criticality of technology and information, including
797   "Company Confidential" or "Business Sensitive."

798   ### 2.2.1.3   Automation Support for Inventory Accuracy

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

804   Automated tools can aid in discovering and monitoring various technical components used by
805   the enterprise. For example, a use case described by the NIST Security Content Automation
806   Protocol (SCAP) specification is *inventory scanning*. Products that have been successfully
807   reviewed as part of the SCAP Validation Program help maintain a comprehensive and accurate
808   inventory of digital assets [9]. Valuation information recorded in that inventory can, in turn, help
809   maintain a comprehensive view of the enterprise assets for which cybersecurity risks should be
810   identified, analyzed, treated, and monitored. The use of automation helps to ensure that
811   enterprise asset inventory is current, accurate, and complete.

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

816   ### 2.2.2   Determination of Potential Threats

817   The enumeration of potential threat sources and the threat events that those sources could
818   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].

819 represents part B of the Risk Description cell of the CSRR. Because information and
820 technology exist in many forms, this threat-informed risk management approach combines
821 data-driven processes (awareness of threats) and sound business judgment (consideration of
822 mission impact) to support comprehensive risk identification.
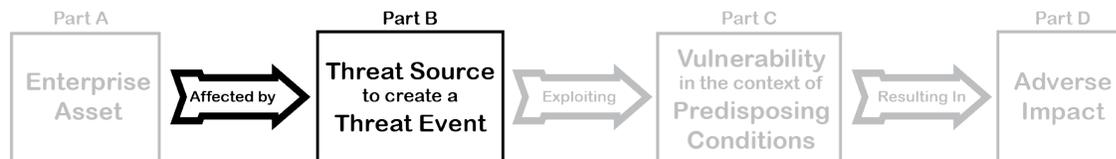
823

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

825 ### 2.2.2.1 Threat Enumeration

826 Many public- and private-sector processes are available to help enumerate threats. One example
827 is the OCTAVE Allegro method from Carnegie Mellon University's Software Engineering
828 Institute [10]. That model includes identification of areas of concern – a process for determining
829 the "possible conditions or situations that can threaten an organization's information asset." The
830 OCTAVE Allegro approach describes a process where risk managers create a tree diagram of
831 various threats based on:

832 • Human actors using technical means;

833 • Human actors using physical methods;

834 • Technical problems, such as hardware and software defects, malicious code (e.g.,
835 viruses), and other system-related problems; and

836 • Other problems that are outside of the control of an organization (e.g., natural disasters,
837 unavailability of critical infrastructures).

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

841 **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

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

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

851 •   What might a human actor accidentally disclose, modify, or destroy?

852 •   What information or technology might a person (e.g., a disgruntled employee)
853   *intentionally* disclose, interrupt, or delete?

854 •   Are there threat conditions that might be introduced by supply chain partners, such as
855   external service providers?

856 •   Are any cyber-physical systems or other operational technology (OT) subject to an attack
857   that might impact safety or otherwise affect enterprise operations?

858 •   What similar considerations might apply to accidents or intentional actions from an
859   external source using technical means?

860 •   What technical flaws or malicious code might affect valuable systems and lead to adverse
861   impacts on enterprise objectives?

862 •   What natural disasters or utility outages might have harmful effects?

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

868 **2.2.2.2   Reducing Unwanted Bias in Threat Considerations**

869 While cybersecurity threat discussions often focus on the intentional and adversarial digital
870 attack, it is important that all risk practitioners consider a broad array of threat sources and
871 events. In addition, while highly unlikely scenarios might not need to be listed (e.g., a meteorite
872 crashing into the data center), risk managers should avoid dismissing threats prematurely. For

873   these reasons, practitioners will benefit from identifying and overcoming bias factors in
874   enumerating potential threat sources and the events they might cause. Consideration of these
875   factors will also help reconcile reactionary thinking with analytical reasoning. An intentional
876   approach to enumerate threats without bias helps to avoid complacency before an incident and
877   supports a proactive evaluation based on relevant data, trends, and current events.

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

879   **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

880   ### 2.2.2.3 Threat Enumeration Through SWOT Analysis

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

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

891   **Table 5: Example SWOT Analysis**

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

892   ### 2.2.2.4   Use of Gap Analysis to Identify Threats

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

900   NISTIR 8286 provides an example of the process described by the NIST Cybersecurity
901   Framework [6], which includes a set of activities that consider the five functions:

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

907   The framework decomposes the functions into categories, each of which is further described in
908   terms of strategic and tactical outcomes (subcategories). For each subcategory, the framework
909   recommends the creation of profile artifacts that document the *current* and *desired* (or target)
910   policies, processes, and practices. By documenting the "as-is" outcomes, organizations can
911   consider potential risk implications, including potential threat events. That information will later
912   help develop target state profiles. Table 6 provides an example excerpt from a current profile
913   with example threat considerations.

914   **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)

915   Another source of ideas for threat modeling is NIST SP 800-53, *Security and Privacy Controls*
916   *for Information Systems and Organizations*, which provides a catalog of security and privacy

917　controls[19] [11]. A companion document, SP 800-53A, *Assessing Security and Privacy Controls*
918　*in Federal Information Systems and Organizations: Building Effective Assessment Plans*,
919　documents methods for assessing the effectiveness and suitability of those controls for various
920　purposes [12]. Through the examination of controls and assessment methods, practitioners can
921　observe conditions that align with enterprise situations, sparking discussions about potential
922　threats. For example:

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

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

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

944　**2.2.2.5　Technical Threat Enumeration**

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

951　To be successful in protecting information and technology and to rapidly detect, respond, and
952　recover from threat events, the organization may choose to apply an intelligence-driven
953　approach, commonly referenced as Cyber Threat Intelligence (CTI). Using sources of

---

[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.

954   information and data, such as those described in Table 7, practitioners will gain insight into
955   adversaries' tactics, techniques, and procedures (TTPs) as well as other information about how to
956   prepare and what conditions to monitor.

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

966   **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.
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/

---

[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.

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

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

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

980   The free (DHS) AIS capability enables the exchange of cyber threat indicators
981   between the Federal Government and the private sector at machine speed. Threat
982   indicators are pieces of information like malicious IP addresses or the sender address
983   of a phishing email (although they can also be much more complicated).

984   AIS participants connect to a DHS-managed system in the Department's National
985   Cybersecurity and Communications Integration Center (NCCIC) that allows
986   bidirectional sharing of cyber threat indicators. A server housed at each participant's
987   location allows them to exchange indicators with the NCCIC. Participants will not
988   only receive DHS-developed indicators but can share indicators they have observed
989   in their own network defense efforts, which DHS will then share back out to all AIS
990   participants.[22]

991 An analysis of network packet capture data can help identify potential threats based on observed
992 traffic. Armed with understanding from CTI sources regarding TTPs and IoCs, practitioners will
993 be able to observe potential indicators and likely attack paths. In conjunction with past and
994 existing cyber incident information, organizations can use CTI to support internal risk
995 communication and risk analysis and to improve risk scenario development. In addition to the

---

[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] The NCCIC is part of the Cyber Information Sharing and Collaboration Program (CISCP) and is available at https://www.cisa.gov/ciscp.

996 technical advisories, the alerts and analysis reports at the DHS National Cyber Alert System
997 provide information about recent TTPs and how they have affected various enterprises.

2.2.3   Vulnerability Identification

999   For any of the various threat conditions described above to result in an impactful risk, each needs
1000 a vulnerable or predisposing condition that can be exploited. The identification of vulnerabilities
1001 or conditions that a threat source would use to cause impact is an important component of risk
1002 identification and represents part C (Figure 10) of the CSRM risk scenario.
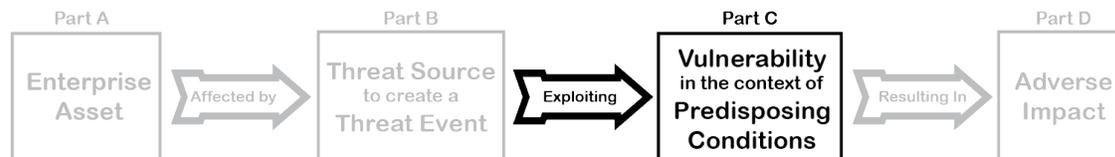
1003

1004   **Figure 10: Vulnerability Inputs to Risk Scenario Identification (Part C)**

2.2.3.1   Determination of Vulnerabilities and Predisposing Conditions

1006 While it is necessary to review threats and vulnerabilities as unique elements, they are often
1007 considered at the same time. Many organizations will consider a given loss scenario and evaluate
1008 both. What threat sources might initiate which threat events? What vulnerabilities or
1009 predisposing conditions might those threat sources exploit to cause a loss event?[23] Much of the
1010 information provided through CTI will also inform an understanding of vulnerability. For
1011 example, analysis of the infamous 2017 WannaCry ransomware attack includes understanding
1012 the threat source and motive (a known and capable cybercrime group seeking financial gain), the
1013 intended threat event (deliberate modification, interruption, and potential destruction of key
1014 enterprise information assets), and the vulnerability to be exploited by the adversary (CVE-2017-
1015 0144).

1016 Practitioners should (within the scope agreed upon in activities described in Section 2.1)
1017 systematically consider the potential physical and logical vulnerabilities and predisposing
1018 conditions that can be exploited by a threat source. This consideration can be facilitated by many
1019 of the methods described in Table 7, including:

1020 •   The use of commercial intelligence sources can provide threat and vulnerability
1021   information. Many providers will take note of a customer's enterprise information and
1022   technology (e.g., hardware, software, and operating systems in use) to alert the
1023   organization to any vulnerabilities in those platforms that are known to be targeted by
1024   existing threat sources.

1025 •   The integration of AIS feeds may include automated alerts regarding known
1026   vulnerabilities. Many security incident event monitoring (SIEM) products and intrusion

---

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

1027   detection systems (IDS) can help enterprises associate asset inventory information with
1028   AIS alerts to support incident reporting and monitoring.

1029   • A threat tree model (e.g., the diagram in the OCTAVE ALLEGRO guidance) can
1030   consider various human factors, technical defects, software flaws, physical entry points,
1031   utility dependencies, and supply chain vulnerabilities that present vulnerabilities.

1032   • A review of the various threat categorization models (e.g., MITRE ATT&CK®) can inspire
1033   internal discussions, such as "What vulnerabilities might enable execution of malicious
1034   code?" or "What predisposing conditions foster lateral movement within the enterprise?"

1035   As with threat modeling, practitioners will also benefit from applying known risk management
1036   frameworks as a tool for vulnerability discovery. For example, a review of the controls catalog in
1037   SP 800-53 may lead to consideration of control MP-3, Media Marking, which can then inspire
1038   discussion regarding potential vulnerabilities that might result from unmarked (or improperly
1039   marked) system media.

1040   Notably, the enterprise will benefit from the advice of external specialists with expertise in
1041   identifying and categorizing various types of vulnerabilities. Some entities, such as those
1042   operating moderate- and high-impact federal information systems, require formal penetration
1043   testing to identify potential vulnerabilities and the exploitability of those conditions. In addition
1044   to some government and law enforcement agencies that are able to assist enterprises with
1045   evaluating physical and technical vulnerabilities, many commercial organizations offer these
1046   services.

2.2.3.2   System Complexity as a Vulnerability

1048   NISTIR 8286 states that additional risks can result from the dynamic complexity of enterprise
1049   information and technology. In fact, that complexity is itself a vulnerability to be considered and
1050   documented. Evaluation of "what-if" scenarios regarding potential vulnerabilities, especially
1051   those affecting critical assets, should include the determination of critical dependencies on other
1052   resources. Because risk identification and risk analysis are iterative, risk analysis methods (such
1053   as the Event Tree Analysis described in Section 2.3.2.2) will help determine those dependencies.
1054   Having made that determination, those critical dependencies can be recorded in the BIA
1055   (described in Section 2.2.1.1). Risk identification then includes scenario discussions that evaluate
1056   complex or cascading events as vulnerabilities to be identified.

1057   For example, the 2003 Northeast Power Grid interruption demonstrated how several moderate
1058   risk events cascaded into a national emergency. Another example of systemic risk are the
1059   financial institutions that were impacted by cascading risk in 2008. In that case, large enterprises
1060   experienced catastrophic events because they had interdependencies with other banks, insurance
1061   companies, and customers. When identifying and recording risks in the register, such emerging
1062   risk conditions created by the interdependence of systems and counterparty risk must also be
1063   identified, tracked, and managed using the same methods described for more straightforward
1064   scenarios.

1065　As with other CSRM components, vulnerability identification can be considered through either
1066　qualitative or quantitative means. An organization might determine that it has a large number of
1067　high severity vulnerabilities based on an internal review. A qualitative review might result from
1068　a gap analysis between NIST Cybersecurity Framework Current State and Target State profiles
1069　since such an analysis is intended to foster discussion and communication regarding risks but
1070　will not likely produce a highly specific quantitative result.

1071　More quantitative vulnerability identification results from a formal testing approach that
1072　examines a discrete set of enterprise resources for a specified set of known vulnerabilities.
1073　Particular vulnerability assessments (e.g., software code review or simulated phishing attack) can
1074　provide quantitative results. Results of a formal assessment might include a specific number of
1075　identified issues, which can be used to help complete the likelihood column of the risk register.

1076　**2.2.3.3　Vulnerability Identification Automation**

1077　The complexity and interconnection of technology results in many thousands of potential
1078　vulnerabilities. Because of this broad scale combined with a rapidly evolving technical
1079　landscape, automation can improve the enterprise's ability to manage relevant vulnerabilities.
1080　Automation also enables a timelier monitoring of risk as well as adaptation to changing risk
1081　scenarios.

1082　Hardware and software products are significant sources of vulnerabilities for any enterprise,
1083　whether through inherent flaws in those products or through errors in product implementation or
1084　application. To help support the consistent identification and monitoring of these vulnerabilities,
1085　security organizations have developed broad clearinghouses of vulnerability information. For
1086　example, NIST operates the National Vulnerability Database (NVD) and the National Checklist
1087　Program (NCP) to support vulnerability and security configuration management via catalogs of:

1088　　　• Configuration checklists for securing key information technologies,

1089　　　• Information about secure configuration settings (with associated SP 800-53 security
1090　　　　controls),

1091　　　• Vulnerabilities (with associated severity scores),

1092　　　• Standardized security checklists for automated security configuration scanning (e.g.,
1093　　　　security checklists in Security Content Automation Protocol format[24]), and

1094　　　• Products that use standards to identify and report vulnerabilities.

1095　Automated data feeds, such as those described above, enable enterprise monitoring tools to
1096　ingest information about known vulnerabilities in near-real time and compare them with the asset
1097　inventory. A key factor in that data feed is information regarding the date that a vulnerability was
1098　publicly disclosed. The severity of a given vulnerability increases exponentially after it becomes
1099　publicly known, so it is important that practitioners prioritize remediation of flaws. The risk of
1100　the vulnerability must be balanced with the risk of implementing a fix for that issue too quickly.

---

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

1101   Automated tools can help monitor and maintain that balance through specific reports regarding
1102   severe vulnerabilities that have not been patched within a reasonable time. An example of this is
1103   the DHS AWARE (Agency-Wide Adaptive Risk Enumeration) scoring methodology used by the
1104   DHS Continuous Diagnostics and Mitigation (CDM) risk management dashboard. AWARE is
1105   not intended to identify all issues, but the scoring methodology helps to highlight and prioritize
1106   cybersecurity risks that are likely to exceed allowable risk tolerance (e.g., known software
1107   vulnerabilities on critical assets that are not mitigated within a designated grace period).[25]

2.2.4   Determining Potential Impact

1109   The final prerequisite for creating a practical list of risk scenarios for the risk register is the
1110   determination of the potential impact of the threats and vulnerabilities described above. The
1111   section below describes the completion of part D of the CSRM Risk Description column (Figure
1112   11.)
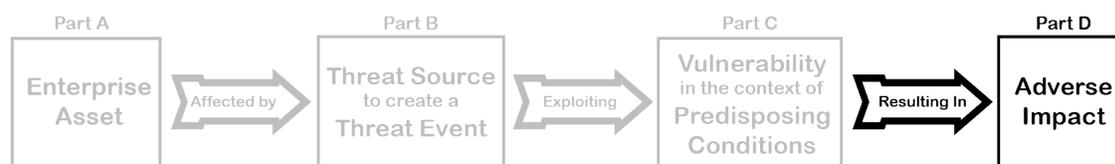
1113

1114   **Figure 11: Adverse Impact Inclusion in Risk Scenario Identification (Part D)**

1115   Discovery activities throughout Section 2.2 may have already highlighted potential adverse
1116   impacts to explore. Description of the impact is a key element for enterprise stakeholders and
1117   represents the connection between cybersecurity risks and the enterprise objectives that would be
1118   affected by those risks. Reviewing the key enterprise objectives, as identified in scoping, and
1119   armed with a broad list of potential threats and vulnerabilities, personnel can develop a list of
1120   realistic scenarios.

1121   While some types of impact may not be immediately apparent, the long-term effects can be
1122   significant. For example, consider a situation where a criminal has gained unauthorized access to
1123   an enterprise system and has exfiltrated a large amount of confidential data. If that criminal is
1124   cautious, there may not be any disruption of operations. In fact, sometimes cyber criminals
1125   actually try to *improve* the health of a victim's technology to ensure that it will be available for
1126   their malicious activity. In this case, the system may seem to be working fine – even better than
1127   ever – and then later, the enterprise realizes that a catastrophic loss has occurred.

1128   Notably, impact scenarios can be considered as a continuum rather than as a binary state. Many
1129   impacts will cause mission degradation or reduced performance and may not exhibit themselves
1130   as a full interruption of service or capability. This consideration should be factored into risk
1131   prioritization and analysis.

---

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

1132 Risk scenarios should be assessed in terms of both initial impact and downstream consequences.
1133 Factors to consider include:

1134 • Primary impact – The initial impact following a negative cybersecurity event, such as the
1135   downtime when a website is unavailable to customers

1136 • Secondary impact – A loss event that occurs subsequent to the primary impact as a
1137   downstream or cascading impact to the enterprise

1138 For example, consider a large enterprise that experiences a breach of confidential customer data.
1139 In this example, an external attacker with criminal intent might attack a highly critical and
1140 sensitive customer database through a software vulnerability in the internet-facing website. The
1141 initial impact may be minimal since exfiltration is not disruptive, and the company may not even
1142 detect an issue. Once the problem has been discovered, there may be primary impacts, such as:

1143 • Cost of a focused investigation into the breach

1144 • Price of restitution for customer losses (e.g., credit monitoring services)

1145 • The expense of third-party specialists to provide forensic expertise and to ensure
1146   adequate mitigation of the cybersecurity incident

1147 • Cost of immediate capital investment to address cybersecurity issues that contributed to
1148   the breach

1149 Long-term or secondary effects may be more impactful. They can include:

1150 • Loss of market share due to eroded trust in the company's reputation

1151 • Revenue losses from organizations that choose not to renew contracts

1152 • Fines and penalties from regulators

1153 When considering the impact component of risk scenarios, it is important to consider the
1154 frequency of potential consequences. A risk event of moderate impact that occurs weekly may,
1155 over time, represent a higher risk than that of a major event that occurs infrequently. Such
1156 temporal factors may be valuable for stakeholders' understanding and reporting of risks. For
1157 example, senior leaders may wish to see the impact of a risk expressed as the loss for each
1158 occurrence (the *single loss expectancy,* or *SLE*), or they might prefer to see the total loss for that
1159 risk over an annual period (the *annualized loss expectancy,* or *ALE*). Consistent documentation
1160 of impact frequency is also important for supporting the integration and aggregation of risk
1161 registers.

1162 As with other risk components, impact considerations may be either qualitative or quantitative,
1163 as illustrated by the examples in Table 8.

1164   **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 record relevant cybersecurity risks in the risk register.

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 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

1182 continually changing, so CSRM is an iterative activity of ongoing discovery, communication,
1183 response, and monitoring. In addition to the known risks that are already being monitored, there
1184 may also be developing or *emergent risks* that are yet to be fully defined but might disrupt
1185 enterprise objectives in the future.

1186 Each of the activities in Section 2.2 is iterative and supports the top-down/bottom-up approach
1187 described above. An if/then scenario analysis can be developed and used to consider threats and
1188 vulnerabilities, which may lead to the discovery of additional risk scenarios to be considered.
1189 This iterative process can be adjusted and tailored to develop and maintain a practical and
1190 manageable set of risks.

1191 As an example, consider some high-value assets that are important to a local hospital and issues
1192 that could jeopardize those assets. Some top-down considerations may include:

1193 • Patient record database – A ransomware attack could encrypt critical records; a network
1194   outage could disrupt availability; an authentication issue could hamper the ability to log
1195   in; a software upgrade could inadvertently corrupt the data.

1196 • Pharmaceutical system provided by a third party – A malicious (or tricked) insider could
1197   alter pharmacy records, resulting in incorrect medication being given to a patient; the
1198   malicious external party could break in and disclose or destroy pharmacy records; a
1199   construction incident could sever network communications to the service.

1200 • Point of care (PoC) terminals – Authentication system failure could disrupt the ability to
1201   provide patient care; user data error could result in inaccurate and potentially unsafe
1202   patient conditions; an improperly tested software patch could render terminals unusable.

1203 Bottom-up considerations start with threats and vulnerabilities and consider where those can
1204 lead:

1205 • Ransomware attack through a social engineering attack (e.g., web-based malware drive-
1206   by attack, email phishing attack) – An attack could render many systems unreadable,
1207   including patient care databases, pharmacy records, billing systems, and payroll.

1208 • Network outage due to a firewall malfunction – An internal failure of a major switch or
1209   router could result in localized failures of PoC terminals, patient in-processing, and
1210   medical care services (e.g., review of radiology reports). External connectivity failure
1211   would disrupt electronic mail, clinical professional services, pharmaceutical processing,
1212   some laboratory results.

1213 • Physical hardware malfunction through a failed component – Technical equipment (e.g.,
1214   televisions) could be rendered unavailable with few consequences, and technology (e.g.,
1215   patient scanners) malfunctions could fail to provide timely and accurate patient results.
1216   Awaiting replacement systems could lead to potential injuries (e.g., through fire or
1217   electrical shock) or delays in patient care.

1218 Thorough risk identification in realistic and mission-oriented scenarios help to communicate the
1219 connection between various uncertainties and the mission objectives that might be affected.

1220 **2.2.6   Risk Categorization**

1221 Each risk in the CSRR should also indicate the relevant risk category (indicated by the yellow
1222 dashed box in Figure 13) based on the risk strategy guidance described in Section 2.1. Categories
1223 could be any taxonomy that helps aggregate risk information and supports the integration of
1224 cybersecurity risk registers for ERM decision support. Example risk categories include:

1225 • Risk framework groupings, such as NIST RMF families (e.g., Access Control, Supply
1226   Chain Risk Management)

1227 • Threat types, such as intentional disclosures, unintended modifications, system failures,
1228   or natural disasters

1229 • Impact considerations based on business units affected or information systems impacted

1230 Consistent risk categorization supports the effective integration of cybersecurity risks throughout
1231 the enterprise and aggregation into an enterprise cybersecurity risk register. That information
1232 ultimately becomes part of the overall Enterprise Risk Register and the Enterprise Risk Profile.

1233 **2.3   Detailed Risk Analysis**

1234

1235 **Figure 13: CSRR Highlighting Risk Category and Current Assessment Columns**

1236 Risk analysis enables the determination of the likelihood of impact and priority of treatment.
1237 This section helps to complete the likelihood and impact columns of the cybersecurity risk
1238 register and the exposure column that represents the product of those two values. These columns
1239 are illustrated by the solid red box in Figure 13.

1240 Because cybersecurity risk reflects the effect of uncertainty on or within a digital component that
1241 supports enterprise objectives, risk analysis helps to measure both the level of uncertainty
1242 entailed by the risk scenario and the extent of the uncertain effect upon enterprise objectives.
1243 Deterministic models can provide a detailed analysis of likelihood and impact where sufficient
1244 information is available for such a determination. In other cases, the randomness of uncertainty
1245 and the many factors involved in complex information and technology better support a
1246 probabilistic (or stochastic) methodology.

1247   ### 2.3.1 Selecting Risk Analysis Methodologies

1248   International Electrotechnical Commission (IEC) standard 31010:2019, *Risk management —*
1249   *Risk assessment techniques*, provides a comprehensive list of risk analysis techniques. The
1250   standard states,

1251   In deciding whether a qualitative or quantitative technique is more appropriate,
1252   the main criteria to consider are the form of output of most use to stakeholders
1253   and the availability and reliability of data. Quantitative techniques generally
1254   require high quality data if they are to provide meaningful results. However, in
1255   some cases where data is not sufficient, the rigor needed to apply a quantitative
1256   technique can provide an improved understanding of the risk, even though the
1257   result of the calculation might be uncertain [13].

1258   The Open Group Standard for Risk Taxonomy (O-RT), part of the OpenFAIR series of
1259   documents, supports the assertion that quantitative risk analysis can provide an improved
1260   understanding of risk [14]. It points out,

1261   While there's nothing inherently wrong with a qualitative approach in many
1262   circumstances, a quantitative approach provides better clarity and is more useful
1263   to most decision-makers – even if it's imprecise. For example, [one] may not have
1264   years of empirical data documenting how frequently cleaning crew employees
1265   abuse usernames and passwords on sticky-notes, but [we] can make a reasonable
1266   estimate using ranges, particularly if [we] have been trained in how to make
1267   estimates effectively.

1268   Analysis considerations are often provided in a qualitative way, such as, "The patient database is
1269   at high risk of unauthorized disclosure because we have learned that hackers are targeting health
1270   information systems with ransomware, and we have determined that there are numerous
1271   vulnerabilities in our health information system."

1272   In other cases, the analysis can be quantitative, such as in the example below:

1273   The health information system contains about 12,000 records. A successful ransomware
1274   breach could cost approximately $1.3 million if the data is destroyed or $2.5 million
1275   dollars if the breach results in a disclosure. We know that the Arctic Zebra APT team has
1276   been targeting similar databases; through our understanding of their techniques and those
1277   of others, we believe that there is a 70 % chance they will target us and a 30 % chance
1278   (based on internal testing and network scans) that it would be successful. Based on that
1279   data, we believe that there is a 21 % chance of single loss exposure, or between $273,000
1280   and $525,000. This exposure calculation does not consider additional secondary losses,
1281   such as lost revenue due to customer erosion from loss of trust or personal lawsuits
1282   against the firm.

1283   As shown by the referenced standards and examples in this section, there are benefits to both
1284   qualitative and quantitative risk analysis methodologies and even the use of multiple

1285   methodologies, based on enterprise strategy, organization preference, and data availability.
1286   Regardless of the methodologies being applied, it is important to consider as many data points as
1287   needed to render a judgement regarding likelihood and impact values. Unfortunately, without
1288   supporting data, well-intentioned but misguided methods of risk analysis amount to little more
1289   than a guess. In many cases, the application of even a moderate amount of deductive reasoning,
1290   combined with various analysis techniques, can render a more accurate and reliable risk analysis.
1291   Quantitatively informed qualitative decision-making should be the objective in the absence of
1292   purely quantitative-driven decisions.

1293   Because CSRM is intended to inform ERM activities, the selection and application of risk
1294   analysis methods must be aligned. The enterprise CSRM strategy should inform risk analysis
1295   methodologies, support coordination, and direct the consistent use of available data. As with
1296   many risk management elements, the strategy should help consider the methods available and
1297   provide for a tailored approach that results in effective risk management.

1298   When selecting a risk assessment technique, organizations should consider the costs of analysis
1299   in light of the desired outcome to help determine the most cost-effective technique. An
1300   inexpensive but accurate qualitative analysis that identifies the most risks and leads to mitigating
1301   those risks to the best possible degree may be the right move for a particular organization. For
1302   others, a highly detailed quantitative risk assessment may require more resources than a
1303   qualitative approach but may also provide specific and actionable information that helps to focus
1304   attention on important threat scenarios.

1305   **2.3.2   Techniques for Estimating Likelihood and Impact**

1306   NISTIR 8286 highlights the need for improved risk analysis when estimating and recording the
1307   likelihood and impact of cybersecurity events and monitoring to ensure that risks remain within
1308   acceptable parameters.[26] To improve enterprise risk estimation accuracy and consistency, CSRM
1309   practitioners are encouraged to explore the use of tools and processes that support measurable
1310   and meaningful risk analysis and reporting.

1311   Some analysis techniques are based on estimates from subject matter experts' (SMEs) experience
1312   and knowledge. Some methods, such as this SME estimation, can be subjective. Other methods
1313   are more objective and based on analytical considerations, statistical analysis, and scenario
1314   modeling, as well as potentially drawing on knowledge of previous events.

1315   Understanding the intended purpose of the analysis can help one decide which techniques to use.
1316   For example, a detailed and quantified approach may be valuable as a basis for a comprehensive
1317   review or update of the enterprise cybersecurity approach. Detailed evaluation helps to reinforce
1318   defense measures and increase resilience, as in the following example:

1319   Enterprise leaders have learned through an InfraGard alert that there is a high
1320   probability that companies in its sector will be targeted by a particular APT group.

---

[26]   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.

1321 Because internal cybersecurity risk managers have performed threat modeling based
1322 on the MITRE Adversarial Tactics, Techniques, and Common Knowledge
1323 (ATT&CK®) and Pre-ATT&CK frameworks, the company was able to quickly
1324 consider high-value assets that would most likely be at risk.

1325 A key TTP of this attack is "password spraying" brute force login attempts. Several
1326 critical systems have not yet been updated to support multi-factor authentication and
1327 would be vulnerable to such an attack. A poll of the security leaders in the
1328 organization (using a Delphi exercise) determined that there is a 50-70 % chance that
1329 the payroll system will be attacked (the mean value was 60 %). A successful attack on
1330 that system would have direct and indirect financial impacts of between $1.7 million
1331 and $2.4 million USD with the most likely impact being $2.0 million. Therefore, the
1332 risk exposure value for this row of the risk register was established at $1.2 million
1333 (based on .6 x $2 million).

1334 Notably, the example above provides several ranges of estimates. Some industry specialists have
1335 indicated that a range of possible values is more helpful and likely more accurate than a single
1336 "point estimate." Additionally, while this example uses the mean values of those ranges to
1337 identify the likelihood and potential impact, the ranges themselves are often recorded in the risk
1338 register. In this instance, given a possible impact of "between $1.7 million and $2.4 million," the
1339 exposure may have been presented as "$1.02 million to $1.44 million."

1340 2.3.2.1 Improving Estimation Based on Knowledge of Prior Events

1341 In many cases, information about previous risk events may be helpful when estimating the
1342 likelihood and impact of those in the future. For example, practitioners should consult industry
1343 literature, their current power companies, or internet service providers for descriptions of loss
1344 events within a given sector or over a particular time frame. To determine the likelihood of a
1345 utility outage, the utility provider can be asked to provide details regarding previous disruptions
1346 and their duration.

1347 As an example, consider the example organization in the first row in Table 1: Examples of Risk
1348 Appetite and Risk Tolerance. It describes a global retail firm at which a senior leader has
1349 expressed the risk tolerance statement that "any outage that exceeds four hours for any customer
1350 requires significant corrective action." Risk practitioners can review the actual availability of that
1351 website for the previous year (using a table similar to Table 9).

1352   **Table 9: Example Risk Tolerance Results Assessment**

Month	Total Hours in the Month	# of Hours Unavailable	Outage Customer %	Available Hours (Total Hours Outage)	Appetite Limit (99.95% of Total)	Tolerance Limit (Total - 4 hrs.)	Avail % (Avail. Hours + Total Hours)
Jan	744	1	2.4	743	743.628	739	99.87%
Feb	672			672	671.664	668	100.00%
Mar	744			744	743.628	740	100.00%
Apr	720	1.5	4.5	718.5	719.64	714.5	99.79%

Month	Total Hours in the Month	# of Hours Unavailable	Outage Customer %	Available Hours (Total Hours Outage)	Appetite Limit (99.95% of Total)	Tolerance Limit (Total - 4 hrs.)	Avail % (Avail. Hours + Total Hours)
May	744			744	743.628	740	100.00%
Jun	720			720	719.64	716	100.00%
Jul	744			744	743.628	740	100.00%
Aug	744			744	743.628	740	100.00%
Sep	720	2	0.5	718	719.64	714	99.72%
Oct	744			744	743.628	740	100.00%
Nov	720	3	1.5	717	719.64	713	99.58%
Dec	744			744	743.628	740	100.00%
Yearly	**8760**			**8752.5**	**8755.62**	**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,[27] illustrated in Figure 14, is useful because it considers the judgement of available subject matter experts (SMEs). For example, to determine the impact[28] 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

---

[27]   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.

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

1375   that the most likely impact of recovering from such a successful phishing attack would be
1376 $50,000. Each of these data points can be used to calculate the expected value (also known as
1377   EV, expectation, average, or mean value).
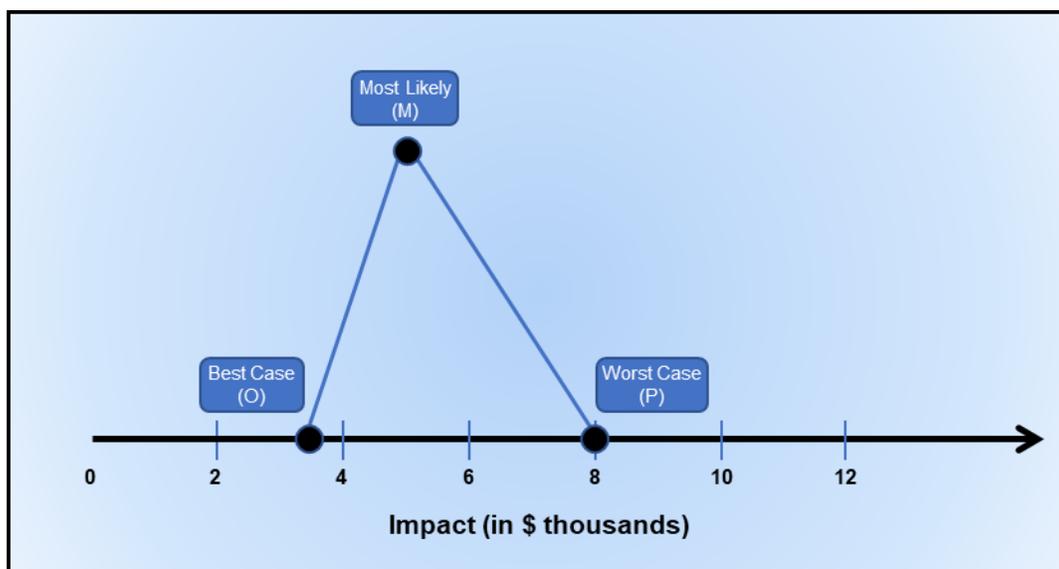
1378
1379   **Figure 14: Example Three-Point Estimate Graph (Triangle Distribution)**

1380   The three datapoints can be categorized as **O**ptimistic ($35,000), **P**essimistic ($80,000), and
1381   **M**ost likely ($50,000). A simple average of the three numbers (called a *Triangular Distribution*)
1382   is:

1383 $EV = \frac{P+M+O}{3}$ = $55,000 in this example, where O=$35,000, P=$80,000, and M=$50,000

1384   In this phishing attack scenario, perhaps the estimator believes that the pessimistic and optimistic
1385   values are too different and that the "most likely" estimate is a better predictor. The estimator
1386   can give greater weight (perhaps four times as much) to the "most likely" value using the
1387   following standard formula (called the *Average for a Beta Distribution*):

1388 $EV = \frac{P+4M+O}{6}$ = $52,5000 in this example, where O=$35,000, P=$80,000, and M=$50,000

1389   The next question is, "How confident is the estimator regarding this estimated impact of a
1390   successful phishing attack?" In three-point estimating, confidence (referred to as *sigma,* or *σ*) in
1391   the estimated value can be predicted by calculating the standard deviations from the mean. A
1392   useful model for determining sigma is $\sigma = \frac{P-O}{6}$.

1393   Figure 15 illustrates these values graphically. Statistical models have demonstrated that one can
1394   determine the level of confidence (or confidence interval [CI][29]) in the financial estimates given
1395   the mean (EV) and standard deviation. For the example above, the estimator will have a 68.27 %

---

[29]   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.)

1396 confidence that the financial impact of a successful phishing attack will result in a loss between
1397 $39,000 and $66,000. The estimator will have approximately a 95 % confidence that the loss will
1398 be between $25,500 and $79,500 and a nearly 100 % confidence in the $12,000 to $93,000
1399 estimate. This application of CI is useful for each of the analysis methods in this section and
1400 helps to represent the level of uncertainty in each of the estimates.
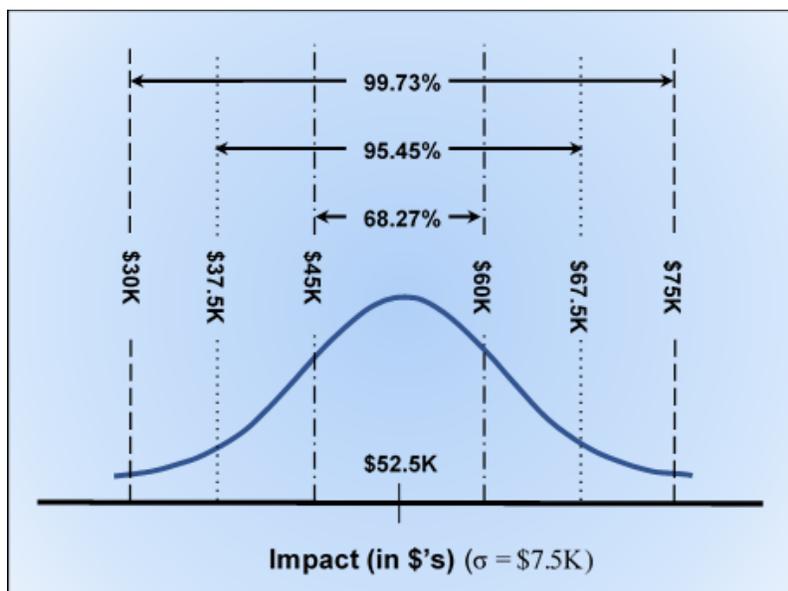
1401

1402 **Figure 15: Example Three-Point Estimate Graph (Normal Distribution)**

1403 Confidence requirements and standardized methods of calculation should be included in senior
1404 leaders' ERM strategy as part of enterprise risk management policy. This directive helps all risk
1405 practitioners in the enterprise consider risk in a similar manner and may help to improve the
1406 reliability of likelihood and impact estimates. Additionally, as more information becomes
1407 available regarding previous risk results and those of external organizations, this information can
1408 be included in the estimation models and used to reduce uncertainty.

1409 Notably, the level of effort for estimating risk factors increases with the required level of rigor.
1410 An estimate with very low CI might be simple to develop (perhaps as simple as flipping a coin)
1411 but likely offers little value. A CI of 99 % may be important in some situations, but the work to
1412 develop a more precise estimate can cost significantly more than that required for a 90 % CI.
1413 Because the appropriate levels of accuracy and precision for cybersecurity risk analysis will vary
1414 based on enterprise needs, the techniques and expectations should be clearly defined as part of
1415 the enterprise's risk management guidance.

1416 It is critical that the risk practitioner consider the accuracy of the SME estimates over time to
1417 determine who or what source is more accurate and then consider that expert judgement more
1418 prominently in calculations for the ongoing risk management cycles. Experts who are overly
1419 optimistic or pessimistic create a broad range. However, when accuracy is required, especially
1420 when calculating likelihood, knowing who the best estimators are in the organization is vitally
1421 important.

1422   **2.3.2.3   Event Tree Analysis**

1423   Event Tree Analysis (ETA) is a graphical technique that helps practitioners evaluate the
1424   downstream impact of a given scenario (as determined in Section 2.2.4.) In the same way that a
1425   Root Cause Analysis helps consider previous events that have already led to an event, ETA helps
1426   consider the potential consequences of future events. The exercise helps document a sequence of
1427   outcomes that could arise following an initiating threat event (e.g., a particular TTP, as described
1428   in Section 2.2.2). By iterating through a series of what-if scenarios, the practitioner can analyze
1429   each set of circumstances and determine the likelihood that the results would occur.

1430   Figure 11 demonstrates the layered defense that an organization employs to prevent malicious
1431   code from being used to exfiltrate data. For each condition, the analyst considers a Boolean (i.e.,
1432   true or false) answer. The analyst then follows through each iterative outcome until an end result
1433   is reached. This analysis can be performed in a qualitative way (using the yes or no conditions),
1434   or a probability could be calculated for each scenario. In Figure 11, the probability is calculated
1435   based on whether the attack was prevented (Yes) or if the attack was successful (No). Since each
1436   branch of the tree represents a binary option, the sum of the two probabilities is always equal to
1437   100 % (or 1.00 in decimal format). In this example, the calculated probabilities provide
1438   information about the potential success (or failure) of risk response. The resulting probability (*Pr*
1439   values in the example below) is multiplied by the anticipated financial loss of the scenario. In the
1440   tree below, if the anticipated loss of sensitive data being exfiltrated is $1.4 million, then there is a
1441 $205,100 risk exposure ($1.4 million x.1463).
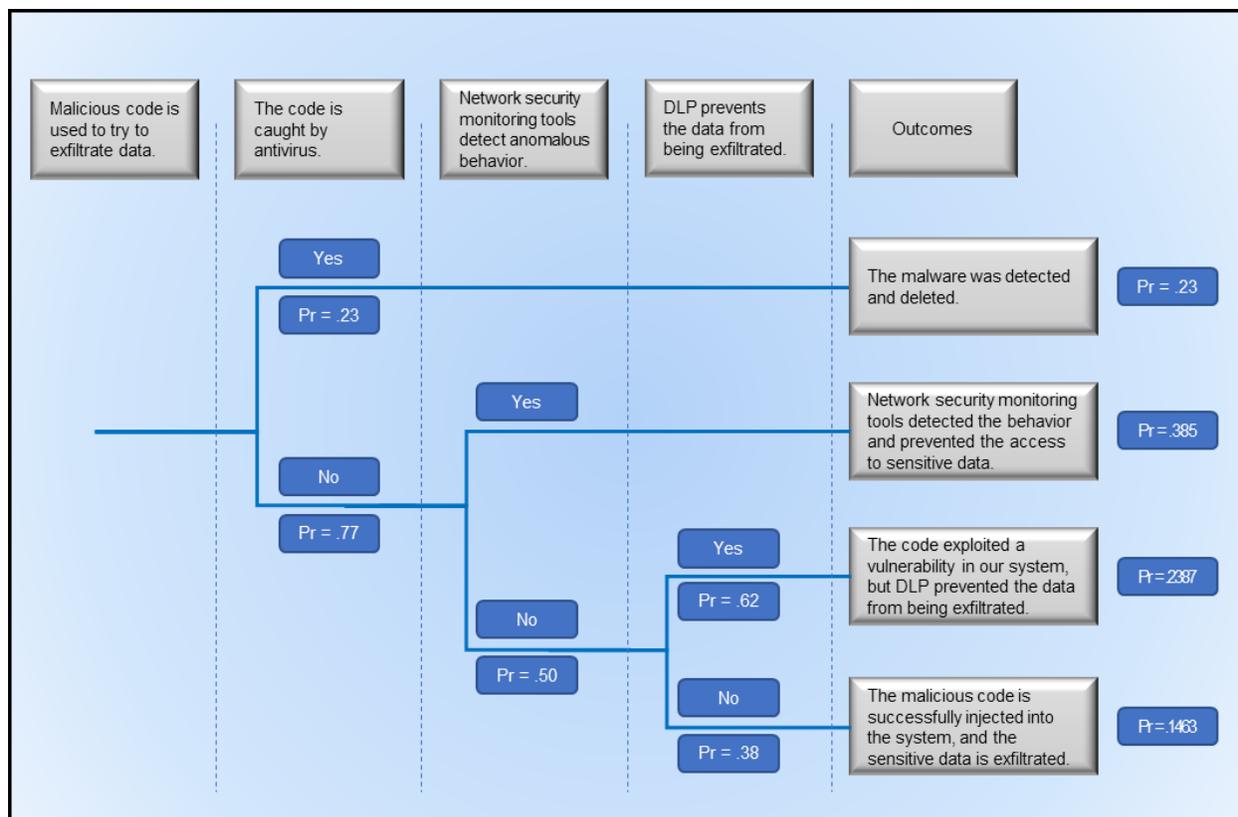
Figure 16: Example Event Tree Analysis

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.[30] The results of such a simulation can be plotted on a graph or
distribution to facilitate a visual understanding.

---

[30]   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.

1459　For example, when calculating the financial impact of the attack on the payroll system (from the
1460　example above), practitioners can use a simulation model to consider the most likely range
1461　between the low value ($1.7 million) and the high value ($2.4 million). The result of this
1462　simulation could be recorded as a histogram that records the frequency at which certain random
1463　values occurred, in this case resulting in a simulated estimated impact of $2 million.
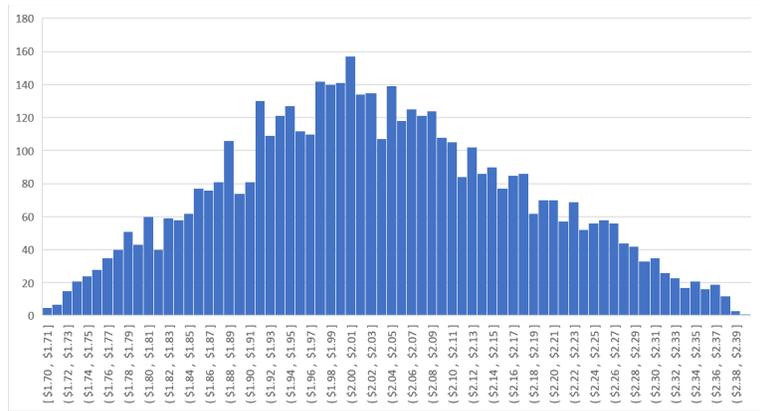
1464

1465　**Figure 17: Illustration of a Histogram from a Monte Carlo Estimation Simulation**

1466　**2.3.2.5　Bayesian Analysis**

1467　While there is value in using expert judgement to help estimate risk parameters, it might be
1468　improved based on information known from prior events, and the results may represent a more
1469　objective determination. For example, if the organization has identified that several critical
1470　software vulnerabilities have remained uncorrected, there is an increased likelihood that a threat
1471　actor will be able to exploit a software vulnerability to successfully gain access to the enterprise
1472　and exfiltrate valuable data. Bayesian analysis describes methods for considering conditional
1473　probability – applying a distribution model and a set of known prior data to help estimate the
1474　probability of a future outcome.

1475　While an SME might render an opinion regarding how likely a breach might be, that opinion can
1476　be improved by what the enterprise risk managers already know about the success of previous
1477　attempts by others or about the success of adversaries in similar enterprises. Prior knowledge,
1478　drawn from internal observations and events at similar organizations can be of significant value
1479　for improving the accuracy and reliability of estimates, such as those for determining the
1480　likelihood of an impactful event or for estimating the impact of that uncertainty on the enterprise
1481　objectives. Similar methods can be used to estimate whether several conditions might occur
1482　(joint probability) or that certain conditions would occur given other external variables (marginal
1483　probability).

1484 **2.4   Determination and Documentation of Risk Exposure**

1485 Once the probability that an impactful event will occur has been determined and the most
1486 probable impact of such an occurrence has been calculated, the information is recorded in the
1487 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

1488
1489   **Figure 18: Example Quantitative Analysis Results**

1490 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

1491
1492   **Figure 19: Example Qualitative Analysis Results**

1493 In this example, internal SMEs feel that the likelihood of an attack on the organization's mobile
1494 banking application is high. A survey of the SMEs reflects their determination that the impact to
1495 the organization if customers experience such an event would be high based on customers'
1496 perception that the application lacked sufficient security protections. In this case, the practitioner
1497 would use the enterprise assessment scale for determining qualitative risk, such as the application
1498 of Table I-2, *Assessment Scale – Level of Risk (Combination of Likelihood and Impact)*, from SP
1499 800-30, Revision 1. Based on that table, an event with a high likelihood and high impact would
1500 be ranked as a high exposure. As an example, this decision would help inform the selection of
1501 strong user authentication and encryption controls.

1502 Risk priority is described in NISTIR 8286B and will be determined based on mission objectives,
1503 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.

1533   **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]   Joint Task Force (2018) Risk Management Framework for Information Systems and
        Organizations: A System Life Cycle Approach for Security and Privacy. (National
        Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication
        (SP) 800-37, Rev. 2. https://doi.org/10.6028/NIST.SP.800-37r2

[6]   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

[7]   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

[8]   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

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

[10]   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

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

[12]   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

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

[14]   The Open Group. (2020) Risk Taxonomy (O-RT), Version 3.0 (OpenFAIR). Available
        at https://publications.opengroup.org/security-library/risk-analysis/c20b.

1534

1535 **Appendix A—Acronyms**

1536 Selected acronyms and abbreviations used in this paper are defined below.

1537	AIS	Automated Indicator Sharing
1538	ALE	Annualized Loss Expectancy
1539	APT	Advanced Persistent Threat
1540	BIA	Business Impact Analysis
1541	CCE	Common Configuration Enumeration
1542	CDM	Continuous Diagnostics and Mitigation
1543	CI	Confidence Interval
1544	CISA	Cybersecurity and Infrastructure Security Agency
1545	CMDB	Configuration Management Database
1546	CPE	Common Platform Enumeration
1547	CSRM	Cybersecurity Risk Management
1548	CTI	Cyber Threat Intelligence
1549	CVE	Common Vulnerabilities and Exposures
1550	CVSS	Common Vulnerability Scoring System
1551	DHS	Department of Homeland Security
1552	DIB	Defense Industrial Base
1553	DISCE	U.S. Department of Defense Information Sharing Environment
1554	ERM	Enterprise Risk Management
1555	ETA	Event Tree Analysis
1556	EV	Expected Value
1557	FOIA	Freedom of Information Act
1558	HVA	High-Value Asset

1559	IDS	Intrusion Detection Systems
1560	IEC	International Electrotechnical Commission
1561	IoC	Indicators of Compromise
1562	ISAC	Information Sharing Analysis Center
1563	ISAO	Information Sharing and Analysis Organization
1564	ITAM	Information Technology Asset Management
1565	ITL	Information Technology Laboratory
1566	NCCIC	National Cybersecurity and Communications Integration Center
1567	NISTIR	NIST Interagency or Internal Report
1568	NTCTF	NSA/CSS Technical Cyber Threat Framework
1569	NVD	National Vulnerability Database
1570	OLIR	Online Informative References
1571	OMB	Office of Management and Budget
1572	OVAL	Open Vulnerability Assessment Language
1573	RMF	Risk Management Framework
1574	SCAP	Security Content Automation Protocol
1575	SIEM	Security Incident Event Monitoring
1576	SME	Subject Matter Experts
1577	SWOT	Strength, Weakness, Opportunity, Threat
1578	TTP	Tactics, Techniques, and Procedures
1579	VPN	Virtual Private Network

1580　Appendix B—Notional Example of a Risk Detail Record (RDR)

1581　NISTIR 8286 pointed out that it may be helpful to record specific attributes and information
1582　about risk identification in a *risk detail record*, or RDR. As shown in the following notional
1583　example, an RDR may help provide information regarding each risk; roles and stakeholders
1584　involved in risk decisions and management; schedule considerations, such as the date the risk
1585　was first documented and the date of the next expected assessment; and risk response decisions
1586　and follow-up, including detailed plans, status, and risk indicators.

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		

1587　**Figure 21: Notional Risk Detail Record**