Withdrawn Draft

Warning Notice

The attached draft document has been withdrawn and is provided solely for historical purposes. It has been superseded by the document identified below.

Withdrawal Date July 6, 2021

Original Release Date December 14, 2020

Superseding Document

Status	2 nd Public Draft (2I	PD)
--------	----------------------------------	-----

Series/Number NIST Interagency or Internal Report 8286A

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

Publication Date July 2021

DOI https://doi.org/10.6028/NIST.IR.8286A-draft2

CSRC URL https://csrc.nist.gov/publications/detail/nistir/8286a/draft

Additional Information



1	Draft NISTIR 8286A
2	Identifying and Estimating
3	Cybersecurity Risk for Enterprise Risk
4	Management (ERM)
5	
6	Kevin Stine
7	Stephen Quinn
8 9	Larry Feldman Greg Witte
9 10	R. K. Gardner
11	
12	
13	
14	
15	This publication is available free of charge from:
16	https://doi.org/10.6028/NIST.IR.8286A-draft
17	
18	
19	



20]	Draft NISTIR 8286A
21	v O	and Estimating
22	Cybersecurity Risk for 1	Enterprise Risk
23	Mana	gement (ERM)
24		0 ()
25	Kevin Stine	Larry Feldman
		-
26 27	Applied Cybersecurity Division Information Technology Laboratory	Greg Witte
28	Information Technology Laboratory	Huntington Ingalls Industries Annapolis Junction, MD
29		
30	Stephen Quinn	R. K. Gardner
31	Computer Security Division	New World Technology Partners
32	Information Technology Laboratory	Annapolis, MD
33	Information Teennotogy Ducor alory	111114 0005, 112
34		
35		
36		
37	This publication i	s available free of charge from:
38		/10.6028/NIST.IR.8286A-draft
	https://doi.org	710.0020/10151.1R.0200A-draft
39		
40		
41		D 1 2020
42		December 2020
43		
44		SURFTIMENT OF COMMITMENT SURFTIMENT OF COMMITMENT SURFTIM
45 46 47 48 49		U.S. Department of Commerce Wilbur L. Ross, Jr., Secretary
49 50 51	Nat Walter Copan, NIST Director and Under Secretary of	ional Institute of Standards and Technology of Commerce for Standards and Technology

National Institute of Standards and Technology Walter Copan, NIST Director and Under Secretary of Commerce for Standards and Technology

52	National Institute of Standards and Technology Interagency or Internal Report 8286A
53	55 pages (December 2020)
54	This publication is available free of charge from:
55	https://doi.org/10.6028/NIST.IR.8286A-draft
56 57 58 59	Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the entities, materials, or equipment are necessarily the bes available for the purpose.
60	

60 There may be references in this publication to other publications currently under development by NIST in accordance 61 with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies, 62 may be used by federal agencies even before the completion of such companion publications. Thus, until each 63 publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For 64 planning and transition purposes, federal agencies may wish to closely follow the development of these new 65 publications by NIST.

66 Organizations are encouraged to review all draft publications during public comment periods and provide feedback to 67 68 NIST. Many NIST cybersecurity publications, other than the ones noted above, are available at https://csrc.nist.gov/publications.

69	Public comment period: December 14, 2020 through February 1, 2021 March 1, 2021
70	National Institute of Standards and Technology
71	Attn: Applied Cybersecurity Division, Information Technology Laboratory
72	100 Bureau Drive (Mail Stop 2000) Gaithersburg, MD 20899-2000
73	Email: <u>nistir8286@nist.gov</u>
74	All comments are subject to release under the Freedom of Information Act (FOIA).

Reports on Computer Systems Technology

76 The Information Technology Laboratory (ITL) at the National Institute of Standards and 77 Technology (NIST) promotes the U.S. economy and public welfare by providing technical 78 leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test 79 methods, reference data, proof of concept implementations, and technical analyses to advance the 80 development and productive use of information technology. ITL's responsibilities include the 81 development of management, administrative, technical, and physical standards and guidelines for 82 the cost-effective security and privacy of other than national security-related information in federal 83 information systems.

84

Abstract

85 This document supplements NIST Interagency/Internal Report 8286, *Integrating Cybersecurity*

86 and Enterprise Risk Management (ERM), by providing additional detail regarding risk guidance,

87 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

89 development of an enterprise risk register, this report describes documentation of various

90 scenarios based on the potential impact of threats and vulnerabilities on enterprise assets.

91 Documenting the likelihood and impact of various threat events through cybersecurity risk

92 registers integrated into an enterprise risk profile, helps to later prioritize and communicate

93 enterprise cybersecurity risk response and monitoring.

95 cybersecurity risk management; cybersecurity risk measurement; cybersecurity risk register;

- 96 enterprise risk management (ERM); enterprise risk profile.
- 97

94

Acknowledgments

98 The authors wish to thank those who have contributed to the creation of this draft. A detailed 99 acknowledgement will be included in the final publication.

100

Audience

Keywords

101 The primary audience for this publication includes both federal government and non-federal

102 government cybersecurity professionals at all levels who understand cybersecurity but may be

103 unfamiliar with the details of enterprise risk management (ERM).

104 The secondary audience includes both federal and non-federal government corporate officers,

105 high-level executives, ERM officers and staff members, and others who understand ERM but

106 may be unfamiliar with the details of cybersecurity.

107 This document begins with information generated at the enterprise level of the organization and

108 frames the discussion and the response from the risk management practitioners. All readers are

109 expected to gain an improved understanding of how cybersecurity risk management (CSRM) and

110 ERM complement and relate to each other, as well as the benefits of integrating their use.

Document Conventions

For the purposes of this document, the terms "cybersecurity" and "information security" are used 112

113 interchangeably. While technically different in that information security is generally considered

114 to be all-encompassing—including the cybersecurity domain—the term cybersecurity has

115 expanded in conventional usage to be equivalent to information security. Likewise, the terms 116

Cybersecurity Risk Management (CSRM) and Information Security Risk Management (ISRM)

- 117 are similarly used interchangeably based on the same reasoning.
- 118

Call for Patent Claims

This public review includes a call for information on essential patent claims (claims whose use 119

120 would be required for compliance with the guidance or requirements in this Information

121 Technology Laboratory (ITL) draft publication). Such guidance and/or requirements may be

directly stated in this ITL Publication or by reference to another publication. This call also 122

123 includes disclosure, where known, of the existence of pending U.S. or foreign patent applications

- 124 relating to this ITL draft publication and of any relevant unexpired U.S. or foreign patents.
- 125 ITL may require from the patent holder, or a party authorized to make assurances on its behalf, 126 in written or electronic form, either:
- assurance in the form of a general disclaimer to the effect that such party does not hold and 127 does not currently intend holding any essential patent claim(s); or 128

129 assurance that a license to such essential patent claim(s) will be made available to applicants

desiring to utilize the license for the purpose of complying with the guidance or requirements 130

- 131 in this ITL draft publication either:
- 132 under reasonable terms and conditions that are demonstrably free of any unfair
- 133 discrimination: or
- 134 without compensation and under reasonable terms and conditions that are demonstrably 135 free of any unfair discrimination.
- 136 Such assurance shall indicate that the patent holder (or third party authorized to make assurances
- 137 on its behalf) will include in any documents transferring ownership of patents subject to the

138 assurance, provisions sufficient to ensure that the commitments in the assurance are binding on

139 the transferee, and that the transferee will similarly include appropriate provisions in the event of

- 140 future transfers with the goal of binding each successor-in-interest.
- 141 The assurance shall also indicate that it is intended to be binding on successors-in-interest
- regardless of whether such provisions are included in the relevant transfer documents. 142
- 143 Such statements should be addressed to: nistir8286@nist.gov.

144			Table of Contents	
145	1	Intro	oduction	1
146		1.1	Supporting CSRM as an Integrated Component of ERM	1
147		1.2	Purpose and Scope	3
148		1.3	Document Structure	3
149	2	Cyb	ersecurity Risk Considerations Throughout the ERM Process	4
150		2.1	Risk Scope, Context, and Criteria	5
151			2.1.1 Risk Appetite and Risk Tolerance	5
152			2.1.2 Enterprise Strategy for Cybersecurity Risk Reporting	13
153		2.2	Risk Identification	14
154			2.2.1 Inventory and Valuation of Assets	16
155			2.2.2 Determination of Potential Threats	17
156			2.2.3 Vulnerability Identification	25
157			2.2.4 Determining Potential Impact	29
158			2.2.5 Recording Identified Risks	31
159			2.2.6 Risk Categorization	32
160		2.3	Detailed Risk Analysis	33
161			2.3.1 Selecting Risk Analysis Methodologies	33
162			2.3.2 Techniques for Estimating Likelihood and Impact	35
163		2.4	Determination and Documentation of Risk Exposure	42
164	3	Con	clusion	43
165	Re	feren	ces	44
166			List of Appendices	
167	Ap	pendi	x A— Acronyms	46
168	Ap	pendi	ix B— NVD/NCP Support for Vulnerability Identification and Analysis	s 48
169				
170			List of Figures	
171	Fig	gure 1:	Integration of CSRRs into Enterprise Risk Profile	2
172	Fig	gure 2:	Notional Cybersecurity Risk Register Template	4
173	Fig	gure 3:	Illustration of Enterprise Risk Communication and CSRM Coordination	7
174	Fig	gure 4:	Continuous Interaction between ERM and CSRM using the Risk Register	r 10
175	Fig	gure 5:	CSRR highlighting Risk Description Column	14

176	Figure 6: Inputs to Risk Scenario Identification	15
177	Figure 7: Threats as an Input to Risk Scenario Identification (Part B)	17
178	Figure 8: Vulnerability Inputs to Risk Scenario Identification (Part C)	26
179	Figure 9: Adverse Impact Inclusion in Risk Scenario Identification (Part D)	29
180	Figure 10: Example Risk Register with Sample Risk Descriptions	31
181	Figure 11: CSRR Highlighting Risk Category and Current Assessment Columns	33
182	Figure 12: Example Three-Point Estimate Graph (Triangle Distribution)	37
183	Figure 13: Example Three-Point Estimate Graph (Normal Distribution)	38
184	Figure 14: Example Event Tree Analysis	40
185	Figure 15: Illustration of a Histogram from a Monte Carlo Estimation Simulation	41
186	Figure 16: Example Quantitative Analysis Results	42
187	Figure 17: Example Qualitative Analysis Results	42
188	Figure 18: Use of a Cybersecurity Risk Register Improves Risk Communications	43
189	List of Tables	
190	Table 1: Inputs and Outputs for ERM Governance and Integrated CSRM	8
191	Table 2: Examples of Risk Appetite and Risk Tolerance	9
192	Table 3: Example Threat Modeling Analysis	18
193	Table 4: Example Bias Issues to Avoid in Risk Management	19
194	Table 5: Example SWOT Analysis	20
195	Table 6: Cybersecurity Framework Profiles Help Consider Threats	21
196	Table 7: Example Sources of Threat Information	24
197	Table 8: Example Negative and Positive Impact Scenarios	30

199

200 **1** Introduction

201 This report provides guidance that supplements NIST Interagency/Internal Report (NISTIR) 202 8286, Integrating Cybersecurity and Enterprise Risk Management (ERM) [1]. This is the first of 203 a series of companion publications that provide guidance for implementing, monitoring, and 204 maintaining an enterprise approach designed to integrate cybersecurity risk management 205 (CSRM) into ERM.¹ This is the first in a series of companion publications that provide guidance 206 for implementing, monitoring, and maintaining an enterprise approach designed to integrate cybersecurity risk management (CSRM) into ERM. Readers of this report will benefit from 207 208 reviewing the foundation document, NISTIR 8286, since many of the concepts described in this 209 report are based upon practices and definitions established in that NISTIR.

- A key point established by NISTIR 8286 is that the terms *organization* and *enterprise* are often
- 211 used interchangeably. That report defines an organization as an entity of any size, complexity, or
- 212 positioning within a larger organizational structure (e.g., a federal agency or company). It further
- 213 defines an *enterprise* as a unique type of organization, one in which individual senior leaders
- 214 govern at the highest point in the hierarchy and have unique risk management responsibilities
- such as fiduciary reporting and establishing risk strategy (e.g., risk appetite, methods). Notably,
- 216 government and private industry cybersecurity risk management (CSRM) and ERM programs
- 217 have different oversight and reporting requirements (e.g., accountability to Congress versus
- accountability to shareholders), but the general needs and processes are quite similar.

219 **1.1** Supporting CSRM as an Integrated Component of ERM

220 There are significant similarities and variances among approaches by public- and private-sector 221 practices for ERM/CSRM coordination and interaction. Notably, many ERM and CSRM 222 practices treat the two as separate stovepipes. This report highlights that CSRM is an integral 223 part of ERM, both taking its direction from ERM and informing it. The universe of risks facing 224 an enterprise includes many factors, and risks to the enterprise's information and technology 225 often rank high within that list. Therefore, ERM strategy and CSRM strategy are not divergent 226 but rather CSRM strategy should be a subset of ERM strategy with particular objectives, 227 processes, and reporting. Therefore, this report and those in this series provide a starting point for 228 further discussion about improving ERM and CSRM coordination. As the general risk 229 management community continues that discussion, NIST will continue to solicit and publish

- 230 lessons learned and shared by that community.
- 231 Section 2 shows that enterprise governance activities direct the strategy and methods for risk
- 232 management, including CSRM. Results of those activities are recorded in various risk registers.
- 233 Cybersecurity risks are documented through cybersecurity risk registers (CSRRs) that are
- aggregated at appropriate levels and are used to create an *enterprise* cybersecurity risk register,
- that, in turn, becomes part of a broader Enterprise Risk Register (ERR) as depicted in Figure 1.
- 236 The ERR, when prioritized by those with fiduciary responsibilities, represents an Enterprise Risk
- 237 Profile.

¹ For the purposes of this document, the terms "cybersecurity" and "information security" are used interchangeably.

- 238 Figure 1 also illustrates the
- 239 integration of risk register
- 240 information. The figure demonstrates
- that ERM and CSRM are not separate
- 242 processes, but CSRM represents an
- 243 important subset of risk management
- 244 under the broader umbrella of
- 245 enterprise risk management.
- 246The NISTIR 8286x series builds
- 247 upon existing NIST frameworks by
- 248 demonstrating methods for applying
- 249 risk management processes at all
- 250 enterprise levels and representing
- 251 how the NIST frameworks are
- anchored in ERM. A key construct
- 253 for performing that integration is the
- 254 cybersecurity risk register (CSRR)
- 255 described in NISTIR 8286.² As
- shown in Figure 1., the risk register is
- a key tool to document,
- communicate, and manage
- 259 cybersecurity risk at each level of the
- 260 enterprise.³



- 262 completing and maintaining that risk
- 263 register by identifying threats and

analyzing the likelihood of successful exploitation of certain conditions to result in threat events,

- the estimated impact on enterprise objectives, and whether estimates are within established risk tolerance parameters. This report focuses on the first three elements of the enterprise CSRM
- 267 process: establishing scope, context, and criteria; identifying the cybersecurity-related risks that
- 268 may affect an enterprise's ability to achieve its objectives; and calculating the likelihood and
- 269 impact of such risks. Subsequent publications will address methods for evaluating risk treatment
- 270 options, selecting an appropriate treatment, communicating the plans and results of that
- treatment, and adhering to stakeholders' risk strategies.



² 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.

³ 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.

272 **1.2 Purpose and Scope**

273 This document focuses on improving CSRM understanding and communications between and 274 among cybersecurity professionals, high-level executives, and corporate officers to help ensure 275 the effective integration of cybersecurity considerations as a critical subset of the overarching 276 enterprise risks. The report recognizes that the risk management community has observed an 277 opportunity for increased rigor in the manner in which cybersecurity risk identification, analysis, 278 and reporting are performed at all levels of the enterprise. This publication is designed to provide 279 guidance and to further conversations regarding ways to improve CSRM and the coordination of 280 CSRM with ERM.

- 281 The goals of this document are to:
- Help describe governance processes by which senior leaders build strategy and express
 expectations regarding CSRM as part of ERM and
- Provide guidance for CSRM practitioners in applying the risk direction received from senior leaders, communicating results, coordinating success, and integrating activities.
- 286 This document continues the discussion to bridge existing private industry risk management
- 287 processes with government-mandated federal agency enterprise and cybersecurity risk
- requirements derived from OMB Circulars A-123 and A-130 [6]. It builds upon concepts
- 289 introduced in NISTIR 8286 and complements other documents in this series. It references some
- 290 materials that are specifically intended for use by federal agencies and will be highlighted as
- such, but the concepts and approaches are intended to be useful for all enterprises.

292 **1.3 Document Structure**

This publication helps establish an enterprise risk strategy (Section 2.1) to identify risks to mission objectives (Section 2.2)), and to analyze (Section 2.3) their likelihood and possible impact while considering the enterprise's risk strategy as expressed through risk appetite and risk tolerance. The remainder of this document is organized into the following major sections: ⁴

- Section 2 details CSRM considerations, including enterprise risk strategy for risk identification and risk analysis.
- Section 3 provides a short summary and conclusion.
- The References section provides links to external sites or publications that provide
 additional information.
- Appendix A contains acronyms used in the document.
- Appendix B describes how the National Vulnerability Database (NVD) and National
 Checklist Program (NCP) support risk identification activities.

⁴ 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. [2] See <u>https://www.nist.gov/cyberframework/informative-references</u> for an overview of OLIR.

2 Cybersecurity Risk Considerations Throughout the ERM Process

- 306 Because digital information and technology are valuable enablers for enterprise success and
- 307 growth, they must be sufficiently protected from various types of risk. Government entities for
- 308 whom growth may not be a strategic objective are still likely to find value in dynamically adding
- 309 or changing their services or offerings as their constituents' needs evolve. Thus, both private and
- 310 public sector endeavors need to evaluate the role of information and technology in achieving
- enterprise objectives. This understanding enables a deeper consideration of the various
- 312 uncertainties that jeopardize those objectives.
- 313 In the context of ERM, senior leaders must clearly express expectations regarding how risk
- 314 should be managed. Those expectations provide CSRM practitioners with objectives for
- 315 managing cybersecurity risks, including methods for reporting the extent to which risk
- 316 management activities successfully achieve those objectives. The document for recording and
- 317 sharing information about those risks is the cybersecurity risk register (CSRR).
- 318 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
- 320 that, while a risk register represents various risks at a single point in time, it is important for the
- 321 enterprise to ensure that the model is used in a consistent and iterative way. As risks are
- 322 identified (including calculation of likelihood and impact), the risk register will be populated
- 323 with relevant information once decisions have been made. As risks are reviewed, the agreed-
- 324 upon risk response becomes the current state, and the cycle begins anew.
- 325 Figure 2 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
- 327 subsequent publication. Note that, while prioritization is informed by some of the information
- 328 recorded in these columns, risk priority will be discussed in that future publication as part of
- 329 Risk Evaluation and Risk Response activities. While the example illustrates a template for
- 330 cybersecurity risks, a similar template could be used for any type of risk in the enterprise.



333 **2.1** Risk Scope, Context, and Criteria

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

342

- ISO 31000:2018 points out that there are three prerequisites for supporting a CSRM program asan input to ERM [3]:
- The *scope* of the CSRM activities should be defined;
 - The internal and external *context* of the CSRM activities should be determined; and
- The criteria from enterprise stakeholders should be declared and documented through a comprehensive CSRM *strategy*.
- 345 Senior leaders define the ERM scope, context, and strategy, which inform enterprise priorities,
- 346 resource utilization criteria, and responsibilities for various enterprise roles. The ERM strategy
- 347 helps define how various organizational systems, processes, and activities cooperate to achieve
- 348 risk management goals, including those for CSRM, in alignment with mission objectives.
- 349 **2.1.1 Risk Appetite and Risk Tolerance**
- 350 CSRM, as an important component of ERM, helps assure that cybersecurity risks do not hinder
- 351 established enterprise mission and objectives. CSRM also helps ensure that exposure from
- 352 cybersecurity risk remains within the limits assigned by enterprise leadership. Figure 3 illustrates
- 353 the ongoing communications among ERM and CSRM stakeholders to set, achieve, and report on
- risk expectations throughout the enterprise. This illustration builds upon the well-known levels
- 355 of the Organization-Wide Risk Management Approach described in NIST Special Publication
- 356 (SP) 800-37, Revision 2 [4]. The diagram extends the Notional Information and Decision Flows
- 357 figure from the NIST Framework for Improving Critical Infrastructure Cybersecurity
- 358 (Cybersecurity Framework) by indicating risk appetite and risk tolerance definition,
- 359 interpretation, and achievement [5].
- 360 The process described in Figure 3 illustrates that *risk appetite* is declared at the enterprise level.
- 361 Risk appetite provides a guidepost to the types and amount of risk, on a broad level, that senior
- 362 leaders are willing to accept in pursuit of mission objectives and enterprise value.⁵ As leaders
- 363 establish an organizational structure, business processes, and systems to accomplish enterprise
- 364 mission objectives, the results define the structure and expectations for CSRM at all levels.⁶
- 365 Based on these expectations, cybersecurity risks are identified, managed, and reported through

⁵ 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." [6]

⁶ 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.

- risk registers and relevant metrics. The register then directly supports the refinement of risk
- 367 strategy considering mission objectives.

368 Risk appetite can be interpreted by enterprise- and organization-level leaders to develop specific

risk tolerance, which is defined by OMB as "the acceptable level of variance in performance

- relative to the achievement of objectives" [6]. Risk tolerance represents the specific level of
- 371 performance risk deemed acceptable within the risk appetite set by senior leadership (while
- recognizing that such tolerance can be influenced by legal or regulatory requirements).⁷ Risk
- tolerance can be defined at the Executive Level (e.g., at the Department level for U.S. federal
- agencies), but OMB offers a bit of discretion to an organization, stating that risk tolerance is
- 375 "generally established at the program, objective, or component level."⁸

376 Risk appetite and risk tolerance are related but distinct, in a similar manner to the relationship

- between governance and management activities. Where risk appetite statements define the
- 378 overarching risk guidance, risk tolerance statements define the specific application of that
- direction. Together, these risk appetite and risk tolerance statements represent risk limits, help
- 380 communicate risk expectations, improve the focus of risk management efforts, and reduce the
- 381 likelihood of unacceptable loss. Achievement of those expectations is conveyed through risk
- registers that document and communicate risk decisions. Risk assessment results and risk
 response actions at the System Level are reflected in CSRRs. As CSRRs from multiple systems
- are collated and provided to higher level business managers at the Organization level, those
- 385 managers can evaluate results and refine risk tolerance criteria to optimize value delivery.
- resource utilization, and risk. The aggregation of all enterprise CSRRs at the Enterprise Level
- 387 enables senior leaders to monitor risk response considering the expectations set. Figure 2
- 388 illustrates the tight coupling of ERM, where senior leaders set enterprise risk strategy and make
- 389 risk-informed decisions, and CSRM, where cybersecurity practitioners can best identify where
- 390 cybersecurity risk is likely to occur.

OMB Circular A-123 states that "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." [6]

⁸ Examples of the Organization Level include Business Units, Company Departments, or Agency Divisions.





Figure 3: Illustration of Enterprise Risk Communication and CSRM Coordination⁹

Notably, Figure 3 and Figure 4 illustrate general integration and coordination activities but are fairly simplistic representations. For example, risk appetite statements should originate from the most senior leaders, but those leaders may choose to delegate the creation of cybersecurity risk appetite statements to a senior cybersecurity risk official (e.g., CISO or Risk Executive Function). Each enterprise is unique, and the intent of this document is to foster the integration of CSRM as part of ERM. Readers should also note that the processes described are cyclical. Early iterations may include the definition of terms, strategies, and objectives. Subsequent iterations

- 400 may focus on refining those objectives based on previous results, observations of the risk
- 401 landscape, and changes within the enterprise.
- 402 Table 1 describes the process by which senior leaders express their strategy and expectations for
- 403 managing cybersecurity risk throughout the enterprise. In general, NISTIR 8286A addresses
- 404 activity points 1 through 3, and activity points 4 through 6 will be addressed in NISTIR 8286B.

⁹ Figure 3 on page 8 further decomposes the risk management cycle, information flow, and decision points illustrated in Figure 2, which provides a high-level understanding in the context of the organization structure. Subsequent publications in this series will provide additional information about the activities described in Figure 2 and Table 1.

Table 1: 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 system 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 germane 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 Business 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, ERR, and Enterprise Risk Profile	Normalized and harmonized CSRRs from various Organization Level CSRM reports; Internal compliance and auditing reports; Results from other (non-cybersecurity) risk management activities; Observations regarding ERM and CSRM achievement	Aggregated and normalized Enterprise CSRR; integrated Enterprise Risk Register 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 for monitoring and reporting overall risk management activities and results

- 406 Table 2 provides examples of actionable, measurable risk tolerance that illustrate the application
- 407 of risk appetite to specific context within the organization level structure:
- 408

Table 2: 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 High Value Assets (per OMB definition) must be patched against critical software vulnerabilities (severity score of 10) within fourteen 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 level.
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 <u>no</u> appetite for 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.

409 Figure 4 illustrates a more detailed information flow of inputs and outputs, as described in Figure

410 2 and Table 1. Senior leaders and business managers define risk tolerance direction that is

411 applied at the System Level. System Level practitioners interpret those risk tolerance statements

and apply CSRM activities to achieve risk management objectives. The results are then reviewed

413 to confirm effectiveness, highlight opportunities for improvement, and identify important trends

that might require Organization or Enterprise Level action. The specific process activities will be

415 based on the risk management methods applied but will generally include those below.



Figure 4: Continuous Interaction between ERM and CSRM using the Risk Register¹⁰

- 418 The activities in Figure 4 are listed below.¹¹
- As described in earlier portions of this section, leaders at Levels 1 and 2 define specific and measurable risk appetite and risk tolerance statements that reinforce enterprise mission objectives and organization goals. Those leaders may also choose to define aggregate metrics (e.g., key risk indicators [KRIs], key performance indicators [KPIs]) to help track and report achievement of risk direction.
- At Level 3, practitioners interpret the risk tolerance statements for the specific systems
 that operate to provide business (or agency) benefits. Those in various roles (e.g., system
 owners, security officers) work together to derive system-level requirements for
 confidentiality, integrity, and availability.
- The value of each asset of a given system (e.g., information type, technical component, personnel, service provider) is appraised to determine how critical or sensitive it is to the operation of the system (see Section 2.2.1). Subsequent risk decisions depend on accurate understanding of the importance of each resource to the system.

¹⁰ 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.

¹¹ For those topics that are addressed in NISTIR 8286A, a pointer to the relevant section is included. Topics without a pointer to sections on this document will be addressed in subsequent publications in this series.

- For each of these components, the practitioner identifies threat sources that might cause a harmful effect (see Section 2.2.2) and the vulnerabilities or conditions that might enable such an effect (see Section 2.2.3). To complete development of the risk scenario, the practitioner determines the adverse effect of the threat source exploiting the vulnerable conditions. The scenario is recorded in the CSRR as the "Risk Description" (see Section 2.2.5). The category for the scenario will be recorded in the "Risk Category" column, based on enterprise criteria, to support risk correlation, aggregation, and reporting.
- The practitioner performs risk analysis (see Section 2.3) to determine the likelihood that the threat events and vulnerable conditions would result in harmful impacts to the system asset. Similarly, the practitioner analyzes the impact value and calculates the risk exposure using the methodology defined in the enterprise risk strategy (e.g., as the product of [risk likelihood] x [risk impact].) The results of these analyses are recorded in the CSRR's "Current Assessment" column as "Likelihood," "Impact," and "Exposure."
- 445 The determined exposure is compared with the risk tolerance. If exposure is within risk 446 tolerance limits, the risk may be "accepted." If exposure exceeds tolerable levels of risk, 447 practitioners can consider whether they can achieve risk tolerance through other forms of 448 risk response. In many cases, security controls may be applied to **mitigate** risk by 449 reducing the likelihood or impact of a risk to a tolerable level. Risk response may also 450 include risk transfer, also known as risk sharing. For example, an organization might 451 hire an external organization to process sensitive transactions (e.g., payment card 452 transactions), thus reducing the likelihood that such sensitive data would be processed by 453 an in-house system. Another common risk transfer method is through cybersecurity 454 insurance policies that can help reduce the economic impact if a risk event occurs.
- 455 In some cases, it might be determined that the exposure exceeds risk tolerance and cannot 456 be brought within limits through any combination of mitigation or risk transfer. In this 457 case, practitioners (e.g., the system owner) may need to work with Level 2 leaders to revisit the risk tolerance itself. This negotiation presents an opportunity for the Level 2 458 459 and Level 3 managers to determine the best course of action, in light of mission 460 objectives, to refine the risk direction (e.g., through an exception process, an adjustment to the risk tolerance statement, or increased security requirements for the relevant 461 462 system). In any case, stakeholders will have applied a proactive approach to balancing risk and value to the benefit of the enterprise. 463
- If an unacceptable cybersecurity risk cannot be adequately treated in a cost-effective
 manner, that risk must be **avoided**. Such a condition may require significant redesign of
 the system or service. These circumstances should be rare, and they highlight the value of
 CSRM coordination early in the system engineering process. Notably, risk avoidance is
 not the same as ignoring a risk.

- Results of risk activities and decisions are recorded in the CSRR and, if applicable, in a 469 documented Plan of Actions & Milestones (POA&M)¹² that records future risk activities 470 471 agreed upon.
- 472 The process continues until all system assets have been evaluated for risk from currently 473 understood threats and vulnerabilities. For some enterprises, the composite set of system 474 risks (as recorded in the CSRR), risk response applied, agreements regarding additional 475 CSRM actions to be taken (e.g., as recorded in the POA&M), and other relevant artifacts 476 will be reviewed by a senior official to confirm that risk decisions and risk response align 477 with risk tolerance and risk appetite directives. For federal government agencies, this 478 represents the system authorization process.
- 479 Subsequently, CSRRs from throughout the Business Level are normalized and 480 aggregated to provide a composite view of the risk posture and decisions for that 481 Organization. As Level 2 managers consider feedback from system CSRM activities, 482 those managers may decide to refine risk tolerance levels. It may be that the aggregate 483 risk across multiple systems represents too great an exposure and needs to be reduced. In 484 other cases, based on successful risk management results, stakeholders may be able to 485 permit a little more risk in some areas if such a decision would support mission 486 objectives and potentially save resources or allow them to be directed to areas that require 487 additional resources in order to meet expected risk tolerances.
- 488 Similar reviews and refinement occur at Level 1 to support enterprise governance and 489 risk management decisions. Some types of enterprises may be required to formally 490 disclose risk factors (e.g., through annual reports), and this aggregate understanding of 491 cybersecurity risks and risk decisions supports that fiduciary responsibility. These 492 activities may also help others, such as Federal Government agencies, to help comply 493 with mandatory requirements such as those established by OMB.

494 Interpreting risk tolerance at Level 3, practitioners develop requirements and apply security 495 controls to achieve an acceptable level of risk. This process helps to ensure that CSRM occurs in 496 a cost-effective way. As an example, consider the global retail firm described in the first row of 497 Table 2. The system owner of the customer website will select controls that will ensure 498 adherence to availability service levels. In deciding which controls to apply, the system owner 499 collaborates with a security team to consider methods to meet service level objectives. The team 500 can contact the local power utility supplier to determine electrical availability history and gather 501 other information regarding the likelihood of the risk of a loss of power to the important website. 502 This additional information might help the system owner decide whether to invest in a backup

503 generator to ensure sufficient power availability.

Federal agencies are required 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 the outstanding risk 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.

- 504Results from previous assessments can be useful for estimating the likelihood of achieving risk
- 505 goals in the future (this topic is described in Section 2.3.2.1.) The team would then move to the
- 506 next risk scenario (e.g., perhaps an internet service outage) and review the history and reliability
- 507 of the organization's telecommunications provider to ascertain the likelihood and impact of a
- 508 loss of service. Iterating through each potential risk, as described in Figure 4, practitioners can
- 509 develop a risk-based approach to fulfilling CSRM objectives in light of risk appetite and risk
- 510 tolerance. This, in turn, helps CSRM practitioners demonstrate how their actions directly support
- 511 mission objectives and enterprise success.

512 **2.1.2 Enterprise Strategy for Cybersecurity Risk Reporting**

- 513 The enterprise strategy for cybersecurity risk management and monitoring includes common
- 514 definitions for how and when assessment, response, and monitoring should take place. Notably,
- 515 ERM monitoring is for communication and coordination regarding overall risk and should not be
- 516 confused with system-level monitoring (or continuous monitoring.)
- 517 Guidance from senior leaders provides risk guidance—including advice regarding mission
- 518 priority, risk appetite and tolerance, and capital and operating expenses to manage known risks—

519 to the organizations within their purview. There are some details that need to be defined at the

520 Enterprise Level so that information can be combined and compared effectively, including the

521 ability to communicate about risks through the various types of risk registers.

522 While many of these details will be delegated to Organizational Level processes, several key 523 factors should be defined at the Enterprise Level, including:

- 524 • Criteria regarding risk category selection that enables risk register entries to be 525 consolidated and compared; 526 • Direction regarding the classification and valuation of enterprise assets, including 527 approved methods for business impact analysis; 528 • Assessment methodologies, including direction regarding analysis techniques and the 529 appropriate scales to be applied; 530 • Frequency of assessment, reporting, and potential escalation; Methods for tracking, managing, and reporting (i.e., use of the cybersecurity risk 531 • 532 register); and,
- Resources available for risk treatment, including common baselines, common controls,
 and supply chain considerations.
- 535 As cybersecurity risks are recorded, tracked, and reassessed throughout the risk life cycle and
- 536 aggregated within the enterprise cybersecurity risk register, this guidance ensures that risk will
- 537 be consistently communicated, managed, and potentially escalated. Strategic guidance from
- 538 enterprise stakeholders should also include:

- Definition of the organizational boundaries to which CSRM activities will apply; 539
- 540 documentation that the scope for cybersecurity objectives supports alignment among enterprise, business and mission objectives, and operational achievement. 541
- Direction regarding specific roles for managing, communicating, and integrating risks 542 • throughout the enterprise; defining the types of stakeholders (by role) will support risk 543 544 communication and timely decision-making.
- 545 • Determination of key risk indicators (KRIs) and key performance indicators (KPIs) that 546 will support the management and monitoring of the extent to which risk response remains 547 within acceptable levels.
- 548 Through the processes described above, senior leaders express risk limits and expectations as
- 549 risk appetite statements. That risk appetite is then interpreted through risk tolerance and then
- applied at the System Level. The subsections below describe how feedback is provided using the 550
- 551 risk register to identify and document risk, analysis, and results.

552 **Risk Identification** 2.2

- 553 This section describes methods for identifying and documenting sources and their potential
- 554 consequences (recorded in the Risk Description column of the CSRR, as shown by the red border 555 in Figure 5.)

	Notional Cybersecurity Risk Register										
	Priority	Risk Description	Risk	Curr	ent Assessi	ment	Risk	Risk Response	Risk Response	Risk	
ID Pri	Phoney Risk Description	Category	Likelihood	Impact	Exposure Rating	Response Type	Cost	Description	Owner	Status	
1		Parts A, B, C, and D (described below)									
2											
3											
4											
5											
Continually Communicate, Learn, and Update											

557

Figure 5: CSRR highlighting Risk Description Column¹³

558 Risk identification represents a critical activity for determining the uncertainty that can impact

559 mission objectives. The primary focus of NISTIR 8286A is on negative risks (i.e., threats and

560 vulnerabilities that lead to harmful consequences), but it is important to remember that positive

561 risks represent a significant opportunity and should be documented and reviewed as well.

562 Consideration and details regarding positive risks will be addressed in subsequent publications.

563 Through the activities in the following sections, risk practitioners determine and record those

¹³ The CSRR template is available in the Open Risk Register Format (ORRF) format; an automated JavaScript Object Notation (JSON) notation 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.

- 564 events that could enhance or impede objectives, including the risk of failing to pursue
- 565 opportunities.



Figure 6: Inputs to Risk Scenario Identification¹⁴

- 568 As shown in Figure 6, which is derived from the Generic Risk Model in NIST SP 800-30,
- 569 Revision 1, Guide for Conducting Risk Assessments, cybersecurity risk identification is
- 570 composed of four necessary inputs—parts A through D—in the Risk Description cell of the
- 571 cybersecurity risk register [7]. Combining these elements into a risk scenario helps to provide the
- 572 full context of a potential loss event. The use of this scenario-based approach helps ensure
- 573 comprehensive risk identification by considering many types of physical and logical events that
- 574 might occur. Notably, the scope of cybersecurity has expanded from its original boundaries of
- 575 adversarial digital attacks and encompasses all types of uncertainty that can impact any form of
- information and technology. Accordingly, the risks to be identified and registered are muchbroader as well.
- 578 The completion of the Risk Description column is composed of four activities that are detailed in 579 Subsections 2.2.1 through 2.2.4. The activities include:
- Part A Identification of the organization's relevant assets and their valuation
- Part B Determination of potential threats that might jeopardize the confidentiality,
 integrity, and availability of those assets
- Part C Consideration of vulnerabilities or other predisposing conditions of assets that
 make a threat event possible
- Part D High-level evaluation of the potential consequences if the threat source (part B)
 exploited the weakness (part C) against the organizational asset (part A)
- The integration of those elements enables the practitioner to record each scenario in the CSRR as
 a description of cybersecurity risk. The quantity and level of detail of the risks identified should
 be in accordance with the risk strategy.
- 590 Enterprises that are just beginning to integrate the cybersecurity risk register results into broader
- 591 ERM activities will benefit from focusing on an initial and limited number of top risks. Those
- 592 creating a risk management program for the first time should not wait until the risk register is
- 593 completed before addressing extraordinary issues. However, over time, the risk register should
- 594 become the ordinary means of communicating risk information.

¹⁴ Positive risks apply a similar process through which an enterprise asset considers an opportunity that takes advantage of a new or pre-existing condition that results in a positive impact (benefit) to the enterprise.

595 2.2.1 Inventory and Valuation of Assets

The first prerequisite for risk identification is the determination of enterprise assets that could be 596

597 affected by risk (part A in Figure 6). Assets are not limited to technology; they include any 598 resource that helps to achieve mission objectives (e.g., people, facilities, critical data, intellectual

599 property, and services).¹⁵

600 Enterprises may benefit from applying a comprehensive method to inventory and monitor

enterprise assets, such as the use of a *configuration management database (CMDB)* or an 601

602 information technology asset management (ITAM) system. These management tools help to

603 record and track the extent to which various assets contribute to the enterprise's mission. They

604 can also help track enterprise resources throughout their own life cycle. For example, as the use

605 of mobile devices (including personal devices) expands, there are commercial products that can 606

help maintain inventory to support ongoing risk identification, analysis, and monitoring.

607 2.2.1.1 Business Impact Analysis

608 Risk managers can benefit by using a business impact analysis (BIA) process to consistently

609 evaluate, record, and monitor the criticality and sensitivity of enterprise assets. A BIA can help

610 document many aspects of the value of an asset that may extend well beyond replacement costs.

611 For example, while one can calculate the direct cost of research and development underlying a

612 new product offering, the long-term losses of the potential theft of that intellectual property

613 could have more far-reaching impacts, including future revenue, share prices, enterprise

614 reputation, and competitive advantage. That is among the reasons why it is beneficial to gain the

guidance of senior leadership regarding the determination of assets that are critical or sensitive. 615

The relative importance of each enterprise asset will be a necessary input for considering the 616

617 impact portion of the Risk Description (part D) in the cybersecurity risk register. Considerations 618 include:

- 619 Would loss or theft of the resource compromise customer or enterprise private 620 information?
- 621 • Would disclosure of an asset's information trigger legal or regulatory fines or actions?
- Would a lack of availability of the asset interrupt the enterprise's ability to fulfill its 622 623 mission or result in costly downtime?
- Would the lack of confidentiality, integrity, or availability of the asset undermine public 624 625 or consumer confidence or trust in the enterprise?
- 626 Do internal or external critical resources depend on this asset to operate? •
- As the organization reviews the results of previous system-level categorization decisions and 627
- 628 monitors risk assessment findings, practitioners can use that information to review system 629 prioritization as an input into business impact analysis.

¹⁵ NIST SP 800-37 Revision 2 points out that risk could impact "organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals."

630 **2.2.1.2 Determination of High-Value Assets**

631 An example of asset valuation is the U.S. Government's designation of "high-value assets," or

HVAs. HVAs, described in OMB Memorandum M-19-03, represent agency resources that have

been determined as highly sensitive or critical to achieving the business mission [8]. OMB
 M-19-03 represents an example of an enterprise approach to valuation since the memorandum

635 defines the specific categories for consistent designation (i.e., information value, role in Mission

- 636 Essential Function support, and role in support for Federal Civilian Essential Functions) yet
- 637 leaves permits each agency to determine which assets meet those criteria. Other common
- 638 industry examples include the use of specific classifications to reflect the sensitivity and
- 639 criticality of technology and information, including "Company Confidential" or "Business
- 640 Sensitive."

641 **2.2.1.3** Automation Support for Inventory Accuracy

642 Accurate and complete asset inventory is an important element of CSRM, and the measurement

of that accuracy is often a key performance measurement for CSRM reporting. To illustrate that

644 importance, federal agencies, as part of their annual reporting metrics, must report how

645 completely their hardware and software asset management inventories reflect what is actually

- 646 installed on agency networks.
- 647 Automated tools can aid in discovering and monitoring various technical components used by
- 648 the enterprise. For example, a use case described by the NIST Security Content Automation
- 649 Protocol (SCAP) specification is *inventory scanning* (see Appendix B for more information).
- 650 Products that have been successfully reviewed as part of the SCAP Validation Program help
- 651 maintain a comprehensive and accurate inventory of digital assets [9]. Valuation information
- recorded in that inventory, in turn, can help maintain a comprehensive view of the enterprise
- assets for which cybersecurity risks should be identified, analyzed, treated, and monitored. The
- use of automation helps to ensure that enterprise asset inventory is current, accurate, and
- 655 complete.

656 **2.2.2 Determination of Potential Threats**

- 657 The enumeration of potential threat sources and the threat events that those sources could initiate
- 658 is the second prerequisite for the identification of potential risk scenarios. Figure 7 represents
- 659 part B of the Risk Description cell of the CSRR. Because information and technology exist in
- 660 many forms, a broad approach to modeling threats supports comprehensive risk identification.





661

Figure 7: Threats as an Input to Risk Scenario Identification (Part B)

663 **2.2.2.1 Threat Enumeration**

664 Many public- and private-sector processes are available to help enumerate threats. One example 665 is the OCTAVE Allegro method from Carnegie Mellon University's Software Engineering 666 Institute [10]. That model includes "identification of Areas of Concern," a process for 667 determining the "possible conditions or situations that can threaten an organization's information 668 asset(s)." The OCTAVE Allegro approach describes a process where risk managers create a tree 669 diagram of various threats haved and

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

676 Enumeration of threats can be performed as a "top-down" analysis that considers important

677 assets that might be threatened or as a "bottom-up" analysis that considers what an unknown

678 threat might attempt to accomplish. Table 3 provides an example excerpt of a threat analysis.

679

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 & development division	
Insider	Intentional	Disclosure	Physical files from Personnel Dept., physical design drawings from manufacturing	
External	Accidental	Disclosure	Remote access account info 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	

680 Threat enumeration should consider potential motivation or intent. Accidental and intentional

threat activity can each have significant impacts, but the evaluation, treatment, and monitoring of

each type of activity will vary based on that motivation. Motivation will also have some bearing

on the likelihood calculation (as described in subsequent sections).

684 Note that the list above includes physical security considerations. Numerous physical issues

685 (e.g., theft, mechanical failures) can affect digital and logical devices, so both logical and

686 physical threat sources should be considered.

687 Practitioners consider various factors for each of these threat sources based on the understanding

- 688 of valuable enterprise assets, as determined in Section 2.2.1. Example considerations include:
- What might a human actor accidentally disclose, modify, or destroy?
 What information or technology might a person (e.g., a disgruntled employee)
- *intentionally* disclose, interrupt, or delete?
- 692 Are there threat conditions that might be introduced by supply chain partners, such as outside service providers?
- What similar considerations might apply to accidents or intentional actions from an outside source using technical means?
- What technical flaws or malicious code might affect valuable systems, leading to adverse
 impacts on enterprise objectives?
- What natural disasters or utility outages might have harmful effects?

699 Risk managers should develop a reasonable list of potential threats based on practical and

700 imaginative scenarios, particularly in light of the assets identified in earlier processes. The extent

- of this list depends on the direction of senior leaders. While some stakeholders may prefer fewer
- risks in the register, it is important to remember that any risks that are not identified at this stage
- will not be part of the subsequent risk analysis and may introduce an unforeseen vulnerability.

704 **2.2.2.2** Reducing Unwanted Bias in Threat Considerations

705 While cybersecurity threat discussions often focus on the intentional and adversarial digital

attack, it is important that all risk practitioners consider a broad array of threat sources and

vents. In addition, while highly unlikely scenarios might not need to be listed (e.g., a meteorite

rashing into the data center), risk managers should avoid dismissing threats prematurely. For

- these reasons, practitioners will benefit from identifying and overcoming potential bias factors in
- enumerating potential threat sources and the events they might cause. Table 4 describes some of
- 711 these bias issues as well as methods for addressing those issues.
- 712

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 irrational consideration of recent hype that can result in inappropriate risk response.	Assuming that <i>any</i> digital challenge can be addressed and solved through application of "machine learning" and "artificial intelligence."	Staying informed about the details of current threat patterns. Combined with input from subject matter experts, this 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.

713 2.2.2.3 Threat Enumeration Through SWOT Analysis

714 While it is critical that enterprises address potential negative impacts on mission and business

objectives, it is equally important (and required for federal agencies) that enterprises also plan

for success. OMB states in Circular A-123 that "the profile must identify sources of uncertainty,

517 both positive (opportunities) and negative (threats)" [6].

718 One method for identifying both potential positive and negative risks is through the use of a

719 SWOT (strength, weakness, opportunity, threat) analysis. Because effective risk management is

achieved by balancing potential benefits against negative consequences, a SWOT analysis

provides a visual method for considering these factors. Table 5 provides an example of an

722 overarching SWOT analysis. A similar exercise could be performed at any level of the

- 723 enterprise, including for an information system or cyber-physical system.
- 724

Table 5: Example SWOT Analysis

Strengths	Weaknesses	
Effective communication among a small office with co-located staff	Few dedicated IT and Information Security employees Many endpoints are laptops that could be lost or stolen Office laptops do not employ full-disk encryption	
Online email and financial applications mean no local servers to support and protect		
Modernized office desktop equipment with current operating systems and connectivity		
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 & conditions of the new contract increase the criticality of cybersecurity improvement	
Funds have been allocated to improve cybersecurity improvement	Additional service offerings (e.g., development and remote administration) increase cybersecurity risks	
Third-party partners may be able to help us quickly ramp up new service offerings	Supply chain partners may bring additional security risks to be considered and managed	

725 **2.2.2.4** Use of Gap Analysis to Identify Threats

- As part of the threat modeling exercise, practitioners can benefit from evaluating a comparison
- of current conditions to more desirable conditions, then analyzing any gaps between those to
- identify potential improvements. This process can be iterative in that the organization may not
- know the current state until after several rounds of risk management activities. Similarly,
- 730 practitioners may not fully know the desired state until after several iterations of identifying,
- assessing, analyzing, and responding to risks. Despite this challenge, gap analysis can be a useful
- tool to include as part of a broad methodology.
- 733 NISTIR 8286 provides an example of the process described by the NIST Cybersecurity
- Framework [5]. This framework describes a set of activities that consider the five functions:
- 1. **Identify** what assets are important for achieving enterprise objectives.
- 736 2. **Protect** those assets from known threats and vulnerabilities.
- 737 3. **Detect** risk events on those assets in an efficient and effective manner.
- 738 4. **Respond** to such risk events rapidly and effectively.
- 5. **Recover** from any disruptions in accordance with enterprise strategy.
- 740 The framework decomposes the functions into categories, each of which is further described in
- strategic and tactical outcomes (subcategories.) For each subcategory, the framework
- recommends the creation of profile artifacts that document the *current* and *desired* (or target)
- policies, processes, and practices in each subcategory. By documenting the "as-is" outcomes,
- organizations can consider potential risk implications, including potential threat events. That
- information will later help to develop target state profiles. Table 6 provides an example excerpt
- 746 from a current profile with example threat considerations.
- 747

Table 6: Cybersecurity Framework Profiles Help Consider Threats

ID	Category	Current State	Threat Consideration
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 is 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, responding to incidents.)
ID.BE	Business Environment	 Priorities and responsibilities based on the Commercial Facilities Sector. Dependencies and resilience requirements 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 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 the 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 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 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.)

748 Another source of ideas for threat modeling is NIST SP 800-53, Security and Privacy Controls

749 *for Information Systems and Organizations*, which provides a catalog of security and privacy

controls.¹⁶ A companion document, SP 800-53A, Assessing Security and Privacy Controls in

751 *Federal Information Systems and Organizations: Building Effective Assessment Plans,*

documents methods for assessing the effectiveness and suitability of those controls for various

purposes [12]. Through the examination of controls and assessment methods, practitioners can

observe conditions that align with enterprise situations, sparking discussions about potential

755 threats. For example:

- 756 A practitioner can consider control AC-17, Remote Access, which states, "The use of
- 757 encrypted VPNs provides sufficient assurance to the organization that it can effectively
- treat such connections as internal networks if the cryptographic mechanisms used are
- implemented in accordance with applicable laws, executive orders, directives,
- regulations, policies, standards, and guidelines." The practitioner should then consider the

¹⁶ 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: <u>https://www.nist.gov/cyberframework/informative-references/validation-tool-templates.</u>

- threat conditions that would make encryption necessary (e.g., preventing eavesdropping,
 ensuring authorization) and perhaps identify regulatory compliance requirements.
- Considering controls and their assessments can inspire the imagination and support effectivethreat modeling.

765 As noted in NISTIR 8286, "organizations should not wait until the risk register is completed 766 before addressing obvious issues," such as those issues that arise from the threat modeling exercises. CSRM practitioners, in collaboration with ERM stakeholders, will need to continually 767 768 define and refine the timing of various risk identification processes. An organization that delays 769 risk management until the end of a detailed and exhaustive risk identification activity may find 770 that many risks become realized while the practitioners are still working. At the other extreme, 771 immediately beginning risk management when only a few risks have been catalogued can 772 hamper prioritization or cause a continual recalculation of risk importance as new loss event 773 types are identified and added. Threat identification methods may also discover quick wins (e.g., 774 changing default passwords for devices and applications, enabling cryptography settings, locking 775 file cabinets) that can be efficiently resolved, immediately addressed, and documented in the risk

register while other risk identification activities continue.

777 2.2.2.5 Technical Threat Enumeration

778 While threat sources include many factors, because cybersecurity risks are so closely associated

with information and technology, technical threats are likely to comprise the majority of those

780 enumerated. The complexity and rapid evolution of technical threats make it particularly

781 worthwhile to gain insights from reputable partners regarding how to prepare for, recognize, and

respond to these threat sources.

For the enterprise to be successful in protecting information and technology, and for it to rapidly

detect, respond, and recover from threat events quickly, the organization may choose to apply an

785 intelligence-driven approach, commonly referenced as Cyber Threat Intelligence (CTI). Using

sources of information and data such as those described in Table 7, practitioners will gain

- 787 insights into adversaries' tactics, techniques, and procedures (TTPs) as well as other information
- about how to prepare and for what conditions to monitor.
- 789 Industry-based threat intelligence sharing organizations are available for the exchange of CTI
- among members or subscribers. For example, DoD's Information Sharing Environment (DISCE)
- is a government sharing program that facilitates CTI sharing between its Defense Industrial Base
- 792 (DIB) members and participants. Another example is that of information sharing analysis centers
- 793 (ISACs) and organizations (ISAOs). Using intelligence provided by such sources, risk
- 794 practitioners can make threat-informed decisions regarding defensive capabilities, threat
- detection techniques, and mitigation strategies. By correlating and analyzing cyber threat

- information from multiple sources, an organization can also enrich existing information and
- 797 make it more actionable.¹⁷
- 798

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.
	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, Financial Sector Information Sharing and Analysis Center [FS-ISAC]) provide automated data feeds with information about existing or imminent threats, and vulnerabilities being exploited by those threats.
	Example: DHS Cybersecurity and Infrastructure Security Agency (CISA) <u>https://us-cert.cisa.gov/ais</u> , <u>https://www.cisa.gov/ciscp</u>
Information Sharing and Analysis Centers and Organizations (ISACs and ISAOs)	Many industry types, 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 assessment and maintain risk awareness. Some ISACs offer in-house applications for sharing of indicators of compromise (IoC) and other threat-based alerts.
	Example: National Council of ISACs (<u>https://www.nationalisacs.org/</u>)
Technical Threat Category Models	Many industry models are available for performing technical threat modeling, particularly in 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 impact.
MITRE ATT&CK®	Knowledge base of adversary tactics and techniques based on real-world observations. Used as a foundation for development of specific threat models and methods, helping enterprise risk practitioners to consider the threat conditions that an adversary might apply and the events that adversary might seek to cause. Recent addition of pre-attack indicators and methods can help prepare for and detect signs of an impending event. https://attack.mitre.org/
NSA/CSS Technical Cyber Threat Framework (NTCTF) v2	While this model does not help identify sources, it provides a broad listing of the types of events a threat source might attempt to initiate, particularly a motivated human adversary. By defining 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

- 799 By understanding typical attack patterns, enterprises can mount defenses to improve resilience.
- 800 For example, understanding the methods of various attackers in privilege escalation or lateral
- 801 movement will help risk managers plan effective preventive and detective controls. Because
- 802 technical attacks can move rapidly, preparation is paramount. Updated, rapid sharing of indictors

¹⁷ Cybersecurity information sharing is discussed in detail in NIST SP 800-150, *Guide to Cyber Threat Information Sharing*, <u>https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-150.pdf</u>

- 803 of compromise (such as those provided through Structured Threat Information Expression
- 804 [STIX]) helps enterprise practitioners better detect and respond to emerging threats.¹⁸

805 Because of the time-critical nature of cybersecurity risks, introducing automation into the threat 806 intelligence analysis enables an enterprise to reduce the potential delays and errors that a human-807 only approach can introduce. While automated information sharing will not entirely eliminate 808 threats, it can help an organization stay aware of and prepared for new or evolving types of 809 attacks. One example of an AIS is that offered by the U.S. Department of Homeland Security 810 (DHS) in accordance with the U.S. Cybersecurity Information Sharing Act of 2015. The DHS

- 811 AIS site includes the following information:
- 812 The free (DHS) AIS capability enables the exchange of cyber threat indicators between 813 the Federal government and the private sector at machine speed. Threat indicators are 814 pieces of information like malicious IP addresses or the sender address of a phishing
- 815 email (although they can also be much more complicated).
- 816 AIS participants connect to a DHS-managed system in the Department's National 817 Cybersecurity and Communications Integration Center (NCCIC) that allows bidirectional sharing of cyber threat indicators. A server housed at each participant's 818 819 location allows them to exchange indicators with the NCCIC. Participants will not only 820 receive DHS-developed indicators but can share indicators they have observed in their 821 own network defense efforts, which DHS will then share back out to all AIS 822 participants.¹⁹
- An analysis of network packet capture data can help identify potential threats based on observed 823
- 824 traffic. Armed with understanding from CTI sources regarding TTPs and IoCs, practitioners will 825 be able to observe potential indicators and likely attack paths. In conjunction with past and
- 826 existing cyber incident information, organizations can use CTI to support internal risk
- 827 communication and risk analysis and to improve risk scenario development. In addition to the
- 828 technical advisories, the alerts and analysis reports at the DHS National Cyber Alert System
- 829 provide information about recent TTPs and how they have affected various enterprises.

830 2.2.3 Vulnerability Identification

- For any of the various threat conditions described above to result in an impactful risk, each needs 831
- 832 a vulnerable or predisposing condition that can be exploited. The identification of vulnerabilities
- 833 or conditions that a threat source would use to cause impact is an important component of risk
- 834 identification and represents part C (Figure 8) of the CSRM risk scenario.

¹⁸ STIX is one of several data exchange specifications for cybersecurity information sharing. More information is available at: https://oasis-open.github.io/cti-documentation

¹⁹ The NCCIC is part of the Cyber Information Sharing and Collaboration Program (CISCP), available at: https://www.cisa.gov/ciscp



Figure 8: Vulnerability Inputs to Risk Scenario Identification (Part C)

837 **2.2.3.1** Determination of Vulnerabilities and Predisposing Conditions

838 While it is necessary to review threats and vulnerabilities as unique elements, they are often 839 considered at the same time. Many organizations will consider a given loss scenario and evaluate 840 both, "What threat sources might initiate which threat events?" and "What vulnerabilities or predisposing conditions might those threat sources exploit to cause a loss event?"²⁰ Much of the 841 842 information provided through CTI will also inform understanding of vulnerability. For example, 843 analysis of the infamous 2017 WannaCry ransomware attack includes understanding of the threat 844 source and motive (a known and capable cybercrime group seeking financial gain), the intended 845 threat event (deliberate modification, interruption, and potential destruction of key enterprise

information assets), and the vulnerability to be exploited by the adversary (CVE-2017-0144).

847 Practitioners should (within the scope agreed upon in activities described in Section 2.1)

systematically consider the potential physical and logical vulnerabilities and predisposing
conditions that can be exploited by a threat source. This consideration can be facilitated through
many of the methods described in Table 7, including:

- Use of commercial intelligence sources that provide threat and vulnerability information.
 Many providers will take note of a customer's enterprise information and technology
 (e.g., hardware, software, and operating systems in use) to alert the organization to any
 vulnerabilities in those platforms that are known to be targeted by existing threat sources.
- Integration of AIS feeds that may include automated alerts regarding known
 vulnerabilities. Many security incident event monitoring (SIEM) products and intrusion
 detection systems (IDS) are able to help enterprises associate asset inventory information
 with AIS alerts to support incident reporting and monitoring.
- Use of a threat tree model (e.g., the diagram in the OCTAVE ALLEGRO guidance) to
 consider various human factors, technical defects, software flaws, physical entry points,
 utility dependencies, and supply chain vulnerabilities that present vulnerabilities.
- A review of the various threat categorization models (e.g., MITRE ATT&CK[®]) can inspire internal discussions, such as "What vulnerabilities might enable execution of malicious code?" or "What predisposing conditions foster lateral movement within the enterprise?"

²⁰ There are many similarities among the 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).

- 865 As with threat modeling, practitioners will also benefit from applying known risk management
- 866 frameworks as a tool for vulnerability discovery. For example, a review of the controls catalog in
- SP 800-53 may lead to consideration of control MP-3, Media Marking, which can then inspire 867
- 868 discussion regarding potential vulnerabilities that might result from unmarked (or improperly
- 869 marked) system media.
- 870 Notably, the enterprise will benefit from the advice of external specialists with expertise in
- 871 identifying and categorizing various types of vulnerabilities. Some entities, such as those
- 872 operating moderate- and high-impact federal information systems, require formal penetration
- 873 testing to identify potential vulnerabilities and the exploitability of those conditions. In addition
- 874 to some government and law enforcement agencies that are able to assist enterprises with
- 875 evaluating physical and technical vulnerabilities, many commercial organizations offer these 876 services.
- 877 2.2.3.2 System Complexity as a Vulnerability
- 878 NISTIR 8286 states that additional risks can result from the dynamic complexity of enterprise
- 879 information and technology. In fact, that complexity is itself a vulnerability to be considered and
- 880 documented. Evaluation of "what-if" scenarios regarding potential vulnerabilities, especially
- 881 those affecting critical assets, should include the determination of critical dependencies on other
- 882 resources. Because risk identification and risk analysis are iterative, risk analysis methods (such
- 883 as the Event Tree Analysis described in Section 2.3.2.2) will help determine those dependencies.
- 884 Having made that determination, those critical dependencies can be recorded in the BIA
- 885 (described in Section 2.2.1.1). Risk identification then includes scenario discussions that evaluate
- 886 complex or cascading events as vulnerabilities to be identified.
- 887 For example, the 2003 Northeast Power Grid interruption demonstrated how several moderate
- 888 risk events cascaded into a national emergency. Another example of systemic risk is that of some
- 889 financial institutions that were impacted by cascading risk in 2008. In this case, large enterprises
- 890 experienced catastrophic events because they had interdependencies with other banks, insurance
- 891 companies, and customers. When identifying and recording risks in the register, such emerging
- 892 risk conditions created by the interdependence of systems and counterparty risk must also be 893
- identified, tracked, and managed using the same methods described for more straightforward
- 894 scenarios.
- 895 As with other CSRM components, vulnerability identification can be considered through either 896 qualitative or quantitative means. An organization might determine it "has a large number of
- 897 high severity vulnerabilities" based on an internal review. A qualitative review might result from
- 898 a gap analysis between NIST Cybersecurity Framework Current State and Target State profiles
- 899 since such an analysis is intended to foster discussion and communication regarding risks but
- 900 will not likely produce a highly specific quantitative result.
- 901 More quantitative vulnerability identification results from a formal testing approach that
- 902 examines a discrete set of enterprise resources for a specified set of known vulnerabilities.
- 903 Particular vulnerability assessments (e.g., software code review or simulated phishing attack) can

- 904 provide quantitative results. Results of a formal assessment might include a specific number of
- 905 identified issues, which can be used to help complete the likelihood column of the risk register.

906 2.2.3.3 Vulnerability Identification Automation

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

921

- 912 Hardware and software products are a significant source of vulnerability for any enterprise,
- 913 whether through inherent flaws in those products or through errors in product implementation or
- 914 application. To help support the consistent identification and monitoring of these vulnerabilities,
- 915 security organizations have developed broad clearinghouses of vulnerability information. For
- 916 example, NIST operates the National Vulnerability Database (NVD) and the National Checklist
- 917 Program (NCP) to support vulnerability and security configuration management via catalogs of:
- Configuration checklists for securing key information technologies;
- Information about secure configuration settings (with associated SP 800-53 security controls);
 - Vulnerabilities (with associated severity scores);
- Standardized security checklists for automated security configuration scanning (e.g., security checklists in Security Content Automation Protocol format²¹); and
- Products that use standards to identify and report vulnerabilities.

925 Automated data feeds, such as those described above, enable enterprise monitoring tools to 926 ingest information about known vulnerabilities in near-real-time and compare those with the 927 asset inventory. A key factor in that data feed is information regarding the date that a 928 vulnerability was publicly disclosed. The severity of a given vulnerability increases 929 exponentially after it becomes publicly known, so it is important that practitioners prioritize 930 remediation of flaws. The risk of the vulnerability must be balanced with the risk of 931 implementing a fix for that issue too quickly. Automated tools can help monitor and maintain 932 that balance through specific reports regarding severe vulnerabilities that have not been patched 933 within a reasonable time. An example of this is the DHS AWARE (Agency-Wide Adaptive Risk 934 Enumeration) scoring methodology used by the DHS Continuous Diagnostics and Mitigation 935 (CDM) risk management dashboard. AWARE is not intended to identify all issues, but the 936 scoring methodology helps to highlight and prioritize cybersecurity risks that are likely to exceed 937 allowable risk tolerance (e.g., known software vulnerabilities on critical assets that are not

938 mitigated within a designated grace period).²²

²¹ Information about the NIST SCAP is available at <u>https://csrc.nist.gov/projects/security-content-automation-protocol/</u>

²² More information about the DHS AWARE scoring method is available from: <u>https://www.cisa.gov/cdm-training</u>
939 2.2.4 Determining Potential Impact

940 The final prerequisite for creating a practical list of risk scenarios for the risk register is the

941 determination of the potential impact of the threats and vulnerabilities described above. The

942 section below describes the completion of part D of the CSRM Risk Description column (Figure943 9.)





Figure 9: Adverse Impact Inclusion in Risk Scenario Identification (Part D)

946 Discovery activities throughout Section 2.2 may have already highlighted potential adverse

947 impacts to explore. Description of the impact is a key element for enterprise stakeholders and

948 represents the connection between cybersecurity risks and the enterprise objectives that would be

affected by those risks. Reviewing the key enterprise objectives, as identified in scoping, and

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

- 951 realistic scenarios.
- 952 While some types of impact may not be immediately apparent, the long-term effects can be
- 953 significant. For example, consider a situation where a criminal has gained unauthorized access to

an enterprise system and has exfiltrated a large amount of confidential data. If that criminal is

955 cautious, there may not be any disruption of operations. In fact, sometimes cyber criminals

actually try to *improve* the health of a victim's technology to ensure that it will be available for

957 their malicious activity. In this case, the system may seem to be working fine—even better than

958 ever—and then later, the enterprise realizes that a catastrophic loss has occurred.

959 Notably, impact scenarios can be considered in light of a continuum rather than as a binary state.

- 960 Many impacts will cause mission degradation or reduced performance and may not exhibit
- 961 themselves as a full interruption of service or capability. This consideration should be factored
- 962 into risk prioritization and analysis.
- Risk scenarios should be assessed in terms of both initial impact and downstream consequences.Factors to consider include:
- Primary impact the initial impact following a negative cybersecurity event, such as the downtime when a website is unavailable to customers
- 967 Secondary impact A loss event that occurs subsequent to the primary impact as a downstream or cascading impact to the enterprise
- 969 For example, consider a large enterprise that experiences a breach of confidential customer data.
- 970 In this example, an external attacker with criminal intent might attack a highly critical and
- 971 sensitive customer database through a software vulnerability in the internet-facing website. The
- 972 initial impact may be minimal since exfiltration is not disruptive, and the company may not even

- 973 detect an issue. Once the problem has been discovered, there may be primary impact, such as:
- 974 • Cost of a focused investigation into the breach
- 975 Price of restitution for customer losses (e.g., credit monitoring services) •
- The expense of third-party specialists to provide forensic expertise and to ensure 976 • 977 adequate mitigation of the cybersecurity incident
- Cost of immediate capital investment to address cybersecurity issues that contributed to 978 979 the breach
- 980 Long-term or secondary effects may be more impactful. They can include:
- 981 Loss of market share due to eroded trust in the company's reputation •
- Revenue losses from organizations that choose not to renew contracts 982 •
- 983 • Fines and penalties from regulators

984 When considering the impact component of risk scenarios, it is important to consider the 985 frequency of potential consequences. A risk event of moderate impact that occurs weekly may, 986 over time, represent a higher risk than that of a major event that occurs infrequently. Such 987 temporal factors may be valuable for stakeholders' understanding and reporting of risks. For 988 example, senior leaders may wish to see the impact of a risk expressed as the loss for each 989 occurrence (the single loss expectancy, or SLE), or they might prefer to see the total loss for that 990 risk over an annual period (the annualized loss expectancy, or ALE). Consistent documentation 991 of impact frequency is also important for supporting the integration and aggregation of risk 992 registers.

- 993 As with other risk components, impact considerations may be either qualitative or quantitative, 994 as illustrated by the examples in Table 8.
- 995

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.

996 2.2.5 Recording Identified Risks

997 Using the four elements described in earlier subsections (i.e., key assets, threats, vulnerabilities, 998 and impacts), practitioners can record relevant cybersecurity risks in the risk register.

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

999



Figure 10: Example Risk Register with Sample Risk Descriptions

1001 The use of detailed risk scenarios helps ensure that all understand the risks being considered and 1002 the impacts on organizational objectives. The risk description need not be exhaustive but should 1003 include sufficient information to support subsequent analysis, evaluation, treatment, and

1004 monitoring. An example risk description based on the data breach illustration above might say:

- 1005 External criminal attacker exploits a software vulnerability in the internet-
- 1006 facing customer data site, resulting in "significant" customer confidential data
- 1007 exfiltration with revenue, reputation, and regulatory implications.

1008 In support of ERM, practitioners need to continually balance an understanding of what mission 1009 objectives can be affected by various threats (a top-down consideration) and how various threats

- 1010 can impact enterprise objectives (a bottom-up consideration). Both sets of conditions are
- 1011 continually changing, so CSRM is an iterative activity of ongoing discovery, communication,

1012 response, and monitoring. CSRM itself is conducted as part of a broader ERM life cycle. In

1013 addition to the known risks that are already being monitored, there may also be developing or

- 1014 *emergent risks* that are yet to be fully defined but might disrupt enterprise objectives in the 1015 future
- 1015 future.

Each of the activities in Section 2.2 is iterative and supports the top-down/bottom-up approach
described above. An initial list of scenarios can be developed and used to consider threats and
vulnerabilities. As threats and vulnerabilities are explored, those might lead to the discovery of

1019 additional risk scenarios to be considered. This iterative process can be adjusted and tailored to

- 1020 develop and maintain a practical and manageable set of risks.
- As an example, consider some high-value assets that are important to a local hospital and issues
 that could jeopardize those assets. Some top-down considerations may include:

- Patient record database a ransomware attack could encrypt critical records; a network outage could disrupt availability; an authentication issue could hamper the ability to log in; a software upgrade could inadvertently corrupt the data.
- Pharmaceutical system provided by a third party a malicious (or tricked) insider could alter pharmacy records, resulting in the incorrect medication being given to a patient; the malicious external party could break in and disclose or destroy pharmacy records; a construction incident could sever network communications to the service.
- Point of care (PoC) terminals authentication system failure could disrupt the ability to provide patient care; user data error could result in inaccurate and potentially unsafe patient conditions; an improperly tested software patch could render terminals unusable.
- 1033 Bottom-up considerations would start with threats and vulnerabilities and consider where those 1034 can lead:
- Ransomware attack through a social engineering attack (e.g., web-based malware driveby attack, email phishing attack) – Attack could render many systems unreadable, including patient care databases, pharmacy records, billing systems, and payroll.
- Network outage due to a firewall malfunction An internal failure of a major switch or router could result in localized failures of PoC terminals, patient in-processing, and medical care services (e.g., review of radiology reports). External connectivity failure would disrupt electronic mail, clinical professional services, pharmaceutical processing, 1042
- Physical hardware malfunction through a failed component risk technical equipment (e.g., televisions) could be rendered unavailable with few consequences. -risk technology (e.g., patient scanners) malfunctions could fail to provide timely and accurate patient results. Awaiting replacement systems could lead to potential injuries (e.g., through fire or electrical shock) or delays in patient care.

1048 Thorough risk identification in realistic, and mission-oriented scenarios help to communicate the 1049 connection between various uncertainties and the mission objectives that might be affected.

1050 2.2.6 Risk Categorization

Each risk in the CSRR should also indicate the relevant risk category (indicated by the yellow
dashed box in Figure 11) based on the risk strategy guidance described in Section 2.1. Categories
could be any taxonomy that helps aggregate risk information and supports the integration of
cybersecurity risk registers for ERM decision support. Example risk categories include:

- 1055
 Risk framework groupings, such as NIST RMF families (e.g., Access Control, Supply Chain Risk Management)
- Threat types, such as intentional disclosures, unintended modifications, system failures, or natural disasters
- Impact considerations based on business units affected or information systems impacted

- 1060 Consistent risk categorization supports effective integration of cybersecurity risks throughout the
- 1061 enterprise and aggregation into an enterprise cybersecurity risk register. That information
- 1062 ultimately becomes part of the overall Enterprise Risk Register and the Enterprise Risk Profile.

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

1063 2.3 Detailed Risk Analysis





Figure 11: CSRR Highlighting Risk Category and Current Assessment Columns

1066 Risk analysis enables to determination of the likelihood of impact and priority of treatment. This 1067 section helps to complete the likelihood and impact columns of the cybersecurity risk register

1068 and the exposure column that represents the product of those two values. These columns are

1069 illustrated by the solid red box in Figure 11.

1070 Because cybersecurity risk reflects the effect of uncertainty on or within a digital component that

1071 supports enterprise objectives, risk analysis helps to measure both the level of uncertainty

1072 entailed by the risk scenario and the extent of the uncertain effect upon enterprise objectives.

1073 Deterministic models can provide a detailed analysis of likelihood and impact where sufficient

1074 information is available for such a determination. In other cases, the randomness of uncertainty

and the many factors involved in complex information and technology better support a

1076 probabilistic (or stochastic) methodology.

1077 **2.3.1** Selecting Risk Analysis Methodologies

1078 International Electrotechnical Commission (IEC) standard 31010:2019, *Risk management* —

1079 *Risk assessment techniques*, states, "In deciding whether a qualitative or quantitative technique is

1080 more appropriate, the main criteria to consider are the form of output of most use to stakeholders

- and the availability and reliability of data. Quantitative techniques generally require high quality
- 1082 data if they are to provide meaningful results. However, in some cases where data is not
- 1083 sufficient, the rigor needed to apply a quantitative technique can provide an improved
- understanding of the risk, even though the result of the calculation might be uncertain" [13].
- 1085 Note that multiple methodologies can be used, based on enterprise strategy, organization
- 1086 preference, and data availability.

- 1087 Regardless of the methodologies being applied, it is important to consider as many data points as
- 1088 needed to render a judgement regarding likelihood and impact values. Unfortunately, without
- 1089 supporting data, well-intentioned but misguided methods of risk analysis amount to little more
- than a guess. In many cases, the application of even a moderate amount of deductive reasoning,
- 1091 combined with various analysis techniques, can render a more accurate and reliable risk analysis.
- 1092 Quantitatively informed qualitative decision-making should be the objective in the absence of
- 1093 purely quantitative-driven decisions.
- 1094 Analysis considerations are often provided in a qualitative way, such as, "The patient database is
- 1095 at high risk of unauthorized disclosure because we have learned that hackers are targeting health
- 1096 information systems with ransomware, and we have determined that there are numerous
- 1097 vulnerabilities in our health information system."
- 1098 In other cases, the analysis can be quantitative, such as in the example below:
- 1099 The health information system contains about 12,000 records. A successful ransomware
- breach could cost approximately \$1.3M if the data is destroyed or \$2.5M dollars if the
- breach results in a disclosure. We know that the Arctic Zebra APT team has been
- 1102 targeting similar databases; through our understanding of their techniques and those of
- 1103 others, we believe that there is a 70 % chance they will target us and a 30 % chance
- 1104 (based on internal testing and network scans) that it would be successful. Based on that 1105 data, we believe that there is a 21 % chance of single loss exposure, or between \$273,000
- and \$525,000. This exposure calculation does not consider additional secondary losses,
- 1107 such as lost revenue due to customer erosion from loss of trust or personal lawsuits
- against the firm.
- 1109 Each of these methodologies provides value for the enterprise, and the technique selection should
- 1110 be tailored based on the context and the strategic guidance provided by governance stakeholders.
- 1111 The choice is often driven by the intended outcome and the amount of detailed information
- 1112 available.
- 1113 When selecting a risk assessment technique, organizations should consider the costs of analysis
- 1114 in light of the desired outcome to help determine the most cost-effective technique. An
- 1115 inexpensive but accurate qualitative analysis that identifies the most risks and leads to mitigating
- 1116 those risks to the best possible degree may be the right move for a particular organization. For
- 1117 others, a highly detailed quantitative risk assessment may require more resources than a
- 1118 qualitative approach but may also provide specific and actionable information that helps to focus
- 1119 attention on important threat scenarios.

1120 **2.3.2** Techniques for Estimating Likelihood and Impact

1121 NISTIR 8286 highlights the need for improved risk analysis when estimating and recording the

1122 likelihood and impact of cybersecurity events and monitoring to assure that risks remain within

1123 acceptable parameters.²³ To improve enterprise risk estimation accuracy and consistency, CSRM

1124 practitioners are encouraged to explore the use of tools and processes that support measurable

- and meaningful risk analysis and reporting.
- 1126 Some analysis techniques are based on estimates from subject matter experts' (SMEs) experience
- and knowledge. Some methods, such as this SME estimation, can be subjective. Other methods
- are more objective and based on analytical considerations, statistical analysis, and scenario
- 1129 modeling, as well as potentially drawing on knowledge of previous events.
- 1130 Understanding the intended purpose of the analysis can help one decide which techniques to use.
- 1131 For example, a detailed and quantified approach may be valuable as a basis for a comprehensive
- 1132 review or update of the enterprise cybersecurity approach. Detailed evaluation helps to reinforce
- 1133 defense measures and increase resilience, as in the following example:
- 1134 Enterprise leaders have learned through an InfraGard alert that there is a high
- probability that companies in its sector will be targeted by a particular APT group.
- 1136 Because internal cybersecurity risk managers have performed threat modeling based
- 1137 on the MITRE Adversarial Tactics, Techniques, and Common Knowledge
- 1138 (ATT&CK®) and Pre-ATT&CK frameworks, the company was able to quickly
- 1139 consider high-value assets that would most likely be at risk.
- 1140 A key tactic, technique, or procedure (TTP) of this attack is through "password
- spraying" brute force login attempts. It is known that several critical systems have not
- 1142 yet been updated to support multi-factor authentication and would be vulnerable to
- such an attack. A poll of the security leaders in the organization (using a Delphi
- exercise) determined that there is a 50-70 % chance that the payroll system will be
- 1145 attacked (the mean value was 60 %). A successful attack on that system would have a 1146 direct and indirect financial impact of between \$1.7M and \$2.4M US with the most
- 1147 likely impact being \$2.0M. Therefore, the risk exposure value for this row of the risk
- 1148 register was established at \$1.2M (based on .6 x \$2M).
- 1149 Notably, the example above provides several ranges of estimates. Some industry specialists have
- 1150 indicated that a range of possible values is more helpful and likely more accurate than a single
- 1151 "point estimate." Additionally, while this example uses the mean values of those ranges to
- 1152 identify the likelihood and the potential impact, the ranges themselves are often recorded in the
- risk register. In this instance, given a possible impact of "between \$1.7M and \$2.4M," the
- 1154 exposure may have been presented as "\$1.02M to \$1.44M."

²³ 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.

1155 **2.3.2.1** Improving Estimation Based on Knowledge of Prior Events

- 1156 In many cases, information about previous risk events may be helpful when estimating the
- 1157 likelihood and impact of those in the future. For example, practitioners should consult industry
- 1158 literature, their current power companies, or ISPs for descriptions of loss events within a given
- 1159 sector or over a particular time frame. To determine the likelihood of a utility outage, the utility
- 1160 provider can be asked to provide details regarding previous disruptions and their duration.

1161 As an example, consider the example organization in the first row in Table 2: Examples of Risk

- 1162 Appetite and Risk Tolerance. It describes a global retail firm at which a senior leader has
- 1163 expressed the risk tolerance statement that "any outage that exceeds four hours for any customer
- 1164 requires significant corrective action." Risk practitioners can review the actual availability of that
- 1165 website for the previous year (using a table similar to Table 9.)
- 1166

Table 9: Example Risk Tolerance Results Assessment

Month	Total Hours in the Month	# of Hours Unavailable	Outage Customer %	Available Hrs (Total hrs- Outage)	Appetite Limit (99.95% of Total)	Tolerance Limit (Total - 4 hrs)	Avail % (Avail. hrs + Total hrs)
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%
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%

1167 In this case, the system did not exceed the risk tolerance since no single outage exceeded four

1168 hours, nor did any outage impact more than 5% of customers. While past performance is not a

1169 guarantee of future probability, it provides some information that helps inform likelihood

1170 estimates. The impact of an outage is likely similar to that in previous iterations; understanding

1171 of the probability of an outage, given what is known about prior disruption, helps consider the

1172 likely exposure in the future.

1173 When considering each risk in the risk register, practitioners will analyze the likelihood that any

1174 risk would result in an impact that would exceed the risk tolerance. That consideration provides a

- 1175 basis for risk treatment decisions, either to ensure sufficient security controls or to review risk
- 1176 tolerance statements to ensure that they represent reasonable and practical expectations.

1177 2.3.2.2 Three-Point Estimation

- 1178 One method for considering the likelihood or impact of a risk event is three-point estimation.
- 1179 This method,²⁴ illustrated in Figure 12, is useful because it considers the judgement of available
- 1180 subject matter experts (SMEs). For example, to determine the impact²⁵ of a successful phishing
- 1181 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)).
- 1185 Figure 12 illustrates the result of an SME estimating a \$80K revenue loss due to an attack that
- 1186 would be successful if employees are not properly trained. This first estimate represents a worst-
- 1187 case scenario (pessimistic). The same estimator may suggest that, if the attack were successful
- 1188 but limited in spread, only a \$35K impact is likely (optimistic). Finally, the SME may suggest
- that the most likely impact of recovering from such as successful phishing attack would be \$50K.



1190 1191

Figure 12: Example Three-Point Estimate Graph (Triangle Distribution)

1192 The three datapoints can be categorized as **O**ptimistic (\$35K), **P**essimistic (\$80K), and **M**ost 1193 likely (\$50K). A simple average of the three numbers (called a *Triangular Distribution*) is:

²⁴ 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.

²⁵ Although impact was used in this example, three-point estimating can also be used in determining likelihood.

1194
$$EV = \frac{P+M+O}{3} = $52.5K \text{ in this example where } O=$35K, P=$80K, and M=$50K$$

1195 In this phishing attack scenario, perhaps the estimator believes that the pessimistic and optimistic

- values are too different and the estimator believes that the "most likely" estimate is a better
- 1197 predictor. The estimator can give greater weight (perhaps 4 times as much) to the "most likely"
- 1198 value using the following standard formula (called the *Average for a Beta Distribution*):

1199
$$EV = \frac{P+4M+0}{6} = $52.5K \text{ in this example where } O=$35K, P=$80K, and M=$50K$$

1200 The next question is, "How confident is the estimator regarding this estimated impact of a

- 1201 successful phishing attack?" In three-point estimating, confidence (referred to as *sigma*, or σ) in
- 1202 the estimated value can be predicted by calculating the standard deviations from the mean. A 1202 useful model for determining signal is $z = \frac{P-0}{P}$

1203 useful model for determining sigma is
$$\sigma = \frac{1}{6}$$
.

1204 Figure 13 illustrates these values graphically. Statistical models have demonstrated that, given

1205 the mean (EV) and standard deviation, one can determine the level of confidence (or confidence

1206 interval $[CI]^{26}$) in the financial estimates. For the example above, the estimator will have a

1207 68.27% confidence that the financial impact of a successful phishing attack will result in a loss

between \$39K and \$66K. The estimator will have approximately a 95% confidence that the loss

1209 will be between \$25.5K and \$79.5K, and a nearly 100% confidence in the \$12K to \$93K

1210 estimate. This application of CI is useful for each of the analysis methods in this section and

1211 helps to represent the level of uncertainty in each of the estimates.





Figure 13: Example Three-Point Estimate Graph (Normal Distribution)

²⁶ 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.)

- 1214 Confidence requirements and standardized methods of calculation should be included in senior
- 1215 leaders' ERM strategy as part of enterprise risk management policy. This directive helps all risk
- 1216 practitioners in the enterprise to consider risk in a similar manner and may help to improve the
- 1217 reliability of likelihood and impact estimates. Additionally, as more information becomes
- 1218 available regarding previous risk results and those of external organizations, this information can
- 1219 be included in the estimation models and used to reduce uncertainty.
- 1220 Notably, the level of effort for estimating risk factors increases with the required level of rigor.
- 1221 An estimate with very low CI might be simple to develop (perhaps as simple as flipping a coin)
- but likely offers little value. A CI of 99% may be important in some situations, but the work to
- develop a more precise estimate can cost significantly more than that required for a 90% CI.
 Because the appropriate levels of accuracy and precision for cybersecurity risk analysis will vary
- Because the appropriate levels of accuracy and precision for cybersecurity risk analysis will vary based on enterprise needs, the techniques and expectations should be clearly defined as part of
- 1226 the enterprise's risk management guidance.
- 1227 It is critical that the risk practitioner consider the accuracy of the SME estimates overtime to
- 1228 determine who or what source is more accurate and then consider that expert judgement more
- 1229 prominently in calculations for the ongoing risk management cycles. Experts who are overly
- 1230 optimistic or pessimistic create a broad range. However, when accuracy is required, especially
- 1231 when calculating likelihood, knowing who the best estimators are in the organization is vitally
- 1232 important.

1233 2.3.2.3 Event Tree Analysis

1234 Event Tree Analysis (ETA) is a graphical technique that helps practitioners evaluate the

- downstream impact of a given scenario (as determined in Section 2.2.4.) The exercise helps
- document a sequence of outcomes that could arise following an initiating threat event (e.g., a
- particular TTP, as described in Section 2.2.2). By iterating through a series of what-if scenarios,
 the practitioner can analyze each set of circumstances and determine the likelihood that the
- results would occur. The below example demonstrates the layered defense that an organization
- 1240 employs to prevent malicious code from being used to exfiltrate data. For each condition, the
- 1240 employs to prevent manerous code from being used to eximitate data. For each condition, the 1241 analyst considers a Boolean (i.e., true or false) answer. The analyst then follows through each
- 1242 iterative outcome until an end result is reached.
- 1243 This analysis can be performed in a qualitative way (using the yes or no conditions), or a
- 1244 probability could be calculated for each scenario.
- 1245 In Figure 11, the probability is calculated based on whether the attack was prevented (Yes) or if
- 1246 the attack was successful (No). Since each branch of the tree represents a binary option, the sum
- 1247 of the two probabilities is always equal to 100% (or 1.00 in decimal format). In this example, the
- 1248 calculated probabilities provide information about the potential success (or failure) of risk
- response. The resulting probability (*Pr* values in the example below) is multiplied by the
- anticipated financial loss of the scenario. In the tree below, if the anticipated loss of sensitive
- 1251 data being exfiltrated is \$1.4M, then there is a \$205,100 risk exposure (\$1.4M x .1463).



1252 1253

Figure 14: 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

1259 impacts to the organization and the sequence of events leading to those consequences.

1260 2.3.2.4 Monte Carlo Simulation

1261 While expert judgement is valuable in estimating risk parameters, one way to reduce subjectivity 1262 in the above methods is to supplement that judgement using simulation models. For example, using the Monte Carlo method, the above parameters could be modeled repeatedly (perhaps 1263 several hundred thousand cycles) to help account for the many random variables inherent in 1264 1265 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 1266 probabilities can help identify a range of possible values.²⁷ The results of such a simulation can 1267 be plotted on a graph or distribution to facilitate a visual understanding. 1268

²⁷ 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

- 1269 For example, when calculating the financial impact of the attack on the payroll system (from the
- 1270 example above), practitioners can use a simulation model to consider the most likely range
- 1271 between the low value (\$1.7M) and the high value (\$2.4M). The result of this simulation could
- 1272 be recorded as a histogram recording the frequency in which certain random values occurred, in
- 1273 this case resulting in a simulated estimated impact of \$2M.



1274 1275

Figure 15: Illustration of a Histogram from a Monte Carlo Estimation Simulation

1276 **2.3.2.5 Bayesian Analysis**

1277 While there is value in using expert judgement to help estimate risk parameters, it might be 1278 improved based on information known from prior events, and the results may represent a more 1279 objective determination. For example, if the organization has identified that several critical

1280 software vulnerabilities have remained uncorrected, there is an increased likelihood that a threat

- actor will be able to exploit a software vulnerability to successfully gain access to the enterprise
- and exfiltrate valuable data. Bayesian analysis describes methods for considering conditional
- 1283 probability, applying a distribution model and a set of known prior data to help estimate the
- 1284 probability of a future (posterior) outcome.

1285 While an SME might render an opinion regarding how likely a breach might be, that opinion can

be improved by what the enterprise risk managers already know about the success of previous

1287 attempts by others or about the success of adversaries in similar enterprises. Prior knowledge,

1288 drawn from internal observations and events at similar organizations can be of significant value

1289 for improving the accuracy and reliability of estimates, such as those for determining the

1290 likelihood of an impactful event or for estimating the impact of that uncertainty on the enterprise

1291 objectives. Similar methods can be used to estimate whether several conditions might occur

- 1292 (joint probability) or that certain conditions would occur given other external variables (marginal
- 1293 probability).

1294 **2.4** Determination and Documentation of Risk Exposure

1295 Once the probability that an impactful event will occur has been determined and the most

1296 probable impact of such an occurrence has been calculated, the information is recorded in the

1297 risk register. Figure 16 shows how an organization can record this information.



1298 1299

Figure 16: Example Quantitative Analysis Results



ID	Priority	Risk Description	Risk	Current Assessment				
		Kisk Description	Category	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)	н	н	н		

1301

1302

Figure 17: Example Qualitative Analysis Results

1303 In this example, internal SMEs feel that the likelihood of an attack on the organization's mobile

banking application is High. A survey of the SMEs reflects their decision that the impact to the

1305 organization if customers experience such an event would be High, based on customers'

1306 perception that the application lacked sufficient security protections. In this case, the practitioner

1307 would use the enterprise assessment scale for determining qualitative risk, such as the application

1308 of Table I-2, Assessment Scale – Level of Risk (Combination of Likelihood and Impact), from SP

1309 800-30, Revision 1. Based on that table, an event with High likelihood and High impact would

1310 be ranked as a High exposure. As an example, this decision would help inform the selection of

- 1311 strong user authentication and encryption controls.
- 1312 Risk priority is described in NISTIR 8286B and will be determined based on mission objectives,
- 1313 enterprise strategy, and the results of comprehensive risk identification and analysis activities.

1314 **3** Conclusion

- 1315 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
- 1318 cybersecurity risk at the Business and System levels. This is reflected by including the
- 1319 determination of enterprise risk appetite and organizational risk tolerance among the first tasks in
- 1320 both the Cybersecurity Framework and the NIST Risk Management Framework.

	Notional Cybersecurity Risk Register											
	Priority	Risk Description	Risk Category	Current Assessment		Risk	Risk	Risk	Risk			
ID				Likelihood	Impact	Exposure Rating	Response Type	Response Cost	Response Description	Owner	Status	
1												
2												
3												
4												
5												
			Co	ntinually	Commu	nicate, Lo	earn, and	Update				



Figure 18: Use of a Cybersecurity Risk Register Improves Risk Communications

1323 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

1325 identifying potential risks (as described in Section 2.2), estimating the probability that an

1326 impactful event will occur, calculating the potential harm to the enterprise after such an event,

1327 and analyzing the actual risk exposure (the product of likelihood and impact).

1328 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

1330 cybersecurity risk. While statistical analysis has been available for hundreds of years, many

1331 within the CSRM community are only recently recognizing the value of applying a more

1332 quantitative approach to risk estimation. It seems likely that those in the CSRM domain will

1333 continue to develop and improve statistical methods to estimate risk and include guidance

1334 regarding the application of various statistical distribution models.

1335 Responses to previous requests for information have indicated that enterprise risk managers

1336 desire increased rigor in the manner in which risk identification, analysis, and reporting are

1337 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

1339 publications in this series will describe improvements to the manner in which risk scenarios are

1340 prioritized, treated, and reported. Through the 8286 series publications, NIST will continue to

1341 collaborate with public- and private-sector communities to address methods for improving

1342 integration and coordination of ERM and CSRM.

1343 **References**

- 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] National Institute of Standards and Technology (2020) *Online Informative References*. Available at <u>https://www.nist.gov/cyberframework/informative-references</u>
- [3] International Organization for Standardization (ISO) (2018) Risk management— Guidelines. ISO 31000:2018. Available at <u>https://www.iso.org/standard/65694.html</u>
- [4] 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. <u>https://doi.org/10.6028/NIST.SP.800-37r2</u>
- [5] National Institute of Standards and Technology (2018) Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. (National Institute of Standards and Technology, Gaithersburg, MD). <u>https://doi.org/10.6028/NIST.CSWP.04162018</u>
- [6] 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 <u>https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2016/m-16-17.pdf</u>
- 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. <u>https://doi.org/10.6028/NIST.SP.800-30r1</u>
- [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 <u>https://www.whitehouse.gov/wpcontent/uploads/2018/12/M-19-03.pdf</u>
- [9] National Institute of Standards and Technology (2020) *Security Content Automation Protocol.* Available at <u>https://csrc.nist.gov/projects/security-content-automation-protocol</u>
- [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. <u>https://doi.org/10.6028/NIST.SP.800-53r5</u>
- 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. <u>https://doi.org/10.6028/NIST.SP.800-53Ar4</u>
- [13] International Electrotechnical Commission (IEC) (2019) Risk management Risk assessment techniques. IEC 31010:2019. Available at https://www.iso.org/standard/72140.html

1344

1345 Appendix A—Acronyms

- 1346 Selected acronyms and abbreviations used in this paper are defined below.
- 1347AISAutomated Indicator Sharing1348APTAdvanced Persistent Threat
- 1349BIABusiness Impact Analysis
- 1350 CCE Common Configuration Enumeration
- 1351 CDM Continuous Diagnostics and Mitigation
- 1352 CI Confidence Interval
- 1353 CISA Cybersecurity and Infrastructure Security Agency
- 1354 CMDB Configuration Management Database
- 1355 CPE Common Platform Enumeration
- 1356 CSRM Cybersecurity risk management
- 1357 CTI Cyber Threat Intelligence
- 1358 CVE Common Vulnerabilities and Exposures
- 1359CVSSCommon Vulnerability Scoring System
- 1360 DHS Department of Homeland Security
- 1361 DIB Defense Industrial Base
- 1362 DISCE U.S. Department of Defense Information Sharing Environment
- 1363 ERM Enterprise Risk Management
- 1364 ETA Event Tree Analysis
- 1365 FOIA Freedom of Information Act
- 1366 HVA High-Value Asset
- 1367 IDS Intrusion Detection Systems
- 1368 IEC International Electrotechnical Commission

- 1369IoCIndicators of Compromise
- 1370 ISAC Information Sharing Analysis Center
- 1371 ISAO Information Sharing and Analysis Organization
- 1372 ITAM Information Technology Asset Management
- 1373 ITL Information Technology Laboratory
- 1374 NCCIC National Cybersecurity and Communications Integration Center
- 1375 NISTIR NIST Interagency or Internal Report
- 1376 NTCTF NSA/CSS Technical Cyber Threat Framework
- 1377 NVD National Vulnerability Database
- 1378 OLIR Online Informative References
- 1379 OMB Office of Management and Budget
- 1380 OVAL Open Vulnerability Assessment Language
- 1381 RMF Risk Management Framework
- 1382SCAPSecurity Content Automation Protocol
- 1383 SIEM Security Incident Event Monitoring
- 1384SMESubject Matter Experts
- 1385 SWOT Strength, Weakness, Opportunity, Threat
- 1386 TTP Tactics, Techniques, and Procedures
- 1387 VPN Virtual Private Network

Appendix B—NVD/NCP Support for Vulnerability Identification and Analysis

- 1389 The Computer Security Division of NIST's Information Technology Laboratory, in collaboration
- 1390 with the DHS Cybersecurity & Infrastructure Security Agency (CISA), provide the National
- 1391 Vulnerability Database (NVD) and the National Checklist Program (NCP) as two key resources
- 1392 for identifying, evaluating, and responding to cybersecurity risks. These sites are available at
- 1393 <u>https://nvd.nist.gov</u> and <u>https://checklists.nist.gov</u>, respectively.
- 1394 These resources, originally created in 2000 as the Internet Categorization of Attacks Toolkit
- 1395 (ICAT), are available without cost to all public- and private-sector organizations to help improve
- 1396 CSRM. The data that these sites provide enable the automation of vulnerability management,
 1397 security measurement, and compliance. The sites include databases of security checklist
- references, security-related software flaws, misconfigurations, product names, and impact
- 1399 metrics. These sites act as the U.S. Government repository of standards-based vulnerability
- 1400 management data represented using the Security Content Automation Protocol (SCAP),
- 1401 including the following data exchange specifications: [9]
- The Common Vulnerabilities and Exposures (CVE) specification helps products and personnel track known vulnerabilities and their characteristics. Each vulnerability is assigned a unique identifier that enables common reference and information sharing.
- The Common Vulnerability Scoring System (CVSS) provides a severity score and other
 severity factors for each CVE. This severity data helps enterprise automation tools
 support risk analysis and prioritization.
- The Common Configuration Enumeration (CCE) provides unique identifiers to system 1408 • 1409 configuration issues in order to facilitate the fast and accurate correlation of configuration 1410 data across multiple information sources and tools. A recent NVD offering provides a correlation between a CCE (that might represent a vulnerability through 1411 1412 misconfiguration) and one or more security controls as described in NIST SP 800-53, 1413 Security and Privacy Controls for Information Systems and Organizations. This feature 1414 supports the improved automation of documentation and the mitigation of vulnerabilities (available at https://nvd.nist.gov/config/cce). 1415
- The Common Platform Enumeration (CPE) uniquely identifies asset types to help automate the association of vulnerabilities with enterprise asset types.
- Checking languages, such as Open Vulnerability Assessment Language (OVAL), enables
 automated assessments to identify and report resources that may be vulnerable.
- While the specifications above support data exchange regarding vulnerabilities on various
 platforms, the methods for identification on endpoints themselves can vary greatly from product
 to product. Many product vendors have developed highly sophisticated methods for detecting
 and reporting those flaws. Because practitioners need to ensure that those detection and reporting
 processes are reliable and interoperable, NIST provides the SCAP Validation Program. Products
- 1425 on the SCAP Validated Products List have demonstrated that they are able to perform against a
- 1426 set of derived test requirements to ensure that they can fulfill the CSRM purpose.