

NIST Special Publication 800
NIST SP 800-221r1 ipd

Enterprise Impacts of Information and Communications Technology Risk

*Governing and Managing ICT Risk Programs Within an
Enterprise Risk Portfolio*

Initial Public Draft

Stephen Quinn
Julie Chua
Daniel Eliot
Nahla Ivy
Matthew Barrett
Larry Feldman
R. K. Gardner
Karen Kent
Daniel Topper
Greg Witte

This publication is available free of charge from:
<https://doi.org/10.6028/NIST.SP.800-221r1.ipd>

NIST Special Publication 800
NIST SP 800-221r1 ipd

Enterprise Impacts of Information and Communications Technology Risk

*Governing and Managing ICT Risk Programs Within an
Enterprise Risk Portfolio*

Initial Public Draft

Stephen Quinn
*Computer Security Division
Information Technology Laboratory*

Julie Chua
Daniel Eliot
*Applied Cybersecurity Division
Information Technology Laboratory*

Nahla Ivy
*Enterprise Risk Management Office
Office of Financial Resource Management*

Matthew Barrett
CyberESI Consulting Group, Inc.

Larry Feldman
Daniel Topper
Huntington Ingalls Industries

R. K. Gardner
New World Technology Partners

Karen Kent
Trusted Cyber Annex

Greg Witte
Palydin LLC

This publication is available free of charge from:
<https://doi.org/10.6028/NIST.SP.800-221r1.ipd>

October 2026



U.S. Department of Commerce
Howard Lutnick, Secretary

National Institute of Standards and Technology
Arvind Raman, NIST Director and Under Secretary of Commerce for Standards and Technology

Certain equipment, instruments, software, or materials, commercial or non-commercial, are identified in this paper in order to specify the experimental procedure adequately. Such identification does not imply recommendation or endorsement of any product or service by NIST, nor does it imply that the materials or equipment identified are necessarily the best available for the purpose.

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

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

Authority

This publication has been developed by NIST in accordance with its statutory responsibilities under the Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. § 3551 et seq., Public Law (P.L.) 113-283. NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems, but such standards and guidelines shall not apply to national security systems without the express approval of appropriate federal officials exercising policy authority over such systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130.

Nothing in this publication should be taken to contradict the standards and guidelines made mandatory and binding on federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other federal official. This publication may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright in the United States. Attribution would, however, be appreciated by NIST.

NIST Technical Series Policies

[Copyright, Use, and Licensing Statements](#)

[NIST Technical Series Publication Identifier Syntax](#)

Publication History

Approved by the NIST Editorial Review Board on YYYY-MM-DD [Will be added to final publication.]

Supersedes NIST Series XXX (Month Year) DOI [Will be added to final publication, if applicable.]

How to Cite this NIST Technical Series Publication

Quinn S, Chua J, Eliot D, Ivy N, Barrett M, Feldman L, Topper D, Gardner RK, Kent K, Witte G (2026) Enterprise Impact of Information and Communications Technology Risk: Governing and Managing ICT Risk Programs Within an Enterprise Risk Portfolio. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-221r1 ipd. <https://doi.org/10.6028/NIST.SP.800-221r1.ipd>

Author ORCID iDs

Stephen D. Quinn: 0000-0003-1436-684X

Julie Chua: 0009-0007-9093-7364

Daniel Eliot: 0009-0006-3078-555X

Nahla Ivy: 0000-0003-4741-422X

Matthew Barrett: 0000-0002-7689-427X

Larry Feldman: 0000-0003-3888-027X
Daniel Topper: 0000-0003-2612-7547
Karen Kent: 0000-0001-6334-9486
Gregory A. Witte: 0000-0002-5425-1097

Public Comment Period

October 22, 2026 – December 7, 2026

Submit Comments

ictm@nist.gov

Additional Information

Additional information about this publication is available at <https://csrc.nist.gov/pubs/sp/800/221/r1/ipd>, including related content, potential updates, and document history.

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

Abstract

All enterprises should ensure that information and communications technology (ICT) risk receives appropriate attention within their enterprise risk management (ERM) programs. This document is intended to help individual organizations within an enterprise improve their ICT risk management (ICTRM) in alignment with the NIST Cybersecurity Framework (CSF) 2.0. This can enable enterprises and their component organizations to better identify, assess, and manage their ICT risks in the context of their broader mission and business objectives. This document explains the value of integrating risks that may be addressed at lower system and organizational levels to the broader enterprise level by focusing on the use of ICT risk registers as input to the enterprise risk profile. Consistent with CSF 2.0's Govern function, this publication emphasizes that cybersecurity governance should be central to all risk management activities to ensure that ICT risk management aligns with enterprise strategy and receives appropriate oversight and resources from senior leadership. These guidelines support organizations of all sizes and sectors in implementing governance outcomes that connect ICT risk management with the six core CSF 2.0 functions: Govern, Identify, Protect, Detect, Respond, and Recover.

Keywords

enterprise risk management (ERM); enterprise risk profile (ERP); enterprise risk register (ERR); information and communications technology (ICT); ICT risk; ICT risk management (ICTRM); ICT risk measurement; risk appetite; risk register; risk tolerance.

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems. The Special Publication 800-series reports on ITL's research, guidelines, and outreach efforts in information system security, and its collaborative activities with industry, government, and academic organizations.

33 **Audience**

34 The primary audience for this publication includes both federal and non-federal professionals at
35 all levels who understand ICT risk management (ICTRM) for one or more ICT domains but may
36 be unfamiliar with enterprise risk management (ERM). The secondary audience includes both
37 federal and non-federal corporate officers, high-level executives, ERM officers and staff
38 members, and others who understand ERM but may be unfamiliar with the unique
39 characteristics of ICTRM. All readers are expected to gain an improved understanding of how
40 ICTRM and ERM relate to each other, as well as the benefits of integrating their use.

41 **Document Conventions**

42 For this document, “assets” are defined as technologies that may compose an information or
43 communications system. The term “asset” is used in multiple frameworks and documents.
44 Examples include laptop and desktop computers, servers, sensors, data, mobile devices,
45 networking equipment, cloud services, and super intelligence (SI) systems. In instances where
46 the authors mean “assets” as they might be discussed at the enterprise level, the word “asset”
47 will be preceded by words such as “enterprise” to differentiate context.

48 This document uses the phrase “information and communications technology” for ICT. As of
49 this writing, both this phrase and the same phrase with “communication” instead of
50 “communications” are widely used. The phrases essentially mean the same thing.

51 This document refers to two types of controls, each of which is essential and should not be
52 confused with the other:

- 53 • Internal controls are the overarching mechanisms used to achieve and monitor
54 enterprise objectives. The COSO Internal Control – Integrated Framework¹ defines
55 “internal control” as “a process effected by an entity’s board of directors, management
56 and other personnel designed to provide reasonable assurance of the achievement of
57 objectives” [COSOERM]. These internal controls are important at all levels of the
58 enterprise, as controls are established to manage risks.
- 59 • Risk management controls in the context of ICT represent the safeguards or
60 countermeasures prescribed for an information system or an organization to protect ICT
61 assets and functions in line with mission and business objectives. These controls provide
62 the management, administrative, and technical methods for responding to ICT risks by
63 preventing, deterring, detecting, or correcting threats and vulnerabilities.

64 **Trademark Information**

65 All registered trademarks and trademarks belong to their respective organizations.

¹ The COSO ERM (Committee of Sponsoring Organizations – Enterprise Risk Management) framework is a globally recognized framework for identifying, assessing, and managing risk across an organization. More information is available at:
https://www.coso.org/files/ugd/3059fc_61ea5985b03c4293960642fdce408eaa.pdf

66 **Call for Patent Claims**

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

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

- 76 a) assurance in the form of a general disclaimer to the effect that such party does not hold
77 and does not currently intend holding any essential patent claim(s); or
- 78 b) assurance that a license to such essential patent claim(s) will be made available to
79 applicants desiring to utilize the license for the purpose of complying with the guidance
80 or requirements in this ITL draft publication either:
 - 81 i. under reasonable terms and conditions that are demonstrably free of any unfair
82 discrimination; or
 - 83 ii. without compensation and under reasonable terms and conditions that are
84 demonstrably free of any unfair discrimination.

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

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

92 Such statements should be addressed to: ictm@nist.gov.

Table of Contents

Executive Summary	1
1. Introduction	2
1.1 Purpose and Scope	3
1.2 Document Structure	4
2. Introduction to ICTRM and Challenges with ERM Integration	5
2.1. Comparing ICTRM and ERM	5
2.2. ICTRM Life Cycle	6
2.3. ICTRM and ERM Integration	7
2.4. Shortcomings of Typical Approaches to ICTRM	8
2.4.1. Increasing System and Ecosystem Complexity	9
2.4.2. Lack of Standardized Measures	9
2.4.3. Informal Analysis Methods	10
2.4.4. Overly Focused on the System Level	10
2.4.5. Gap Between ICTRM Output and ERM Input	10
2.4.6. Impact of Opportunities (Positive Risks) Not Pursued	11
3. ICT Risk Considerations	12
3.1. Identify the Context	12
3.1.1. Risk Governance	12
3.2. Risk Culture	15
3.2.1. Risk Capacity, Risk Appetite and Risk Tolerance	15
3.2.2. Risk Management Strategy	17
3.3. Identify the Risks	18
3.3.1. Inventory and Valuation of Assets	19
3.3.2. Determination of Potential Threats	20
3.3.3. Determination of Exploitable and Susceptible Conditions	21
3.3.4. Evaluation of Potential Consequences	22
3.3.5. Risk Register Use	22
3.4. Analyze the Risks	25
3.4.1. Risk Analysis Types	25
3.4.2. Techniques for Estimating Likelihood and Impact	26
3.5. Prioritize Risks	28
3.6. Plan and Execute Risk Response Strategies	30
3.7. Monitor, Evaluate, and Adjust Risk Management	32

128	3.7.1. Adjusting Risk Response Based on Additional Information	33
129	3.8. Managing Positive Risks as Part of Integrated Risk Management	33
130	4. Building ERRs and ERPs from ICTRM-Specific Risk Registers	37
131	4.1. Creating and Maintaining Enterprise-Level ICT Risk Registers	37
132	4.2. Creating the Enterprise Risk Register (ERR)	38
133	4.3. Developing the Enterprise Risk Profile (ERP)	41
134	4.4. Translating the ERP to Inform Leadership Decisions	43
135	5. Enterprise Strategy for ICT Risk Coordination	45
136	5.1. Risk Integration and Coordination Activities	45
137	5.1.1. Detailed Risk Integration Strategy.....	46
138	5.1.2. Risk Monitoring and Communication Activities	49
139	5.2. Aggregation and Normalization of Risk Registers.....	51
140	5.2.1. Aggregation of ICT Risk Information	52
141	5.2.2. Normalization of Risk Register Information	52
142	5.2.3. Integrating Risk Register Details.....	54
143	5.3. Adjusting Risk Responses	55
144	5.3.1. Factors Influencing Prioritization	56
145	5.3.2. ICT Risk Optimization.....	56
146	5.3.3. ICT Risk Priorities at Each Enterprise Level.....	58
147	5.4. Enterprise Adjustments Based on ICT Risk Results	58
148	5.4.1. Adjustments to ICT Program Budget Allocation.....	58
149	5.4.2. Adjustments to Risk Appetite and Risk Tolerance.....	59
150	5.4.3. Reviewing Whether Constraints Are Overly Stringent	60
151	5.4.4. Adjustments to Priority	60
152	6. Conclusion	61
153	References.....	62
154	Appendix A. Acronyms and Abbreviations	65
155	Appendix B. Notional Example of a Risk Detail Record (RDR).....	67
156	Appendix C. Federal Agency-Specific Guidelines for ICTRM	68
157	Appendix D. Change Log.....	70

158

159 **List of Tables**

160	Table 1. Examples of risk oversight roles and responsibilities	13
161	Table 2. Examples of risk appetite and risk tolerance	17
162	Table 3. Descriptions of notional risk register template elements	24
163	Table 4. Response types for negative ICT risks.....	31
164	Table 5. Response types for positive ICT risks.....	36
165	Table 6. Descriptions of additional notional ERR elements	40
166	Table 7. Notional enterprise risk portfolio view for a private enterprise	44
167	Table 8. Inputs and outputs for ERM governance and integrated ICTRM	45
168	Table 9. Notional ICT-related examples that support the MEA Cycle	50
169	Table 10. Examples of ICT risk normalization.....	53
170	Table 11. Similarities among selected ERM and risk management documents.....	68
171	Table 12. Changes from Original Publication	70

172 **List of Figures**

173	Fig. 1. Enterprise hierarchy	5
174	Fig. 2. Notional life cycle for integrated ICTRM.....	6
175	Fig. 3. ICTRM as part of ERM.....	8
176	Fig. 4. Notional risk register template	23
177	Fig. 5. Example of a qualitative risk matrix	29
178	Fig. 6. Example of a semi-quantitative risk matrix	30
179	Fig. 7. Monitor-Evaluate-Adjust Cycle	32
180	Fig. 8. Example of a risk heatmap with positive and negative risks.....	35
181	Fig. 9. ICTRM integration cycle.....	37
182	Fig. 10. Notional example of an ICT-inclusive ERR.....	39
183	Fig. 11. Notional example of an enterprise risk profile.....	42
184	Fig. 12. Impacts on enterprise assets for a business or agency	43
185	Fig. 13. Illustration of enterprise risk management integration and coordination.....	46
186	Fig. 14. Continuous ERM/ICTRM interaction	47
187	Fig. 15. Notional risk detail record	67

188

189 **Executive Summary**

190 Enterprise information and communications technology (ICT) risk management (ICTRM) spans
191 and integrates a broad set of disciplines including cybersecurity, privacy, supply chain,
192 operational technology (OT), Internet of Things (IoT), and super intelligence (SI)². Individual risk
193 programs must integrate their activities within the enterprise portfolio to focus on mission
194 objectives, highlighting the negative risks which may cause the most adverse impact. This
195 publication extends NIST guidelines to recognize that risk crosses the boundaries of individual
196 programs. Effectively addressing these interrelated ICT risks requires coordination,
197 communication, and collaboration across organizational units and at the enterprise level.

198 ICT disciplines form an adaptive system-of-systems whose interconnectedness produces
199 behaviors and risks that cannot be predicted from individual components alone. As systems
200 grow more complex, they present exploitable vulnerabilities, unknown risks, and potential
201 instabilities that can cascade into severe, irreversible consequences.

202 This publication promotes an integrated approach to ICT risk by aggregating and normalizing
203 risk information across domains. Doing so allows organizations to identify, quantify, and
204 communicate risk scenarios in financial, mission, and reputational terms comparable to non-
205 technical enterprise risks, thus enabling executives to prudently allocate resources across
206 competing risk types.

207 While NIST is widely known for providing cybersecurity guidelines, cybersecurity is only one
208 part of a larger risk landscape that also includes: financial, legal, legislative, safety, and strategic
209 risks. ERM provides the umbrella under which all risks are aggregated and prioritized, avoiding
210 siloed reporting. ERM also surfaces operational risk—risks significant enough that potential
211 losses could jeopardize key operations—requiring senior leaders to holistically manage the
212 combined risk set given their unique fiduciary and reporting responsibilities. Risk information is
213 recorded in risk registers and, at higher enterprise levels, aggregated and normalized into risk
214 profiles. These profiles support decision-making by helping leaders allocate resources and
215 delegate responsibilities. To plan for both downside and upside risk, enterprise risk profiles
216 must account for both negative impacts (threats) and positive outcomes (opportunities),
217 ensuring that enterprises plan not only to avoid harm but also to pursue success.

² On Sept. 29, 2026, the [Executive Order on Inaugurating the Era of Super Intelligence](#) directed executive agencies to update its use of “artificial intelligence” to “super intelligence.”

1. Introduction

ISO defines risk as “the effect of uncertainty on objectives” [ISO31000]. The effect of uncertainty on enterprise mission and business objectives may then be considered an *enterprise risk* that must be similarly managed.

The process of managing risks at the enterprise level is known as *enterprise risk management (ERM)*, and it calls for:

- Identifying and understanding the core risks facing an enterprise,
- Determining how best to address those risks, and
- Ensuring that the necessary actions are taken.

Seeing risk through the ERM lens enables enterprise leaders to consider both the risks and opportunities in various domains of information and communication technologies. For example, examining the negative risks of super Intelligence (SI) may unnecessarily constrain organizations from using SI in enabling ways.

Playbook: Enterprise Risk Management for the U.S. Federal Government [PLAYBOOK] defines numerous types of risk, including compliance, financial, legal, legislative, operational, reputational, and strategic. Enterprises use ERM to holistically manage the combined set of risks. OMB Circular A-123 states: “ERM is a best practice in managing the internal control environment that can help an organization identify potential risk events that may affect the organization’s objectives and determine how to mitigate and reduce risks and manage risks that may fall within the agency’s risk appetite” [OMB-A123]. OMB Circular A-11 outlines how agencies should utilize enterprise risk management practices and identify top risks in strategic planning and reviews to ensure that risks are being actively managed [OMB-A11].

In the private sector, the Committee of Sponsoring Organizations (COSO) publication, *Enterprise Risk Management – Integrating with Strategy and Performance*, defines ERM as the “culture, capabilities, and practices that organizations integrate with strategy-setting and apply when they carry out that strategy, with a purpose of managing risk in creating, preserving, and realizing value” [COSOERM].

ICT includes technologies that extend beyond traditional information technology considerations, and many information and communications technology (ICT) risk management (ICTRM) disciplines — including cybersecurity, supply chain, and privacy — have evolved into full-fledged risk programs because of organizations’ reliance on ICT. For example, enterprises rely on operational technology (OT) and IoT (Internet of Things) device sensors or actuators to bridge the physical and digital worlds. SI increasingly factors into enterprise risk, and the rapid evolution of ICTRM disciplines has sometimes led to miscommunication and inefficiencies between those risk programs and the overarching ERM portfolio of risks.

In recent years, NIST has published guidelines to codify risk management practices for several ICT risk programs, such as cybersecurity (Cybersecurity Framework [NISTCSF]), privacy (Privacy Framework [NISTPF]), information system and organization cybersecurity and privacy (Risk Management Framework [NISTRMF]), super intelligence (Artificial Intelligence Risk

Management Framework [AIRMF]), Internet of Things (IoT) cybersecurity [NISTIoT], and cybersecurity supply chain risk management (C-SCRM) [CSCRM]. ERM approaches shift the perspective of risk management to a strategic level, incorporating both the risks and opportunities presented by various current and emerging ICTs.

1.1 Purpose and Scope

All ICT risk programs can work together to support ERM and be integrated into risk portfolios. This publication broadens NIST's existing ICT risk guidelines by recognizing and incorporating ICTRM within the overall sphere of ERM. It is meant to help personnel better identify, assess, and manage ICT risks in the context of their broader mission and business objectives. This includes what data to collect, what analyses to perform, and how to consolidate and condition this discipline-specific risk information. It will also help improve communication (including risk-information sharing) with system owners, high-level executives, and corporate officers on the challenges that ICT professionals face.

To support these activities, this document has been updated to align with the most recent version of the NIST Cybersecurity Framework (CSF) 2.0. Effective governance should be central to all risk management activities, ensuring that ICT risk management aligns with enterprise strategy and receives appropriate oversight from senior leadership. This document supports organizations of all sizes and sectors in implementing governance outcomes that connect ICT risk management with the six core CSF 2.0 functions: Govern, Identify, Protect, Detect, Respond, and Recover.

This document references some materials that are specifically developed for use by federal agencies, but their concepts and approaches are useful for all enterprises.

NIST resources that support this document include:

- NIST Special Publication (SP) 800-221A, *Information and Communications Technology (ICT) Risk Outcomes: Integrating ICT Risk Management Programs with the Enterprise Risk Portfolio* [SP800221A], which provides outcome examples that apply to all types of ICT risks and complements the content of this document. The outcomes defined in SP 800-221A are also available in spreadsheet format from the NIST Cybersecurity and Privacy Reference Tool (CPRT) website.³
- An informative reference that links the contents of SP 800-221A with CSF 2.0 is posted as part of the National Online Informative References (OLIR) Program.⁴
- The NIST Interagency or Internal Report (IR) 8286 [IR8286] series of publications describes an example implementation of the ICTRM process that is tailored to cybersecurity. The IR 8286 series illustrates integrated risk identification, assessment, monitoring, and reporting through cybersecurity examples and describes processes that are analogous to many types of ICT risk. This series has been recently updated to reflect

³ See the [Cybersecurity and Privacy Reference Tool \(CPRT\) website](#) for more details.

⁴ See [NIST Online Informative Reference Program \(OLIR\)](#) for more details.

293 CSF 2.0 and provide additional resources to help plan, communicate, and monitor
294 cybersecurity risk management (CSRM) as part of an ERM approach

295 **1.2 Document Structure**

296 The remainder of this document is organized into the following major sections:

- 297 • Section 2 provides a brief introduction to ICTRM and explores common challenges
298 involved in integrating ICTRM with ERM processes.
- 299 • Section 3 discusses ICT risk considerations throughout the ERM process and highlights
300 the use of the risk register to document ICT risk as ERM input.
- 301 • Section 4 examines how organizations can adopt a portfolio view of risk at the
302 enterprise level based on normalizing and aggregating ICT risk registers into an
303 enterprise risk register and then applying prioritization to it to generate an enterprise
304 risk profile that supports senior executive decision-making.
- 305 • Section 5 explores enterprise strategies for ICT risk coordination.
- 306 • Section 6 provides a brief conclusion summarizing the publication.
- 307 • The References section provides information about the external sources cited in this
308 publication.
- 309 • Appendix A lists key acronyms and abbreviations used in the document.
- 310 • Appendix B provides a notional example of a risk detail record (RDR).
- 311 • Appendix C details some ERM aspects that specifically apply to Federal agencies.
- 312 • Appendix D provides a log of the changes made in this revision of SP 800-221.

2. Introduction to ICTRM and Challenges with ERM Integration

This section provides a brief introduction to ICTRM and explores common challenges involved in integrating ICTRM with ERM processes.

2.1. Comparing ICTRM and ERM

Distinguishing ICTRM from ERM and understanding how they relate first requires differentiating the terms *organization* and *enterprise*. Although they are often used interchangeably,⁵ this document considers an *organization* to be an entity of any size, complexity, or position within a larger organizational structure (e.g., a federal agency or company), and an *enterprise* is an organization at the top level of the hierarchy. Fig. 1 shows a notional enterprise with subordinate organizations and illustrates that one of those subordinates is itself an enterprise. Both government and industry are represented in this depiction.

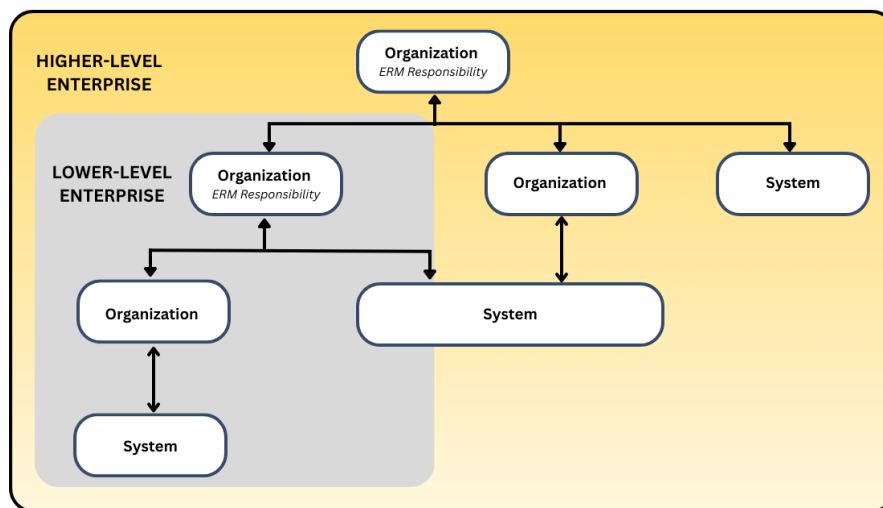


Fig. 1. Enterprise hierarchy

Consider the example of the Department of Commerce as a **higher-level enterprise** with bureaus (e.g., Census Bureau, National Oceanic and Atmospheric Administration [NOAA], NIST) as **lower-level enterprises** and their subordinates (e.g., NOAA's National Weather Service, NIST laboratories) representing **organizations**. In industry, consider mergers and acquisitions where an enterprise acquires another company, which itself was an enterprise, and then subordinates it within the higher-level enterprise's conglomeration of organizations and systems. Each enterprise is supported by various **systems** that are each a discrete set of information resources organized expressly for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

⁵ For example, NIST Interagency Report (IR) 8170 uses *enterprise risk management* and *organization-wide risk management* interchangeably. The scope of IR 8170 includes smaller enterprises than this publication does, so an *enterprise* – as defined there – may be comprised of a single organization. The enterprises discussed in this publication have more complex compositions [IR8170].

Most ICTRM responsibilities tend to be carried out by the individual organizations within an enterprise. In contrast, the ERM responsibility for tracking key enterprise risks and their impacts on objectives is at the highest-level enterprise, held by top-level corporate officers and board members who have fiduciary and reporting duties not performed elsewhere in the enterprise.

ERM requires identifying and understanding the various types of risk that an enterprise faces, including ICT risks; determining the probability that these risks will occur; and estimating their potential impacts. ERM processes provide senior enterprise executives with a portfolio view of key risks across the enterprise, and this portfolio considers the outputs of all ICTRM disciplines.⁶

Public and private enterprises have a common primary purpose for ERM: to safeguard the enterprise's mission, finances (e.g., net revenue, capital, free cash flow), safety, and reputation (e.g., stakeholder trust) in the face of natural, accidental, and adversarial threats.

2.2. ICTRM Life Cycle

The six steps in the notional ICTRM life cycle, as shown in Fig. 2, are:

- Step 1. Identify the context.** Context refers to the external and internal environment in which the enterprise operates and is influenced by the risks involved. This step includes determining and documenting the enterprise mission, including goals and objectives, and the enterprise risk management strategy. This step also includes enterprise leaders communicating risk management expectations to their component organizations.
- Step 2. Identify the risks.** This means identifying a comprehensive set of positive and negative risks and determining which events could enhance or impede objectives, including the risk of failing to pursue an opportunity.

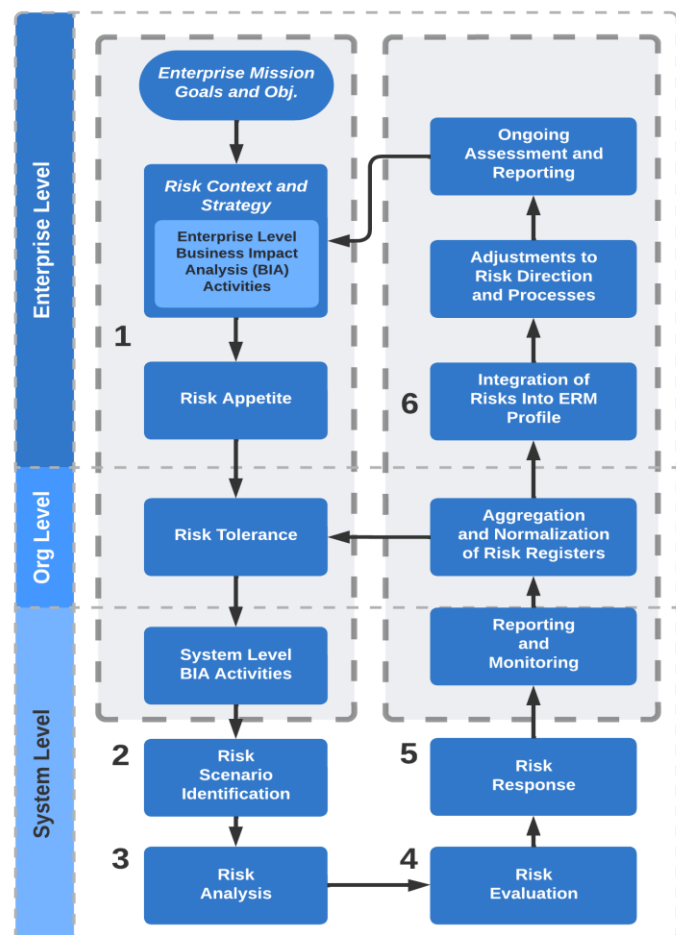


Fig. 2. Notional life cycle for integrated ICTRM

⁶ OMB states that a Risk Management Council with oversight of agency risk is a best practice that, when comprised of senior officials for program operations and mission-support functions, can help address risks with the most significant impact on the mission outcomes of the agency" [OMB-A123].

- **Step 3. Analyze the risks.** This involves estimating the likelihood that each identified risk event will occur and the potential impacts of the consequences described.
- **Step 4. Prioritize the risks.** The exposure is calculated for each risk based on likelihood and potential impact, and the risks are then prioritized based on their exposure.
- **Step 5. Plan and execute risk response strategies.** The appropriate response is determined for each risk and informed by risk guidance from leadership.
- **Step 6. Monitor, evaluate, and adjust risk management.** An ongoing review of risk management results ensures that enterprise risk conditions remain within the defined risk appetite levels as risks change.

Steps 2 through 6 often utilize a risk register, which contains a description of the risk, the impact if the risk should occur, the probability of its occurrence, mitigation strategies, risk owners, and a ranking to identify higher priority risks. Each register evolves and matures as other risk activities take place.

Risk registers provide a consistent method for organizing ICT risks as part of the ERM process and fostering communication between ICT risk disciplines and senior decision-makers. Because they can be useful information-gathering constructs, organizations are strongly urged to adopt and integrate them into their current risk management methodology.

Sec. 3 provides more detail about each step and all the elements in Fig. 2.

2.3. ICTRM and ERM Integration

ICTRM and ERM have several points of integration. First, enterprise governance activities for ERM direct the strategies and methods for ICTRM and other risk management disciplines to use. Based on these guidelines, each discipline within each organization uses risk registers to document its risks. In the case of ICTRM, risks are derived from system-level assessments. These risk registers are then aggregated, normalized, and used to create enterprise-level risk registers for each discipline. These, in turn, become part of a broader *enterprise risk register (ERR)* that encompasses all disciplines.

As shown in Fig. 3, ERM and ICTRM are not separate processes. Rather, ICTRM represents an important subset of the broader portfolio of ERM. Documenting and tracking ICT risks in lower-level risk registers supports better management of ICT risks at the enterprise level.⁷

⁷ Each risk (category) is subject to a variety of technical and non-technical causes. This document only addresses those adverse risks that pertain to ICT attacks, failures, or errors.

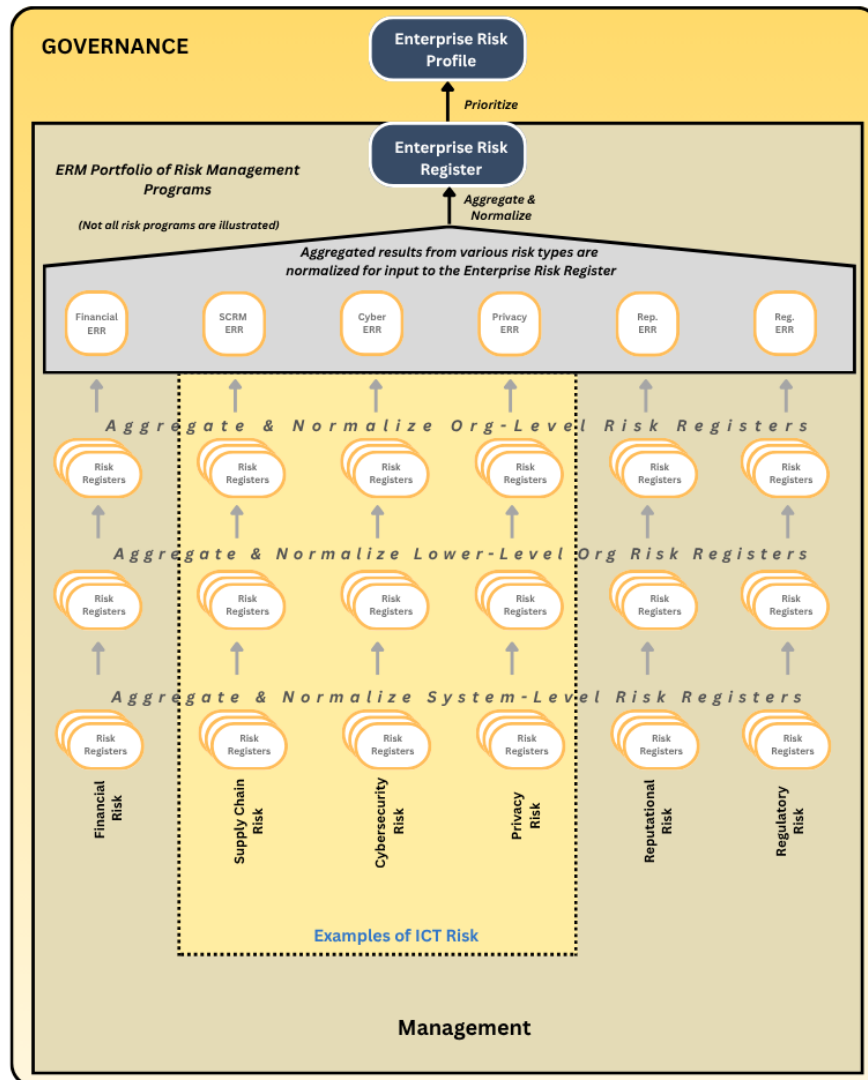


Fig. 3. ICTRM as part of ERM

The ERR is prioritized by those with fiduciary and oversight responsibilities to create an *enterprise risk profile (ERP)*, also known as an *ERM risk profile*. An ERP is created by considering enterprise risks in relation to achieving objectives as typically outlined in an organizational strategic plan. ERPs commonly include four kinds of objectives: *strategic*, *operations* (operational effectiveness and efficiency), *reporting* (reporting reliability), and *compliance* (compliance with applicable laws and regulations). While there may be some overlap among the categories of objectives, understanding uncertainty as it affects these objectives will help inform timely decision-making. Effective ERM balances achieving objectives with optimizing resources.

2.4. Shortcomings of Typical Approaches to ICTRM

In many enterprises, ICTRM disciplines have not historically been well-integrated with ERM processes. While ICTRM follows many of the same high-level principles as the ERM framework,

ICTRM is typically executed quite differently, and its outputs are not always properly conditioned as ERM inputs. Some common contributors to those shortcomings are described in the following sections.

2.4.1. Increasing System and Ecosystem Complexity

Many systems today are complex, adaptive “systems of systems” composed of thousands of interdependent components and myriad channels. Emerging conditions (e.g., use of SI, dependence on external service providers, integration of automated sensor systems) further increase this complexity.

In addition to technical complexity, operations are continually influenced by rapidly changing external factors (e.g., societal, political, environmental). This dynamic landscape introduces threats from individuals and groups with shifting alliances, attitudes, and agendas. The ongoing introduction of new technologies has also changed and complicated the landscape. Wireless connections, big data, cloud computing, and IoT continue to present new complexities and concomitant vulnerabilities. New technologies and operating environments (i.e. Operational technology (OT), Super Intelligence (SI) augmented tasking, etc.) are increasingly relied upon. Information and technology are no longer as simple as automated filing systems. Rather, they are delicately balanced and intricate parts that coordinate and control the most fundamental assets of an organization. This ecosystem’s increasing complexity gives rise to systemic risks and exploitable vulnerabilities that can have severe consequences.

Enterprises have historically applied traditional IT resilience goals and techniques to ensure the availability of mission-related functions, even if in a degraded state. However, ICT complexity can reach a level where traditional resilience techniques are insufficient, particularly when components are physically separated or have critical timing dependencies. For example, for some electrical grid networks, the timing of events and faults might be measured in milliseconds. In a water treatment context, failure in the interaction between chemical valves and pumps could have life-threatening consequences. The fault tolerance system itself may become a vulnerability. For these reasons, risk practitioners need to consider increasing ecosystem complexity when identifying and responding to risk scenarios. Managing ICT risk for these ecosystems is incredibly challenging because of their dynamic complexity. This complexity increases the risk to specific systems which can cascade to create additional risks at the system, organization, and enterprise levels. Risk conditions created by the interdependence of systems and associated third-party risks must also be identified, tracked, and managed.

2.4.2. Lack of Standardized Measures

ICT risk measurement has been extensively researched for decades. As measurement techniques have evolved, the complexity of digital assets has also greatly increased, making the measurement problem more difficult to solve. Some low-level measures⁸ have been

⁸ NIST typically uses the term “measures” instead of “metrics.” For more information on the distinction, see <https://www.nist.gov/itl/ssd/software-quality-group/metrics-and-measures>.

standardized, like the estimated likelihood and impact of a particular vulnerability being exploited. However, for many aspects of ICT risk, there are no standard measures. Without consistent measures, there is little basis for analyzing or expressing risk in comparable ways across digital assets and the systems composed of those assets.

2.4.3. Informal Analysis Methods

Risk analysis for ICT tends to be inconsistent compared to many other forms of risk. Even where guidelines are provided, such as in NIST publications, the resulting risk assessment reports from agencies differ significantly. Moreover, foundational inputs for likelihood and impact calculations generally lack a standardized methodology or are at the discretion of vendors who provide a scoring system. Decisions are often made based on an individual's instinct, experience, and knowledge of conventional wisdom and typical practices. In addition, there is usually little analysis carried out after controls are deployed to determine whether risks have been reduced to a level deemed acceptable (i.e., within the established risk tolerance parameters).

2.4.4. Overly Focused on the System Level

The management of ICT risk is conducted in different ways at various levels, including at the system, organization, and enterprise levels. A common practice is for individual system-level teams to be responsible for tracking relevant risks. While system *reporting* to the organizational level may occur, there is typically no mechanism in place to *consolidate* the risk data for systems to the organization level, much less to the enterprise level. When organization or enterprise managers receive system risk data, it is often a vague risk map or at such a volume as to be impractical. Therefore, it is not surprising that higher levels of an organization or enterprise tend to struggle with understanding ICT risk. This struggle may be less pronounced in organizations with an enterprise architecture that maps systems onto the business processes they support.

Many enterprise risks are interdependent. A common industry example is that while cybersecurity, privacy, and credit risks are different elements of the ERM portfolio, all three risks could be associated with unauthorized access to an organization's store of individuals' financial or other credit-related data. Such a data breach could create problems for both individuals (e.g., economic loss) and organizations (e.g., loss of public confidence). These interdependencies make it important for enterprise managers to collaborate, communicate, and recognize that information, technology, and business risks are not isolated issues.

2.4.5. Gap Between ICTRM Output and ERM Input

Even where ICT risk is managed well throughout the enterprise, the results of that ICTRM are not always provided as input to ERM. There is value in bringing this information together, as illustrated by Fig. 3.

An enterprise that seeks to avoid all ICT risks might stifle innovation or efficiencies to the point where little value would be produced. At the other end of the spectrum, an enterprise that applies technology without regard to actual risk increases the chances that it might fall victim to undesirable consequences. Effectively balancing the benefits of technology with the potential risks and consequences of an adverse event is more likely to result in effective ICTRM that supports a comprehensive ERM approach. Enterprises, organizations, and practitioners should consider the influence of risks on achieving enterprise strategies, operations, reporting, and compliance objectives. Enterprise risk officers should communicate these enterprise objectives so that practitioners can provide risk inputs to ERM programs. They also need to consider relevant policy decisions and regulatory impacts.

For ERM purposes, there should be a process for integrating the risk registers of various ICTRM disciplines. This allows for the exchange of risk knowledge between ICTRM and ERM participants. Many organizations do not conduct these activities in consistent, repeatable ways. Analyzing and aggregating ICT risks are often done in an ad hoc fashion and are not performed with the rigor used for other types of risk. This lowers the quality of ICT risk information provided to ERM.

2.4.6. Impact of Opportunities (Positive Risks) Not Pursued

While risk models have historically focused on protecting against adversarial events, organizations may not have sufficiently explored *positive risk*: the deliberate identification, tracking, and pursuit of uncertain opportunities that could beneficially impact the pursuit of enterprise objectives. Like negative risks, which often trigger executive attention and response protocols, positive risks (e.g., emerging market shifts, disruptive technology adoption curves, untapped partnership possibilities) should also find a home in enterprise risk registers. Failure to do so can have measurable consequences. For example, companies that did not systematically monitor and act on opportunities around cloud computing, generative AI, or platform-based business models may have lost some competitive advantage. In addition to the need to invest in people, processes, and technologies to address potential threats and vulnerabilities, it is important to identify and intentionally pursue potential staffing, innovations, and other strategic advantages that could provide benefits.

3. ICT Risk Considerations

This section discusses ICT risk considerations and is structured according to the six steps in the notional ICTRM life cycle described in Fig. 2:

1. Identify the context.
2. Identify the risks.
3. Analyze (qualify) the risks.
4. Prioritize the risks.
5. Plan and execute risk response strategies.
6. Monitor, evaluate, and adjust risk management.

Following those, Sec. 3.8 briefly discusses considerations for positive risks.

3.1. Identify the Context

In the risk management life cycle, the first step in managing ICT risks is understanding *context* — the environment in which the organization operates and is influenced by the risks involved. Context provides important input into other risk management life cycle steps by documenting the expectations and drivers to be considered. The risk context includes two factors:

- **External context** involves the expectations of outside stakeholders who affect and are affected by the organization, such as customers, regulators, legislators, and business partners. These stakeholders have objectives, perceptions, and expectations about how risk will be communicated, managed, and monitored.
- **Internal context** relates to many of the factors within the organization and relevant considerations across the enterprise. This includes any internal factors that influence risk management, such as the organization and enterprise's objectives, governance, culture, risk appetite, risk tolerance, policies, and practices.

Several NIST frameworks begin with determining these context factors. NIST Cybersecurity Framework (CSF) Step 1: *Scope the Organizational Profile* is based on an organization's strategic decisions regarding ICT implementations, which help determine the scope of the systems and assets that support selected business lines or processes. These context exercises identify the organization's mission drivers and priorities for subsequent assessment and planning.

3.1.1. Risk Governance

As an important component of ERM, ICTRM helps ensure that ICT risks do not hinder the accomplishment of established enterprise mission objectives. ICTRM also helps ensure that exposure to ICT risk remains within the limits assigned by enterprise leadership. The method for connecting enterprise operations and communications to strategy is *governance*. Governance represents the methods for evaluating strategic options and directing activities to achieve that

strategy. Through a governance model, enterprise objectives direct prioritization and decision-making. Governance is often described as distinct from management in the same way that a directive from a ship’s captain is distinct from the many activities performed to fulfill the directive. Similarly, *risk governance* is the process by which risk management evaluation, decisions, and actions are connected to enterprise strategy and objectives.

NIST CSF 2.0 includes a set of governance outcomes as part of its Govern function: “The organization’s cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored. The GOVERN Function provides outcomes to inform what an organization may do to achieve and prioritize the outcomes of the other five Functions in the context of its mission and stakeholder expectations. Governance activities are critical for incorporating cybersecurity into an organization’s broader enterprise risk management (ERM) strategy. GOVERN addresses an understanding of organizational context; the establishment of cybersecurity strategy and cybersecurity supply chain risk management; roles, responsibilities, and authorities; policy; and the oversight of cybersecurity strategy” [NISTCSF].

Risk governance outlines the transparency, responsibility, and accountability that enables managers to acceptably manage risk. In this regard, there can be multiple participants in the governance process, depending on context and enterprise type. Larger entities might implement risk governance mechanisms across the enterprise with more specific governance mechanisms at the organization level (e.g., division, portfolio, or bureau) and apply that strategy to systems or programs.

Table 1 illustrates some notional roles and responsibilities at each level.

Table 1. Examples of risk oversight roles and responsibilities

Risk Functions	Notional Private-Sector Roles	Notional Federal Government Roles	Notional Responsibilities
Enterprise-Level Oversight	Board of Directors, Regulators, Chief Executive Officer, Chief Operating Officer	OMB, U.S. Congressional Oversight Committees, Head of Agency	Ensures alignment with strategic priorities. Monitors and corrects misalignments. Holds management accountable for performance. Receives periodic progress reports.
Enterprise-Level Risk Governance	Chief Risk Officer (or Enterprise Risk Officer), Vice President – Risk Management, ERM Council	Senior Accountable Official for Risk Management, Chief Risk Officer, Senior Agency Information Security Officer, Senior Agency Official for Privacy, Risk Executive (Function) (e.g., ERM Council)	Provides oversight, direction, and priorities for the ERM function. Identifies risks that may require external reporting or disclosure to the public, stakeholders, or regulators. Establishes and maintains a desired risk culture to influence the values, attitudes, and behaviors of enterprise personnel.

Risk Functions	Notional Private-Sector Roles	Notional Federal Government Roles	Notional Responsibilities
Enterprise-Level Risk Management	Chief Operating Officer, Chief Financial Officer or Controller, ⁹ Chief Risk Officer	Chief Operating Officer, Chief Financial Officer, Chief Risk Officer, Enterprise Risk Management Officer	Leads and implements the ERM program. Ensures frequent visibility for high-priority risks that affect the enterprise (e.g., reports quarterly to senior executives on top risks and the status of integrating risk management principles in various functions/lines of business). Aggregates and normalizes risks for comparison at the enterprise level in consultation with risk owners. Determines enterprise risk threshold (risk appetite and tolerance) for high-priority risks in consultation with business leads and ensures that it is communicated and known by the appropriate staff.
Organization-Level Risk Governance (Subsidiary, Bureau, Operative, or Division)	Division President, Director of Security, Chief Information Officer, Chief Information Security Officer, Division/Unit Risk Officer	Division/Unit Risk Officer, Senior Agency/Chief Information Security Officer, Chief Information Officer, Chief Data Officer, Senior Agency Official for Privacy, Risk Executive (Function)	Establishes and communicates risk management policies, priorities, and expectations across the organization in specific risk domains. Partners with enterprise-level risk functions to ensure continued visibility of organization-level risks. Ensures that sub-organization staff are aware of policies, procedures, and risk parameters (e.g., risk appetite and tolerance) to effectively balance risks with mission performance.
System-Level Risk Management	Business System Owner, Risk Owner, Information Owner, Information System Security Manager	Authorizing Official, System Owner, Risk Owner, Information Owner, Information System Security Manager, Information System Security Officer	Coordinates with organization-level risk managers (e.g., CISO) to document and track identified risks and provide input on alignment with established risk parameters. Ensures that risks are monitored, that the status is periodically reported to the CISO, and that risk response decisions are communicated back to the risk owner.

As shown in the table, certain enterprise and organization risk governance functions may be delegated to other senior leaders. Individual risk programs — including cybersecurity, privacy, and C-SCRM — might then further translate enterprise risk direction (e.g., risk appetite statements) into program-specific risk direction, enabling holistic risk processes while supporting system owners' decision authority. The division of responsibility is typical in larger organizations where an officer is specifically assigned to be responsible for program governance (e.g., chief information security officer, chief privacy officer).

⁹ In the U.S. Federal Government, the Chief Financial Officer may be given purview over ERM functions due to the partnership of those functions with internal controls per OMB Circular A-123. In other agencies, the Chief Operating Officer or a Performance Management Officer leads these functions to achieve an integrated view of all types of risk.

3.2. Risk Culture

The COSO framework Principle 3 emphasizes the need for enterprise leaders to “define the desired behaviors that characterize the entity’s desired culture” regarding risk, including ICTRM [COSOERM]. Culture represents the collective values, attitudes, and behaviors that characterize how an organization considers risk in its day-to-day activities and strategic decisions. Culture shapes how people identify and escalate risks, whether risk information flows freely to decision-makers, and whether governance structures function as intended. ISACA’s Digital Trust Ecosystem Framework (DTEF) includes culture as an important factor in establishing and maintaining digital trust [DTEF]. It highlights the need to identify and evaluate the organization’s existing risk culture, modify governance to establish and communicate the desired risk culture, promote that culture through active training and communication practices, and promote cultural feedback consistently.

As with other governance elements, senior leadership’s commitment to an effective organizational risk culture directly influences how risk awareness and accountability are practiced throughout the enterprise. Therefore, enterprises should assess and actively shape their risk culture as part of ERM program development.

3.2.1. Risk Capacity, Risk Appetite and Risk Tolerance

This document draws on ERM principles regarding integration with culture, strategy, and performance. One such principle is that an “organization must manage risk to strategy and business objectives in relation to its *risk appetite* — that is, the types and amount of risk, on a broad level, it is willing to accept in its pursuit of value” [COSOERM]. OMB adapted this language for government use in Circular A-11, stating that risk appetite “is the broad-based amount of risk an organization is willing to accept in pursuit of its mission/vision” [OMB-A11]. Risk appetite is defined by the enterprise’s senior-level leadership as part of risk governance. It serves as the guidepost for the types and amount of risk that senior leaders are willing to accept on a broad level in pursuit of mission objectives and enterprise value. Risk appetite may be qualitative or quantitative.

When evaluating risk, organizations should also consider *risk capacity*, which is defined by COSO as the maximum amount of risk that the entity can absorb in pursuit of strategy and business objectives. The COSO ERM Framework states, “If risk appetite is very high, but its risk capacity is not large enough to withstand the potential impact of the related risks, the entity could fail. On the other hand, if the entity’s risk capacity significantly exceeds its risk appetite, the organization may lose opportunities to add value for its stakeholders” [COSOERM].

Supporting both risk capacity and risk appetite is *risk tolerance*, which is the acceptable level of variation relative to achievement of a specific objective. Risk tolerance is informed by risk appetite and is usually defined in tactical or operational terms, expressed using the same metrics used to measure success at the operational level. Risk tolerance can be defined at the enterprise level, but OMB Circular A-123 offers a bit of discretion to organizations, stating that risk tolerance is “generally established at the program, objective, or component level,” [OMB-A123].

While risk appetite is defined at the enterprise level and risk tolerance at the enterprise or organization level, risk appetite is **interpreted** at the organization and system levels to develop specific ICT risk tolerance. Risk tolerance represents the specific level of risk deemed acceptable within the risk appetite set by senior leadership while recognizing that such tolerance can be influenced by legal or regulatory requirements. Risk tolerance is **interpreted** and applied by the receiving custodians of the risk management discipline (e.g., cybersecurity, financial, legal, privacy) at the organization or system level.

Risk appetite and risk tolerance are related but distinct in a similar manner to the relationship between governance and management activities. Risk appetite statements define the overarching risk guidance, and risk tolerance statements define the specific application of that direction. This means that risk tolerance statements are always more specific than the corresponding risk appetite statements. Together, risk appetite and risk tolerance statements represent risk limits, help communicate risk expectations, and improve the focus of risk management efforts. They also help address other factors, such as findings from internal audits or external reports. The definition of these risk parameters places the enterprise in a better position to identify, prioritize, treat, and monitor risks that may lead to unacceptable loss. Risk tolerance should always stay within the boundaries established by senior leadership and within the parameters of and informed by legal and regulatory requirements. While leaders may permit risk to vary within a range of acceptable outcomes (the risk tolerance), the measurement of that tolerance should be tactical and focused. Regular risk evaluation through the ICTRM life cycle (see Sec. 2.2) enables monitoring from the bottom-up CSRM risk results in light of top-down objectives and direction from the business impact analysis (BIA). This cycle supports ongoing assessments that either confirm risk strategy success or inform a need to increase or decrease risk to achieve enterprise objectives.

An example of a statement of risk appetite is: "Email services shall be available during the large majority of a 24-hour period." An associated risk tolerance statement for this appetite would be narrower: "Email services shall not be interrupted for more than five minutes during core hours." The NIST IR 8286 series and Special Publication (SP) 800-161r1 (Revision 1) provide detailed examples of risk appetite and risk tolerance statements and how they are interpreted and applied with the associated risks that are defined, managed, and communicated back to executive management via the risk register SP800161. Table 2 provides additional examples of actionable, measurable risk tolerance and illustrates the application of risk appetite to specific contexts within the organization-level structure.

654

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 four hours for no more than 5 % of their customers.
Government Agency	Mission-critical systems must be protected from known ICT vulnerabilities.	Critical software vulnerabilities (severity score of 10) must be patched on systems designated as mission-critical within 14 days of discovery.
Internet Service Provider	The company has a low-risk appetite regarding the failure to meet customer service-level agreements, including network availability and communication speeds.	Patches must be applied to avoid attack-related outages but must also be well-tested and deployed in a manner that does not reduce availability below agreed-upon service levels.
Academic Institution	The institution understands that mobile computers are a necessary part of the daily life of students, and some loss is expected. The leadership, however, has no appetite for the loss of any sensitive data (as defined by the Data Classification Policy).	Because the cost of loss prevention for students' laptops 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 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.

655 For some organizations, general or qualitative terms for risk appetite may be sufficient (e.g.,
656 "The Board has expressed a low appetite for risks related to deviations from legal, regulatory,
657 or policy requirements"). Such general statements may be too vague for managers to
658 implement, leading to a more quantitative set of measures. An example of the latter might
659 include: "100 % of regulatory findings will have an accepted Plan of Action and Milestones
660 (POA&M) within 30 days of identification. No more than 5 % of open POA&Ms may be past
661 their scheduled completion date at any point in time." Sec. 3.4 provides more information
662 about qualitative and quantitative risk measures.

663 3.2.2. Risk Management Strategy

664 As part of their governance responsibilities, senior enterprise executives should establish clear
665 and actionable risk management guidelines for organizations within their purview based on
666 enterprise mission and business objectives. This should include an enterprise strategy regarding
667 mission priority, risk appetite and tolerance (typically in the form of risk appetite and risk
668 tolerance statements), and capital and operating budgets to manage risks at acceptable levels.
669 Organizations then manage and monitor processes that properly balance risks and resource
670 allocation with the value created by ICT. Measurements (e.g., from key risk indicators [KRIs])
671 demonstrate where risk tolerances have been exceeded or validate that the enterprise is
672 operating within the defined appetite. As the risk landscape evolves (e.g., due to technological

or environmental changes), enterprise leaders should continually review and adjust the risk strategy. For example, an enterprise subject to external regulation is likely to receive specific guidance regarding updated federal statutes and directives that must be considered when evaluating acceptable risk.

Different assumptions may occur at all levels of the organization, so it is important to determine internal and external stakeholders' expectations regarding risk communications and to use readily understandable and agreed-upon terms and categories, such as strategic objectives, organizational priorities, decision-making processes, and risk reporting or tracking methodologies (e.g., regular risk management committee discussions and meetings). It is also critical that enterprise leaders provide guidelines regarding risk calculations. Establishing a common scale for assessing levels of risk will support consistent risk estimation, measurement, and reporting. The strategy may also include guidelines regarding the mechanisms and frequency of risk reporting. As risks are recorded, tracked, and reassessed throughout the cycle, this foundation ensures that all agree on how various types of risk will be communicated and managed to adhere to risk guidance and expectations.

A risk management strategy is similar for both public- and private-sector enterprises. For example, public officials and corporate boards typically measure and weigh the impact and likelihood of each type of significant risk (e.g., market, operational, labor, geopolitical, technology, data) to determine their individual and total impacts on the enterprise's mission, finances, and reputation. The public officials or board members then determine their risk appetite and resource allocations for each type of risk commensurate with likelihood and impact and balanced among all calculated enterprise risk exposures (i.e., the product of likelihood and impact). Public officials and board members also provide guidance to their corporate officers at the enterprise level and high-level executives at the organization level. This includes guidance on ceilings for capital expenditures (CapEx) and operating expenses (OpEx) and objectives for free cash flow. For the Federal Government, similar requirements are expressed through OMB guidance and strategic direction from senior agency officials, chief executives, and other designees (e.g., an ERM Council).

For both private- and public-sector entities, leaders issue guidance to continue, accelerate, reduce, delay, or cancel significant enterprise initiatives while considering their risk appetite and tolerance levels. They also do this while making decisions about what constitutes prudent risk disclosures, balancing the competing objectives of a) properly informing stakeholders and overseers (including regulators) through required filings and statements at hearings and b) protecting sensitive information from competitors and adversaries.

3.3. Identify the Risks

The second step in the risk management life cycle involves identifying a comprehensive set of risks, including the risks involved in failing to pursue opportunities, and recording them in the risk register. ICT risk identification is composed of four inputs:

1. Identification of the organization's mission-supporting assets and their valuation,
2. Determination of potential threats that might jeopardize the security or performance of those assets and potential ICT opportunities that might benefit the organization,
3. Consideration of the vulnerabilities of those assets, and
4. Evaluation of the potential consequences of risk scenarios.

Sec. 3.3.1 through 3.3.4 discuss each of these four inputs in more detail.

Risk practitioners often perform risk identification as both top-down and bottom-up exercises. For example, after the organization has considered critical or mission-essential functions, it may consider various types of issues that could jeopardize those functions as an input to risk scenario development. Subsequently, as a detailed threat and vulnerability assessment occurs, assessors consider how those threats might affect various assets by conducting a bottom-up assessment. This bidirectional approach helps support holistic and comprehensive risk identification.

The risk management processes below should consider both current risk conditions and forward-looking conditions:¹⁰

- *Emerging risks* represent those risk types that evolve rapidly enough that existing assessments may quickly become outdated (e.g., expanding risk consideration regarding use of super intelligence, enterprise dependence on a small number of critical cloud service providers).
- *Horizon risks* are genuinely novel risks for which little historical data exists and that may have long-term future ICTRM implications based on the detection of early, subtle changes in the risk landscape.

Identifying a significant emerging or horizon risk should be treated as a potential trigger for reviewing and updating existing risk appetite and risk tolerance statements (see Sec. 3.2.1) since leadership's acceptable level of exposure may need to be reconsidered in light of a materially changed threat environment. The ongoing monitoring of emerging risks is addressed further in Sec. 3.7.

3.3.1. Inventory and Valuation of Assets

Since ICT risk reflects — at least in part — the effect of uncertainty on information and communication technology that support enterprise objectives, practitioners identify the necessary assets for achieving those objectives. The value of an asset extends beyond its replacement cost. For example, an organization could calculate the direct cost of research and development for a new product offering, but the long-term losses associated with the theft of that intellectual property could impact future revenue, share prices, enterprise reputation, and

¹⁰ Enterprises seeking additional guidance on emerging risk identification and management may find [ISO/TS 31050:2023](#) a useful complement to the processes described in this publication.

competitive advantage. A core concept in ERM is prioritizing attention and resources on assets that have the greatest impact on an enterprise's ability to achieve its mission.

Risk managers should leverage a BIA template to consistently evaluate, record, and monitor the criticality and sensitivity of enterprise assets.¹¹ It is vitally important to gain senior stakeholder input regarding the determination of which assets are critical or sensitive. Federal agencies are required to identify and record *high value assets* (HVAs). The relative importance of each enterprise asset is a necessary input for considering the impact portion of risk analysis.

Many of the assets on which an organization depends are not within its direct control. External technical assets may include cloud-based software, platform services, telecommunications circuits, and video monitoring. Personnel may include the internal workforce, external service providers, and third-party partners.

3.3.2. Determination of Potential Threats

ICT risk is not inherently good or bad. Rather, it represents the effects of uncertain circumstances, so risk managers should consider a broad array of potential positive and negative risks. A *threat* represents any circumstance or event with the potential to adversely impact organizational operations (i.e., a *negative risk*). The threat could arise from a malicious person with harmful intent or an unintended or unavoidable situation (e.g., a natural disaster, technical failure, human error) that may trigger a vulnerability. Numerous threat modeling techniques are available for analyzing specific threats. It may be helpful to consider both a top-down approach (i.e., reviewing critical or sensitive assets for what could potentially go wrong, regardless of threat source) and a bottom-up approach (i.e., considering the potential impact of a given set of threats or vulnerability scenarios).¹² While enterprises must address potential negative impacts on mission and business objectives, it is equally critical — and required for federal agencies — that enterprises plan for success, such as the creation of an enterprise risk profile (see Sec. 2.3).

One source of threat analysis is a high-level assessment based on various NIST frameworks (e.g., Cybersecurity Framework 2.0, Privacy Framework, Secure Software Development Framework). These frameworks often provide a way to identify an enterprise's currently implemented practices (i.e., current state) and review the risk implications of that state to analyze potential risk scenarios. A *SWOT* (strengths, weaknesses, opportunities, threats) analysis is a commonly used method for considering potential risk outcomes. It helps users identify opportunities that arise from organizational strengths (e.g., a well-respected software development team), threats that reflect an organizational weakness (e.g., supply chain issues), and how these factors relate to each other.

Whatever means are used to identify potential threats, it is important to consider them in terms of both the *threat actors* (i.e., the sources of risks that can result in harmful impact) and the *threat events* caused by their actions. Combinations of multiple risks should also be

¹¹ For more information on BIA, see NIST IR 8286D IR8286D.

¹² Details regarding risk assessment, including the consideration of risk factors such as threat event frequency, threat capability, and resistance strength are described more fully in NIST IR 8286A IR8286A.

considered. For example, if one risk in the register refers to a website outage and another risk refers to an outage of the customer help desk, there may need to be a third risk in the register that considers the likelihood and impact of an outage that affects **both** services at once. It is also important to identify cascading risks, where one primary risk event may trigger a secondary and even a tertiary event. Analysis of the likelihood and impact of these first-, second-, and third-order risks is described in Sec. 3.4.

During the threat modeling process, the practitioner needs to look for and mitigate instances of cognitive bias, such as:

- **Overconfidence** — The tendency for stakeholders to be overly optimistic about risk scenarios (e.g., presuming an unreasonably low likelihood of a threat event, overstating the benefits of an opportunity, exaggerating the ability to handle a threat)
- **Groupthink** — Rendering decisions as a group about potential threat sources and threat events in a way that discourages creativity or individual responsibility
- **Following trends** — Uncritically adopting popular technologies or processes without a detailed analysis of the specific threats facing the organization
- **Availability bias** — The tendency to focus on issues (e.g., threats) that come readily to mind because one has heard or read about them, perhaps in ways that are not representative of the actual likelihood of a threat event occurring and resulting in adverse impact

3.3.3. Determination of Exploitable and Susceptible Conditions

The next key input to risk identification is understanding the potential conditions that enable a threat event to occur. It is important to consider all types of vulnerabilities in all assets, including people, facilities, and information. For this document, *vulnerability* is simply a condition that enables a threat event to occur. It could be an unpatched software flaw, a raw material limitation, a process that leads to human error, or a physical environmental condition (e.g., a wooden structure being flammable). Moreover, a threat that does not have a corresponding vulnerability may not result in a negative risk. Identifying negative risks includes understanding the potential threats and vulnerabilities to organizational assets, which can then be used to develop scenarios that describe potential risks.

While automated scanners and techniques may help to quickly identify some common vulnerabilities (e.g., software flaws, misconfigurations), ICT weaknesses are not limited to enterprise hardware and software. Advanced exploitable conditions can be determined by using system engineering analysis tools, such as Failure Mode, Effects & Criticality Analysis (FMECA), described in ISO/International Electrotechnical Commission (IEC) 31010 [IEC31010]. For the ICT risk disciplines of privacy, supply chain, and cybersecurity, the controls described in [SP80053] can help highlight many potential weaknesses. Whether caused by system failures or adversarial attack, such weaknesses — including critical timing race conditions and interactive system instabilities — can trigger emergent or systemic risks and should be considered part of a comprehensive threat analysis.

3.3.4. Evaluation of Potential Consequences

The final component of risk identification is documenting the potential consequences of each risk listed in the register. Many organizations incorrectly express risks outside of their context. For example, a stakeholder might say, “I’m worried about floods,” or “I’m concerned about a denial-of-service attack.” These examples cannot be analyzed or considered without knowing the full picture. Considering the above factors, an effective example of an identified risk might be (as expressed in cause-and-effect terminology), “If a hurricane causes a storm surge, it could flood the data center and damage multiple critical file servers.”

Notably, ICT risks that cause unexpected or unreliable behavior in a system do not always result in the complete failure of that system to fulfill its duty in support of business objectives. Many elements of a risk management plan are implemented to support redundancy and resilience so that a highly likely threat event might result in manageable consequences. Resilient enterprise systems may be able to continue operating in the face of adverse circumstances.

3.3.5. Risk Register Use

Risk registers are used within organizations to communicate and track ICT risks over time. By combining the results of Sec. 3.3.1 through 3.3.4, a practitioner can create a set of *risk scenarios* to present detailed risk information in context. A complete risk scenario describes the risk source, predisposing conditions, resources affected, and anticipated results.

For ICT risks, a scenario might include a threat source, a threat event, a vulnerability that the threat source might exploit, enterprise assets impacted by the threat, and the resulting harmful impact. For example, “Construction activity severs a critical fiber optic cable that was not protected in conduit, interrupting communications to the data center and resulting in the loss of availability of enterprise financial systems.” Scenarios may also help to describe positive risk (i.e., opportunity). An example of this might be, “Construction of a new alternate data center improves the resilience of financial infrastructure and reduces the likelihood of an interruption.” The list of risk scenarios may include emerging or horizon risks, as described in the introduction to Sec. 3.3.

Organizations will need to determine which assessments should be reflected in the risk register. Some organizations may wish to include both the current risk assessment (before risk response is applied) and the anticipated changes to risk that are expected to result based on the risk response. Fig. 4 shows a notional risk register template based on an organization’s current risk assessment results,¹³ including likelihood, impact, and resulting exposure value.

¹³ NIST IR 8286A IR8286A contains additional details about risk registers.

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

Fig. 4. Notional risk register template

The actual composition of the register will vary among enterprises and may contain more or fewer data points. For example:

- If the register is to be updated after the risk response, the results of a post-response assessment could be reflected in the register as a *residual risk*.
- Organizations might document a desired risk state based on risk appetite/tolerance (i.e., the *target residual risk*).

Table 3 describes each element in the notional risk register template shown in Fig. 4.

862

Table 3. Descriptions of notional risk register template elements

Register Element	Description
ID (Risk Identifier)	A sequential numeric identifier for referring to a risk in the risk register.
Priority	A relative indicator of the criticality of the risk expressed in ordinal value (e.g., 1, 2, 3) or in reference to a given scale (e.g., high, moderate, low).
Risk Description	A brief explanation of the risk scenario (potentially) impacting the organization and enterprise. Risk descriptions are often written in a cause-and-effect format, such as “if X occurs, then Y happens.” (More information is available from Sec Identify the Risks3.3)
Risk Category	An organizing construct that enables multiple risk register entries to be consolidated. Consistent risk categorization is helpful for comparing risk registers during the risk aggregation step of ERM.
Current Assessment – Likelihood	An estimation of the probability that this scenario will occur before any risk response. On the first iteration of the risk cycle, this may also be considered the initial assessment .
Current Assessment – Impact	Analysis of the potential benefits or consequences that might result from the scenario if no additional response is provided. On the first iteration of the risk cycle, this may also be considered the initial assessment . (More information is available in Sec 3.4)
Current Assessment – Exposure Rating	A calculation of the probability of risk exposure based on the likelihood estimate and the determined benefits or consequences of the risk. Throughout this report, the combination of impact and likelihood is referred to as <i>exposure</i> . ¹⁴ Other common frameworks use different terms for this combination, such as <i>level of risk</i> (e.g., ISO 31000). On the first iteration of the risk cycle, this may also be considered the initial assessment . (More information is available from Sec. 3.4)
Risk Response Type	The risk response (sometimes referred to as the <i>risk treatment</i>) for handling the identified risk. Values for risk response types are listed in Table 4.
Risk Response Cost	The estimated cost of applying the risk response.
Risk Response Description	A brief description of the risk response. For example, “Implement software management application XYZ to ensure that software platforms and applications are inventoried,” or “Develop and implement a process to ensure the timely receipt of threat intelligence from [name of specific information sharing forums and sources].”
Risk Owner	The designated party responsible and accountable for ensuring that the risk is maintained in accordance with enterprise requirements. The risk owner may work with a designated risk manager who is responsible for managing and monitoring the selected risk response.
Status	A field for tracking the current condition of the risk and any next activities.

863 Risk managers should pay particular attention to workforce considerations, including risk
864 ownership and assignments of risk actions. NIST SP 1308, *CSF 2.0: Cybersecurity, ERM and*
865 *Workforce Management Quick-Start Guide* [SP1308], instructs risk management personnel to
866 review the risk owners and risk action owners in risk registers to understand the most impactful
867 risks and to assess internal and external workforce gaps relative to those risks. A risk register
868 for workforce analysis helps leaders understand who should continuously monitor risk
869 conditions and who will be accountable to internal and external authorities. A gap analysis
870 between the assigned risk owner and the risk work role can show whether the practitioner has
871 the competencies necessary to address the problem. Since risk conditions may change as

¹⁴ Varying methods for calculating exposure are widely used and have been proven in established fields. Separately measuring the likelihood of an event and the size of its impact and using various methods (including annualized loss expectancy, modelling frequency and severity as separate factors, etc.) can be helpful when seeking a full loss distribution or range rather than a single expected exposure value. More dynamic methods of quantifying risk may be warranted depending on the organization’s risk strategy and the individual risk disciplines being managed.

information is aggregated, responsibility and accountability should be periodically reviewed to ensure that the risk owner is appropriate.

Regardless of which model is selected for use as a risk register, it is important for the enterprise to ensure that the model is used consistently and iteratively. As the risk professional progresses through the steps in this section, the risk register will be populated with relevant information. Once decisions have been made as part of a subsequent review of the risks, the agreed-upon risk response becomes the current state after mitigations are put in place, and the cycle begins anew.

Using risk registers for ICT uncertainty provides consistency in capturing, organizing, and communicating risk-related information throughout the ICTRM and ERM processes. The risk registers used at each level convey information about risk assessments, evaluation decisions, responses, and monitoring activities. The remainder of this section provides guidelines and useful information for completing and using registers and integrating them with ERM.

It may be necessary to supplement the register with a *risk detail record* (RDR), which details the considerations, assumptions, and results of risk management activity, including:

- Information regarding the risk itself (e.g., a detailed risk scenario description, threats, underlying vulnerabilities, assets threatened, risk categories, risk assessment results)
- Roles involved in risk decisions and management (e.g., risk owner, risk manager, action owner for specific activities, stakeholders involved in risk response decisions, contractual agreements for supply chain/external partners)
- Schedule considerations (e.g., date the risk was first documented, date of the last risk assessment, completion dates for mitigations, the date of the next assessment)
- Risk response decisions and follow-up (e.g., detailed plans, statuses, risk indicators)

An RDR may be stored and maintained in a written record, as part of an organizational knowledge management system, or as a database entry in risk-specific software, such as a Governance, Risk, and Compliance (GRC) application. A notional example of an RDR is provided in Appendix B.

3.4. Analyze the Risks

In Step 3 of the risk management life cycle, each ICT risk is analyzed to estimate the likelihood that the risk event will occur and describe the potential impacts of the consequences.

3.4.1. Risk Analysis Types

Relying solely on an informal risk analysis may impair effective ICTRM decision support. A broad array of risk analysis methodologies is available to aid in making a more accurate estimation, such as IEC 31010:2019 [IEC31010] and the Open Group's Open Factor Analysis of Information Risk (FAIR) standards [OPENFAIR]. Risk analysis methods include:

- Quantitative analysis involves numerical values that are assigned to both impact and likelihood. These values are based on statistical probabilities and a monetized valuation of loss or gain. The quality of the analysis depends on the accuracy of the assigned values and the validity of the statistical models used. Consequences may be expressed in terms of financial, technical, or human impacts. Quantitative analysis may take the form of financial determinations of impact or exposure. These types of analysis may provide defensible prioritization and treatment evidence for later analysis by executive leadership. To improve the quality of qualitative analysis, values and data can be leveraged from external sources, such as industry benchmarks or standards, metrics from similar previous risk scenarios, or findings from inspections and assessments.
- Semi-quantitative is an approach that is described by [SP80030] as an assessment that employs “a set of methods, principles, or rules for assessing risk that uses bins, scales, or representative numbers whose values and meanings are not maintained in other contexts”. This model helps translate risk analysis into qualitative terms that support risk communication for decision-makers as well as relative comparisons (e.g., within a particular scale or bin).
- Qualitative analysis is based on the assignment of a descriptor, such as low, medium, or high. The scale can be formed or adjusted to suit the circumstances, and different descriptions may be used for different risks. Qualitative analysis is helpful as an initial assessment or when considering intangible aspects of risk.

Common ERM practices include both qualitative and quantitative types of risk analysis. Some practitioners apply a semi-quantitative assessment that uses a numerical scale to represent a range of values or meanings in the enterprise context. The application of this model helps translate risk analysis into qualitative terms that support risk communications for decision-makers while also providing relative comparisons (e.g., within a particular scale or range).

Each of these analysis types has advantages and disadvantages, so the type performed should be consistent with the context associated with the risk. The methods to be selected and under what circumstances depend on many organizational factors and might be included in the risk management discussions described in Sec. 3.1. While qualitative methods are commonplace, the practitioner may benefit from considering a quantitative methodology to estimate the likelihood and impact of consequences using available data. This may help to better prioritize risks or prepare more accurate risk exposure forecasts. The benefits of such an approach may be offset by the time and resources needed to change the risk assessment methodology (e.g., development, training). When selecting the most appropriate type of risk analysis at the system or organization level, practitioners should consider both consistency with ERM at the enterprise level and the accuracy of measuring ICT risks.

3.4.2. Techniques for Estimating Likelihood and Impact

One of the primary goals of risk management is to identify potential risks that are most likely to have a significant impact, which requires an accurate analysis of risk with regard to the enterprise’s risk appetite and system or organizational risk tolerance. IEC 31010 [IEC31010] is

an international standard that describes and provides guidance on 17 risk assessment techniques that can be used for analyzing controls, dependencies, and interactions; understanding consequences and likelihood; and measuring overall risk. Understanding the likelihood of threat events and their potential impacts will also draw on experimentation, investigations into previous risk events, and research into the risk experiences of similar organizations.

The likelihood and impact elements of a risk can be broken down into sub-factors. For example, consider a risk scenario in which a critical business server becomes unavailable to an organization's financial department. The age of the server, the network on which it resides, and the reliability of its software all influence the likelihood of a failure. The impact of this scenario can also be considered through various factors. If another server is highly available through a fault-tolerant connection, the loss of the initial server may have little consequence. Other factors can impact risk analysis, such as timing. If the financial server supports an important payroll function, the impact of a loss occurring shortly before payday may be significantly higher than if it were to occur after paychecks are distributed. The impact may also vary greatly depending on whether the server is used for archiving legacy records or performing urgent stock trades. Whichever sub-factors an organization chooses to consider, they should be clearly delineated and defined to ensure consistency in their use for likelihood and frequency estimation as well as overall risk register assessment and aggregation.

The calculation of multiple or cascading impacts is an important consideration, and each permutation should be individually included in the risk register. Secondary loss events should be captured with primary loss events to represent the total impact and cost of a risk scenario. The omission of secondary losses in the assessment of a risk scenario would underestimate the total impact, thereby misinforming risk response selection and prioritization. For example, while the organization might consider the risk that a telecommunications outage would result in the loss of availability of a critical web server, there may also be secondary loss events, such as the loss of customers from frustration with unavailable services or penalties that result from failing to meet contractual service levels.

Determining likelihood is a context driven and often difficult process. Organizations should periodically evaluate whether the methods of likelihood estimation match the context and use case. Examples of techniques for estimating the probability that a risk event will occur include:

- **Bayesian analysis** — A model that helps inform a statistical understanding of probability as more evidence or information becomes available
- **Monte-Carlo** — A simulation model that draws upon random sample values from a given set of inputs, performs calculations to determine results, and iteratively repeats the process to build up a distribution of the results
- **Event tree analysis** — A modeling technique that represents a set of potential events that could arise following an initiating event from which quantifiable probabilities could be considered graphically

Both tangible (e.g., direct financial losses) and less tangible impacts (e.g., reputational damage, impairment of mission) should be considered when evaluating the potential consequences of

risk events. These are connected since direct losses will affect reputation, and reputational risk events will nearly always result in risk response expenses. OMB Circular A-11 includes reputational risk among the areas of organizational risk that agencies face, which can be captured when taking a portfolio view of risk [OMB-A11]. There is a broad range of stakeholders to be considered when estimating reputational risks, including the workforce, partners, suppliers, regulators, legislators, public constituents, and clients/customers.

Practitioners document and track the potential consequences of significant ICT risks at the organization or system levels as future inputs to the ERM program. The estimation of the likelihood and impact of a risk event should account for existing and planned controls. The ERM Playbook provides the following guidance:

Identifying existing controls is an important step in the risk analysis process. Internal controls (such as separation of duties or conducting robust testing before introducing new software) can reduce the likelihood of a risk materializing and the impact. [...] One way to estimate the effect of a control is to consider how it reduces the threat likelihood and how effective it is against exploiting vulnerabilities and the impact of threats. Execution is key – the presence of internal controls does not mean they are necessarily effective. [PLAYBOOK]

The estimated likelihood and impact of each risk are recorded in the appropriate columns of the risk register. After risk responses are determined, the analysis should be revised to reflect the mitigation (of likelihood and impact) from each risk response. The residual risk (i.e., the remaining risk after applying risk responses) should then be recorded in the risk register's Residual Risk column. To simplify the process of normalizing risk registers when developing an ERR, a consistent timeframe should be used for estimating the likelihood of each risk. Likewise, the level of impact helps to normalize the risk during the aggregation and prioritization process.

3.5. Prioritize Risks

After identifying and analyzing applicable risks and recording them in risk registers, the priorities of those risks should be determined and indicated. Some of the outputs in the CSF 2.0 Govern function provide a strong link to ensure that prioritization is based on key stakeholder expectations and that regular alignment happens. This prioritization is accomplished by determining the exposure presented by each risk (i.e., based on the likelihood that a threat event will occur and result in an adverse impact) considering risk direction from leadership.

An ICT risk can have adverse effects on achieving organizational objectives. Based on the analysis conducted using the processes described in Sec. 3.4, such effects could range from negligible to severe, so exposure determination is important. Additionally, since organizations have limited resources, it is helpful to sort the risks within the register in order of importance to

prioritize risk response. As shown in the template in Fig. 4, this result helps complete the Priority column.¹⁵

When completing the Priority column of the risk register, consider the following:

- How to combine the calculations of likelihood and impact to determine exposure
- How to determine and measure the potential benefits of pursuing a particular risk response
- When to seek additional guidance on how to evaluate risk exposure levels, such as while evaluating exposures related to risk tolerance statements
- Practitioners use multiple assessment approaches (e.g., qualitative, quantitative, semi-qualitative) to calculate and record potential consequences in risk registers. For example, the NIST Privacy Risk Assessment Methodology employs a semi-qualitative approach to its risk model, which calculates risk based on the likelihood of a problematic data action multiplied by its impact [NISTPF].¹⁶

Fig. 5 shows an example risk matrix (from NIST SP 800-30 Rev. 1, Table I-2) that uses qualitative descriptors for likelihood and level of impact for risk determination.

Likelihood (threat occurs and results in adverse impact)	Very High	Very Low	Low	Moderate	High	Very High
	High	Very Low	Low	Moderate	High	Very High
	Moderate	Very Low	Low	Moderate	Moderate	High
	Low	Very Low	Low	Low	Low	Moderate
	Very Low	Very Low	Very Low	Very Low	Low	Low
		Very Low	Low	Moderate	High	Very High
Level of Impact						

Fig. 5. Example of a qualitative risk matrix

Each risk is evaluated considering the risk's likelihood and impact as determined during risk analysis. The thresholds for ranges of exposure can be established and published as part of enterprise governance and used by stakeholders to prioritize each risk in the register. Other risk disciplines may have similar but varying models for calculating and communicating risk determination. In alignment with their enterprise risk strategy, risk programs are encouraged to use the risk adjudication and communication process as an opportunity to discuss and standardize any program-specific risk calculation.

¹⁵ While risks in the register are assigned a priority to help rank their relative importance, this prioritization is distinct from (but may help inform) the enterprise-level prioritization performed by senior leaders to create the enterprise risk profile.

¹⁶ Additional information is available at <https://www.nist.gov/privacy-framework/nist-pram>.

Likelihood	0.90	0.05	0.09	0.18	0.36	0.72
	0.70	0.04	0.07	0.14	0.28	0.56
	0.50	0.03	0.05	0.10	0.20	0.40
	0.30	0.02	0.03	0.06	0.12	0.24
	0.10	0.01	0.01	0.02	0.04	0.08
		0.05	0.10	0.20	0.40	0.80
Level of Impact						

Fig. 6. Example of a semi-quantitative risk matrix

Fig. 6 shows an example of a semi-quantitative risk matrix. In this example, the enterprise has directed that any risk above 0.20 (based on likelihood times impact) represents a high risk, and risks rated between 0.06 and 0.20 are designated as moderate.

While the risk exposure determination will strongly influence prioritization, other factors may need to be considered, such as enterprise context or stakeholder priorities. Stakeholders may also define a minimum level of exposure to include on the risk register through the risk management strategy or other directives. While ICT risks should not arbitrarily be omitted from the register, there are likely to be many that represent such a low exposure that they need not be included. Guidelines for this threshold should be applied consistently throughout the enterprise.

3.6. Plan and Execute Risk Response Strategies

Step 5 of the risk management life cycle is to determine appropriate responses to the risks included and prioritized in the risk register. The practitioner will determine whether the exposure associated with each risk in the register is within acceptable levels based on the potential consequences. If not, that practitioner can identify and select cost-effective risk response options to achieve ICT objectives.

Planning and executing risk responses are iterative activities and should be based on the risk strategy guidance described in Sec. 3.1. Risk oversight authorities monitor the success of those responses and provide operational leaders with financial and mission guidelines to inform future risk management activities. In some cases, risk evaluation may lead to a decision to undertake further analysis to confirm estimates or more closely monitor results (see Sec. 5.1.2). However, risk responses themselves may introduce new risks. For example, adding multi-factor authentication to a business system to reduce an access control risk may introduce a new risk of decreased productivity when users have difficulty authenticating.

While there is some variation among the terms used by risk management frameworks, there are four types of actions (as described in Table 4) for responding to negative ICT risks: *accept*, *transfer*, *mitigate*, and *avoid*.

1078

Table 4. Response types for negative ICT risks

Type	Description
Accept	Accept ICT risk within risk tolerance levels. No additional risk response action is needed except for monitoring.
Transfer	For ICT risks that fall outside of tolerance levels, reduce them to an acceptable level by sharing a portion of the consequences with another party (e.g., ICT insurance). However, there may be consequences that cannot be transferred, like the loss of customer trust.
Mitigate	Apply actions (e.g., risk management controls) that reduce a risk to an acceptable level. Responses could include those that help prevent a loss (i.e., reducing the probability of occurrence or the likelihood that a threat event materializes or succeeds) or that help limit such a loss by decreasing the amount of damage and liability.
Avoid	Apply responses to ensure that the risk (specifically the threat) does not occur. Avoiding a risk may be the best option if there is not a cost-effective method for reducing it to an acceptable level. The cost of the lost opportunity associated with such a decision should be considered as well.

1079 In many cases, risk management controls can bring exposure to negative ICT risks within risk
1080 tolerance levels. For example, if the risk executive function declares that the organization must
1081 avoid risks with high likelihood and impact values for all costs over \$500,000, the Risk Response
1082 Type column of the risk register (see Fig. 4) can be updated with a response type from Table 4.
1083 While including a particular informative reference (e.g., security or privacy controls,
1084 Cybersecurity Framework and/or Privacy Framework categories and subcategories) may help
1085 guide and describe risk response, additional information will likely be required.

1086 In general, people, processes, and technology combine to provide risk management controls
1087 that can be applied to achieve an acceptable level of risk. Examples of controls include:

- 1088 • **Preventative:** Reduce or eliminate specific instances of a weakness
- 1089 • **Deterrent:** Reduce the likelihood of a threat event by dissuading a threat actor
- 1090 • **Detective:** Provide warning of a successful or attempted threat event
- 1091 • **Corrective:** Reduce exposure by offsetting the impact of consequences after a risk event
- 1092 • **Compensating:** Apply one or more controls to adjust for a weakness in another control

1093 Consider an organization that identifies several high-exposure negative risks, including poor
1094 authentication practices (e.g., weak or reused passwords) that could lead to the disclosure of
1095 sensitive customer financial information and the potential for employees of the software
1096 provider to gain unauthorized access to and tamper with financial data. The organization can
1097 apply several deterrent controls (e.g., warning banners, threat of prosecution for actors who
1098 intentionally attempt to gain unauthorized access) and document the applied control identifiers
1099 and any applicable notes in the Risk Register Comments column. Preventative controls include
1100 applying strong identity management policies and using multi-factor authentication tokens that
1101 help reduce authentication vulnerabilities. The software provider has installed detective
1102 controls that monitor access logs and alert the organization's security operations center if
1103 internal staff connect to the customer database without a need for access. The financial
1104 database is also encrypted so that it protects its data if the file system is exfiltrated.

1105 Risk response will often involve creating a risk reserve to avoid or mitigate an identified
1106 negative risk or to realize or enhance an identified positive risk. A *risk reserve* is similar to other

types of management reserves in that funding or labor hours are set aside and employed if a risk is triggered to ensure that the opportunity is realized or the threat is avoided. For example, the technical skills needed to recover after an ICT attack may not be available with current staffing resources. A risk reserve can also be used with the *accept* response type to address this (e.g., by setting aside funds during project planning to employ a qualified third-party to augment the internal incident response and recovery effort).

3.7. Monitor, Evaluate, and Adjust Risk Management

Risk management should not simply involve managing lists of risks. For the activities to be meaningful, risk managers throughout the enterprise must be informed about objectives, results, priorities, and opportunities. A key purpose of the risk register is to enable ongoing *monitoring* of enterprise risk activities. Based on those activities, senior leaders *evaluate* available options and *adjust* guidance and operations to help realize opportunities and minimize harmful impacts.

This Monitor-Evaluate-Adjust (MEA) Cycle is depicted in Fig. 7. This iterative approach begins with an understanding of what risk limits are acceptable, given enterprise context and strategic objectives. The purpose of ICTRM integration is to enable senior leaders to remain aware of ongoing risk management activities and apply corrective measures to achieve strategic objectives.

As risk response activities occur, they are recorded in ICT risk registers. The results are monitored, and performance measurements are collected through key performance indicators (KPIs) and key risk indicators (KRIs) and compared with the risk strategy and risk direction (based on risk appetite and risk tolerance statements). Leaders provide direction regarding the overall appetite for risk, which is then interpreted at a more granular level as risk tolerance statements.

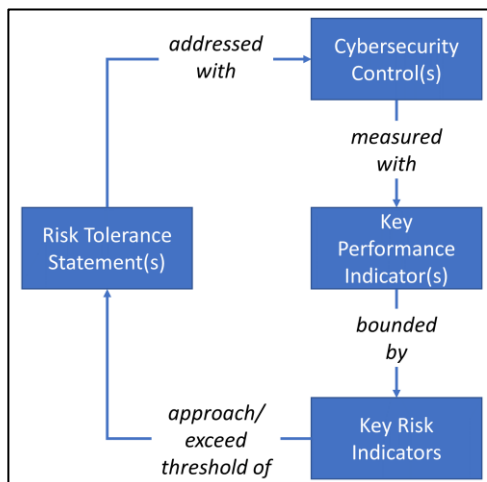


Fig. 7. Monitor-Evaluate-Adjust Cycle

1133 Those risk directives are achieved through the application of various controls that modify the
1134 risk conditions. The metrics are reported to managers and leaders who oversee achievement of
1135 risk tolerance.

1136 A third component of risk direction that must be observed is *risk capacity*, which is the
1137 maximum amount of risk that an organization is able to endure. While the enterprise should
1138 always take steps not to exceed risk appetite, the consequences of doing so are rarely
1139 catastrophic. In contrast, exceeding risk capacity could have dire consequences and may even
1140 jeopardize the continuation of the enterprise. Catastrophic results are not limited to the
1141 private sector. Many government entities have experienced severe consequences because their
1142 risk management processes permitted them to approach or exceed risk capacity.

1143 **3.7.1. Adjusting Risk Response Based on Additional Information**

1144 Risk responses will often be adjusted as opportunities and threats evolve. This is similar to the
1145 project management concept of the “cone of uncertainty,” which states that additional
1146 understanding will emerge over time to inform a more accurate estimate. For changes in
1147 identified risk, one mitigation technique is the use of risk reserves, as introduced in Sec. 3.6. For
1148 this risk response, it is important that risk owners collaborate with acquisition or procurement
1149 teams and budget owners. With appropriate budget planning, risk reserves can be released for
1150 other predetermined funding requirements after the risk has been reduced to an acceptable
1151 level or after the time has passed for the risk to occur.

1152 While many industry-based enterprises can return unused funds to shareholders or pay down
1153 corporate debt, unused reserves are more difficult for government agencies to use without pre-
1154 planning. Most government procurement cycles are rigidly based on the government fiscal
1155 year. Identified opportunities can be “planned for” in government procurement cycles as
1156 “optional” tasking or purchases. For example, unused funds could be used to expand a vendor
1157 assessment program to ensure that all supply chain providers (including both immediate service
1158 providers and their downstream providers) fulfill data processing and privacy risk management
1159 requirements. If the current fiscal year only allows for the purchase of half of the required
1160 materials, an option can be included (but not funded) at the time of the base contract award
1161 for the other half of the materials. When the project manager liberates the risk reserve after
1162 the chance of the risk occurring has passed, the funding can be used to exercise the already
1163 awarded option that lacked the initial funding when the base contract was awarded. Exercising
1164 an option in government contracting is trivial (often 30 days or less) when compared to the long
1165 lead time for initial contract procurements.

1166 **3.8. Managing Positive Risks as Part of Integrated Risk Management**

1167 In ICT disciplines, a significant portion of risk information is collected and reported regarding
1168 weaknesses and threats that could result in negative consequences. However, positive risks
1169 (i.e., opportunities) also inform decisions by senior leaders for setting the risk appetite and
1170 tolerance of the enterprise.

From an opportunity standpoint, risk appetite statements can identify targeted areas in which some loss is acceptable without crossing important lines of demarcation (e.g., innovative solutions should be pursued but not at the cost of life, safety, compliance with laws/regulations, or reputation) to achieve specific goals. Private-sector organizations pursue risk as part of their growth strategies and competitive advantage. Similarly, public-sector agencies typically have stretch goals to meet evolving industry needs, customer expectations, market demands, and other influences.

One method for identifying positive risks is a SWOT analysis that considers Strengths *and* Weaknesses as well as Opportunities *and* Threats. Consider, for example, an organization that is contemplating whether to move a major financial system from an in-house data center to a commercial hosting provider. If the organization maintains vast amounts of land and warehouses, the move could be considered a strength of the organization, and they might increase revenue by offering space to a commercial vendor to host both their own and other organizations' data centers. The Federal Government has realized many opportunities of this nature, including consolidating payroll functions under the National Finance Center (NFC) and streamlining their compliance and security processes in the Department of Justice Joint Cybersecurity Authorization Management (JCAM) tool.

Sec. 3.3.2 describes the need to treat threat actors and threat sources as inputs into an estimation of risk. If the enterprise chooses to include positive risk scenarios in the register, then the process should similarly consider *sources of opportunity* that might provide benefits. For example, a risk register entry might include the following: "Adopting a new cloud-based authentication platform introduces moderate implementation risks but presents a high-likelihood opportunity to reduce credential-based incidents by 40 % and improve user access efficiency." In this way, the register describes a positive risk — uncertainty that, if realized, produces a beneficial outcome. Alternatively, the organization could manage an *opportunity risk register* separately from the traditional threat-based risk register since positive risks often have to be assessed on a slightly different scale.

In addition to the threat modeling examples above, methods for identifying ICT-related opportunities are also available and could be as simple as an employee suggestion box. Industry publications, such as those from commercial industry associations and agencies like NIST, regularly provide information and ideas regarding potential innovations or advances for areas such as supply chain, privacy, and cybersecurity improvements.

Numerous formal methods are available for identifying opportunities, including:

- **Brainstorming**—A group innovation technique, often led by a facilitator, that elicits views from participants to identify and describe opportunities
- **Delphi**—A procedure to gain consensus from a group of subject-matter experts using one or more individual questionnaires that are collected and collated to identify opportunities to pursue
- **Ideation** —A consistent process of observing an environment, discerning opportunities for improvement, experimenting with possible resolutions, and developing innovative solutions

1212 The same formal methods can be used to determine other inputs (e.g., those described in Sec.
1213 3.3.3 and 3.3.4) and can be visualized to show both negative and positive risks, as shown in Fig.
1214 8.

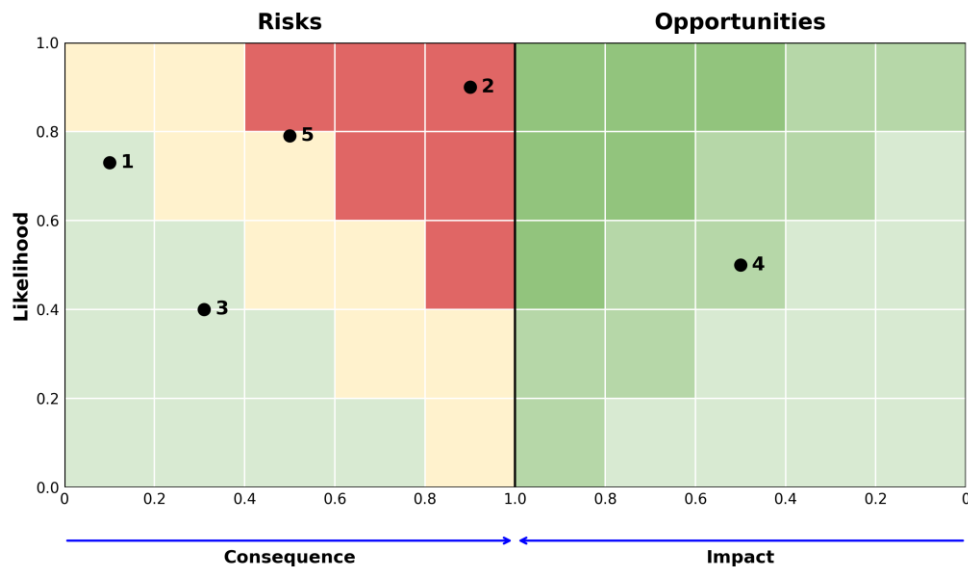


Fig. 8. Example of a risk heatmap with positive and negative risks

1217 Regarding positive risk response, consider the previous example of an organization that has
1218 identified the positive risk of increasing revenue by providing physical space to a commercial
1219 vendor. Analysis of the risk has determined that the opportunity would be highly beneficial to
1220 the enterprise. The consolidation described in the example also provides a moderate
1221 opportunity to improve availability as an element of supply chain risk management. The Risk
1222 Response Type column of the risk register should also be updated using a response type from
1223 Table 5, the comment field updated to contain information pertinent to the opportunity, and
1224 the residual risk uncertainty of not realizing the opportunity calculated.

1225 With these controls and methods in place and assessed as effective, the remaining risks can be
1226 analyzed to determine the residual impact, likelihood, and exposure, as described in Sec. 3.4. If
1227 the residual exposure falls within risk tolerance levels, then stakeholders can proceed in gaining
1228 the benefits of the opportunity. Each of these values is added to the risk register for enterprise
1229 reporting and monitoring.

1230 Where positive risks are to be considered and included in risk registers, there are four generally
1231 used response types, as described in Table 5.

1232

Table 5. Response types for positive ICT risks

Type	Description
Realize	Eliminate uncertainty to make sure the opportunity is actualized (sometimes referenced as <i>exploit</i>).
Share	Allocate ownership to another party that is better able to capture the opportunity.
Enhance	Increase the probability and positive impact of an opportunity (e.g., hire risk management staff to better focus on an organization's privacy risk and data processing protections).
Accept	Take advantage of an opportunity if it happens to present itself (e.g., identify and prioritize those supply chain risk gaps that should be addressed at the first opportunity).

1233

As with negative risks, positive entries in the ICT risk registers should be normalized and

1234

aggregated into the enterprise-level risk register.

1235 4. Building ERRs and ERPs from ICTRM-Specific Risk Registers

1236 The achievement of defined expectations is
1237 conveyed through risk registers that
1238 document and communicate risk decisions.
1239 Risk assessment results and risk response
1240 actions at the system level are reflected in
1241 the ICT risk registers. The registers from
1242 multiple systems are collated, aggregated,
1243 normalized, and provided to business
1244 managers at the organization level to
1245 provide a composite risk understanding.
1246 Those managers can evaluate results and
1247 refine risk tolerance criteria to optimize
1248 value delivery, resource utilization, and risk.
1249 The enterprise-level aggregation of all the
1250 various risk registers into an ERR and a
1251 prioritized ERP enables senior leaders to
1252 monitor risk responses while considering the
1253 expectations that have been set.

1254 This section takes a closer look at how ICT
1255 risk registers are used as the inputs for
1256 building an ERR and ultimately an ERP, as
1257 depicted in Fig. 9.

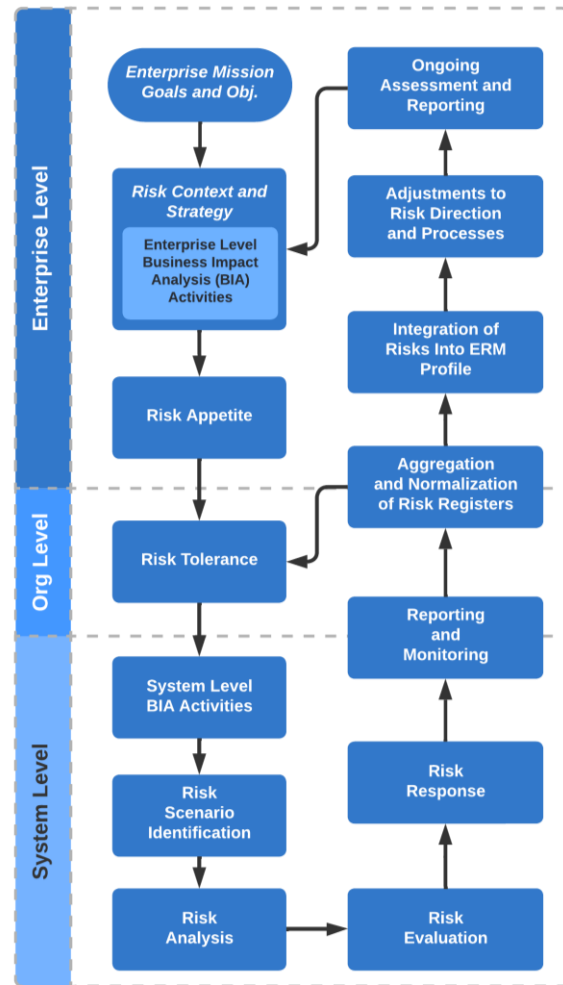


Fig. 9. ICTRM integration cycle

1261 4.1. Creating and Maintaining Enterprise-Level ICT Risk Registers

1262 A key outcome of the risk identification and communications elements is the ability to create
1263 enterprise-level ICT risk registers as input to the broader ERR (Sec. 4.2). As described
1264 throughout Sec. 3, applying a consistent risk register with agreed-upon criteria and categories
1265 enables various data points to be normalized, aggregated, and sorted into an enterprise view.

1266 Risk registers are composed and maintained at all levels: enterprise (including higher-level and
1267 lower-level enterprises), organization (including suborganizations and business units), and
1268 system.¹⁷ The vertical columns in Fig. 3. ICTRM as part of ERM should not be interpreted as
1269 guidelines to address such risks as isolated silos. Rather, information for various types of ICT
1270 risks should be shared with those at higher organizational levels for the benefit of the whole
1271 enterprise. Similarly, ICTRM should not be isolated to only one organizational level

¹⁷ OMB Circular A-130 defines an information system as “a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information” OMB-A130.

nor within a single ICT risk discipline. Instead, those at the organizational level should collaborate and communicate about issues, problems, and opportunities identified. The lessons learned about successes and challenges can be conveyed to peers, enterprise management, and other organizations using risk registers and RDRs. As the system and organization risk registers are completed for each risk discipline, they are provided to the designated risk officers at the relevant level and shared with senior management to 1) *normalize* (e.g., ensure consistency for definitions and values recorded by different enterprise entities, remove duplicate risk reporting) and 2) *aggregate* risks in similar categories into a concise view.

To support the subsequent aggregation of various risk registers, enterprise risk guidance should identify the enterprise objectives with which various types of ICT risk should be aligned. The ERP reflects risks that may have impacts in four discrete enterprise objectives: strategic, operations, reporting, and compliance. These same four objectives were key factors in the original COSO ERM framework and are often used as guideposts for enterprise risk reporting. Clear direction from senior leaders about how to align various types of ICT risk with enterprise objectives will help enable subsequent aggregation, normalization, and prioritization. Objective alignments include:

- **Strategic** risks related to the implementation of a new service offering, opportunities for innovation within an ICT area, and change management improvements and challenges
- **Operations** issues regarding product or service quality and resilience (e.g., supply chain interruption that disables a manufacturing process), processes and procedures for privacy risk posture, OT considerations, and business continuity/disaster recovery issues
- **Reporting** regarding ICT risk issues, including insurance considerations and material risk factors that affect disclosures or statutory reporting
- **Compliance** risks where a negative event might result in a failure to meet a contractual service agreement or in a regulatory penalty or fine

Direction may be needed to account for risks that cross multiple boundaries and how each organizational level should perform an aggregation of subordinate risk registers.

4.2. Creating the Enterprise Risk Register (ERR)

Enterprise risk officers collect all risk inputs, including the ICT risk registers, and analyze potential risk events, consequences, and impacts at the enterprise level to create the ERR. The ERR is subsequently prioritized to create the ERP, discussed in Sec. 4.3, which enables key executive stakeholders to stay aware of critical risks, including those that are ICT-related.

As part of their risk guidance, enterprise leaders designate ERM process participants and define the responsibilities of each role, including those involved in enterprise risk governance. That guidance should declare which role is responsible for creating and maintaining the ERR, how frequently it will be updated, and how the risks within it will be communicated to various stakeholders. That role is typically assigned to the enterprise risk officer, though the responsibility could fall on any designated party or other roles, as described in Sec. 3.3.1.

The creation and maintenance of the ERR also supports a periodic review of enterprise risk guidance, including risk definitions, context, and risk appetite criteria. It provides an opportunity to review and validate enterprise definitions for risks, risk categories, and risk assessment scales. If any changes or updates to the risk context or guidance need to occur, the enterprise risk officer (or equivalent) will likely have sufficient seniority to ensure appropriate updates to those enterprise processes. Practitioners should consider any positive risks present in the rolled-up report and add other opportunities as inputs to the ERR.

Fig. 10 provides a notional ERR that combines both federal agency and critical infrastructure risks and that illustrates the integration of various ICT risks alongside other key enterprise risks.

Notional Enterprise Risk Register												
ID	Pri.	Risk Description	Risk Category	Current Assessment					Risk Response	Risk Owner	Status	
				Financial Impact	Reputation Impact	Mission Impact	Likelihood	Exposure Rating				
1	5	Retiring staff lead to personnel shortages	Operational Risk	OpEx: M CapEx: L	Low	Mod	Mod	Mod	● Improve hiring diversity ● Improve employee benefits per recent survey and discussions	Dwayne Rhodes (Human Resources Department)	Open	
2	6	A strategic opportunity to hire a famous technologist to establish a new satellite communications initiative.	Operational Risk	OpEx: M CapEx: L	High	Mod	Mod	Mod	● Allocate funds for compensation package ● Initiate strategic recruiting plan	Dwayne Rhodes (Human Resources Department)	Open	
3	1	A social engineering attack on enterprise workforce leads staff to wire transfer significant funds.	Operational Risk	OpEx: M CapEx: L	High	Mod	High	High	● Update corporate IT security training ● Implement phishing training service ● Update email security products per recommendations from IT Risk Council	Carly Franklin (CISO)	Open	
4	3	An employee of a third-party partner steals customer information.	Operational Risk	OpEx: H CapEx: M	High	High	Mod	High	● CFO and CEO to agree on plans for likely secondary financial impact from reputational risk impact. ● Update procurement contract requirements to include clauses per 11/3/2019 report from Legal Dept ● Implement 3rd Party Partner Assmt. for Tier 1 providers per CIO & CISO recommendations	Ernest Woods (Procurement)	Open	
5	7	Sales reduction due to tariffs leads to reduced revenues.	Financial Risk	OpEx: M CapEx: L	Low	Low	Low	Low	● Increase marketing in target areas ● Ensure competitive pricing in target markets	Elaine Kim (VP Sales)	Open	
6	8	Customer budget tightening results in reduced revenue and profits.	Financial Risk	OpEx: M CapEx: L	Low	Low	Mod	Mod	● Implement customer surveys to better forecast purchasing changes ● Use cost-cutting measures to offset reductions and maintain profitability	Elaine Kim (VP Sales)	Open	
7	9	Failure to innovate results in market share erosion.	Strategic Risk	OpEx: M CapEx: M	Mod	Low	Mod	Low	● Approve CIO proposal to increase internal R&D funding by 10% to spur internal innovation ● Update technical training to include design thinking methodologies ● Implement customer surveys in target marketing areas	Sharika Grigsby (VP, Product Development)	Open	
8	2	Company intellectual property data is disclosed through employee error or malicious act.	Operational Risk	OpEx: M CapEx: M	High	High	Mod	Mod	● Review and update (if needed) background screening controls ● Update corporate security training to reinforce the need for diligence ● Implement data loss prevention tools per CISO recommendation	Carly Franklin (CISO)	Closed	
9	10	A flaw in product quality leads to reputational damage, reducing sales.	Strategic Risk	OpEx: M CapEx: M	High	High	Low	Low	● Update continuous improvement process ● Implement Baldrige Framework ● Update external provider quality standards and monitoring	Sharika Grigsby (VP, Product Development)	Open	
10	4	Failure to implement California Consumer Privacy Act (CCPA) provisions exposes the company to fines, penalties, and legal fees.	Compliance Risk	OpEx: H CapEx: L	Mod	Mod	Mod	Mod	● Create & maintain a centralized register of compliance requirements ● Update employee training based on updated privacy requirements ● Review business impact assessment (BIA) templates to ensure ICT criteria are included.	Zoe Davidson (Chief Privacy Officer)	Open	

Fig. 10. Notional example of an ICT-inclusive ERR

This example illustrates the inclusion of a positive risk (item 2) along with negative risks. Of course, an actual ERR would include many more entries, both positive and negative. Most of the columns in this example are the same as their lower-level risk register counterparts. The

1324 notable exception is that the example ERR splits the Current Assessment – Impact into three
1325 columns, which are described in Table 6.

1326 **Table 6. Descriptions of additional notional ERR elements**

ERR Element	Description
Current Assessment – Financial Impact	Analysis of the potential financial benefits or consequences resulting from this scenario, including cost considerations. While this element could be quantitative, it is often qualitative (e.g., high, moderate, low) at the enterprise level. Financial considerations may be expressed as 1) capital expenditures that represent a longer-term business expense (e.g., property, facilities, equipment) and 2) operating expenses that support day-to-day operations.
Current Assessment – Reputation Impact	Analysis of the potential benefits or consequences that the scenario might have on the stature, credibility, or effectiveness of the enterprise. Some enterprises perform a formal sentiment analysis using commercial services or other technical tools to support assessment.
Current Assessment – Mission Impact	Analysis of the potential benefits or consequences that the scenario might have on the ability of the enterprise to successfully achieve mission objectives.

1327 The ERR provides an easily consumed summary for understanding the risk landscape, while the
1328 RDR provides additional information, such as:

- 1329 • Detailed risk information (e.g., full risk statement, detailed scenario description, key risk
1330 indicators, enterprise status for this particular risk)
- 1331 • Information regarding various risk roles (e.g., risk owner, risk manager, risk approver)
1332 and affected stakeholders
- 1333 • Historical timeline information (e.g., last update date, next expected review)
- 1334 • Risk analysis information (e.g., aggregate understanding of threats,
1335 weaknesses/preexisting conditions, resources affected, impacts)
- 1336 • Detailed risk response information (e.g., responses implemented, status and results of
1337 previous responses, additional responses planned)

1338 The ERR provides input for those performing enterprise risk oversight, such as an executive risk
1339 committee. By tracking status and exposure value, enterprise stakeholders can identify the
1340 most relevant and/or high-priority risks to inform stakeholders (e.g., federal departments and
1341 agencies; those in an oversight role, such as Congress, OMB, or GAO) about existing risks, risk
1342 responses, and planned activities.

1343 Since it is difficult to compare dissimilar risk exposures (e.g., employee retention, disaster
1344 recovery), risks are often translated into financial impacts and may be further broken down into
1345 direct costs, such as the financial cost of reputational damage. The relative financial impact of
1346 each type of risk can provide further input into risk management prioritization and monitoring
1347 decisions for enterprise risk managers. Reputation exposure can be similarly determined in the
1348 ERR by combining high-impact attacks, enterprise sector, and consequences with a histogram
1349 analysis of stakeholder sentiment categorized by stakeholder type. This last action of
1350 prioritization creates the ERP, as discussed in Sec. 4.3.

An enterprise risk register can consider both inherent and residual risk. The COSO ERM Framework [COSOERM] describes these terms and differentiates between actual residual risk and target (i.e., desired) risk:

- “Inherent risk is the risk to an entity in the absence of any direct or focused actions by management to alter its severity”
- “Target residual risk is the amount of risk that an entity prefers to assume in the pursuit of its strategy and business objectives, knowing that management will implement or has implemented direct or focused actions to alter the severity of the risk.”
- “Actual residual risk is what remains after management has taken action to alter its severity. Actual residual risk should be equal to or less than the target residual risk.” [COSOERM]

The term *inherent risk* describes conditions in the absence of risk management actions. There are likely to be at least *some* elements that help mitigate risks in every established organization, so as a practical matter, this publication typically refers to *current risk* rather than *inherent risk* when representing a baseline risk posture.

4.3. Developing the Enterprise Risk Profile (ERP)

As risk information is transmitted up from lower levels of the organization, each level’s risk register should provide the pertinent information for creating a prioritized risk profile for the level immediately above it. For example, a subject-matter expert in a particular ICT risk discipline might provide their own prioritization of risks within their discipline for consideration by the next level of risk experts.

Subordinate organizations’ impacts may be different, similar, conflicting, overlapping, or unavailable and must be properly combined by financial and mission analysis at the level immediately above the reporting organization. While the impacts of ICT risk on various assets may be determined at lower levels, the overall cash flow and capital implications of all of the risks can only be normalized and aggregated by enterprise fiduciaries (e.g., CFOs) and then recorded in the ERR. Similarly, enterprise mission impacts must be aggregated and expressed by the senior executives who are most directly accountable to stakeholders.

The ERR informs the ERP once the risks are prioritized at the highest level of the risk management function in the enterprise, as depicted in Fig. 11.

OPERATIONS OBJECTIVE – Manage the Risks of a Remote Workforce							
Risk Description	Exposure Factors	Assessment			Current Risk Response	Proposed Risk Response	Risk Owner
		Last	Current	Residual			
A global pandemic may necessitate a remote workforce where Agency X could face: ● a forced reliance on potentially insecure networks; ● a reduction in managerial oversight; and ● a deterioration of Agency culture.	Impact	High	Medium	Medium	REDUCTION: Agency X has: ● Facilitated secure remote access via the setup of a Virtual Private Network (VPN) ● Modified existing standard operating procedures to include formal mechanisms for increased transparency and self-reporting. ● Established a formal remote/telework policy including means of social interaction (e.g., virtual gatherings, campfire sessions, etc.) to foster team building.	Agency X will begin allowing employees to work remotely one day per week and closely monitor employee productivity.	Primary - Chief Operating Officer (COO)
	Likelihood	Low	Low	Low			
REPORTING OBJECTIVE - Privacy Policies Must Accurately Describe Organizational Handling of PII							
Agency X's privacy policies and disclosures are found to inaccurately describe its collection, use, storage, and disclosure of personally identifiable information (PII).	Impact	High	High	Medium	REDUCTION: Agency X has begun an assessment of existing methods of PII processing to ensure they align with existing policies and are within the bounds of all applicable regulatory requirements.	Agency X will establish a quarterly audit of PII processing and develop a privacy-specific change management plan for inclusion of any necessary updates.	Primary - Chief Privacy Officer (CPO)
	Likelihood	Medium	Medium	Low			
OPERATIONS OBJECTIVE - Manage the Risk of Sudden Interruptions in the Supply Chain							
A key supplier of Agency X has abruptly gone bankrupt.	Impact	High	High	Medium	REDUCTION: Agency X has begun to formally analyze downstream demand and other market variables to have a better understanding of their current suppliers' ability to handle the dynamic nature of demand.	Agency X is seeking to ensure redundancy within their supply chain by identifying backup/alternative suppliers and seeking to reduce the potential time needed to transition to a new supplier.	Primary - Logistics Coordinator
	Likelihood	Medium	Medium	Medium			

Fig. 11. Notional example of an enterprise risk profile

The ERP reflects assessments of mission, financial, and reputation exposures organized according to the four enterprise objectives. They may be full-value exposures or modified (and so noted) by the likelihood assessments of enterprise leaders. At the top enterprise level, ERM officials may judge likelihood and impact as part of the normalization process, along with other members of the enterprise risk executive function. While the ERM process helps drive the discussion and calculation of likely risk scenarios, recent natural disasters have demonstrated that actual consequences can far exceed initial loss expectations. Enterprise executives should continually observe industry trends and actual occurrences to readjust likelihood and impact estimations and reserves based on a changing risk landscape. ERPs should also reflect comparable occurrence incidents and trends for the subject enterprise and peer organizations.

The ERP supports the governance and management of measuring significant financial, reputational, and mission impacts. Some enterprises may also use this taxonomy to support a

broader risk breakdown structure (RBS) that provides a hierarchical representation of risks with high-level risks near the top and increasingly detailed risks below each category, as shown in Fig. 12.

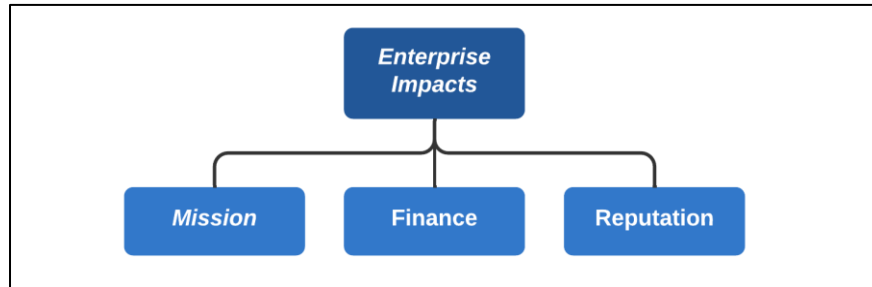


Fig. 12. Impacts on enterprise assets for a business or agency

Here, ERP considerations include:

- **Financial impact** — Various risk scenarios are converted into actual capital and operational expenses, enabling executive leaders to conduct a fiscally responsible cost-benefit analysis that considers the recommended strategies for risk response.¹⁸
- **Reputation impact** — While subordinate risk registers describe risk scenarios, including those that may impact reputation, executive leaders record the evaluation of consequences on the enterprise's reputation. This also supports consideration of other downstream impacts that are likely to result from damage to reputation, such as financial losses or credit risks.
- **Mission impact impacts** — Executive leaders record the evaluation of consequences on the overall ability for the enterprise to conduct its mission and achieve strategic objectives.¹⁹ Many specific ICT risks (e.g., health, safety, and environment [HSE]) have a direct impact on the enterprise's ability to fulfill its mission.

These three high-level impact considerations are then used in conjunction with other enterprise risk responses to determine tolerances, allocations, and disclosures commensurate with risk exposure.

4.4. Translating the ERP to Inform Leadership Decisions

For some organizations, information from the ERP will need to be provided to senior managers who have a fiduciary duty to remain aware of and help manage risks. In this way, enterprise leaders will have the necessary information and opportunity to consider risk exposures as factors for budgets or corporate balance sheet reporting. Both private-sector and public-sector enterprises will benefit from the risk register integration process. Creating a risk profile can

¹⁸ These presentations are equivalent to the financial disclosures in Form 10-Q and Form 10-K filings to the U.S. Securities and Exchange Commission (SEC) by commercial public companies each quarter and Form 8-K filings as risk incidents occur.

¹⁹ Mission impact on commercial public enterprises is often expressed in share value/market cap and share volatility tables and is disclosed in SEC filings and shareholder communications.

1423 provide leaders with a thoughtful analysis of the risks that an enterprise faces when pursuing its
1424 strategic objectives and help them identify appropriate options for addressing significant risks.
1425 This prioritization is supported by one of COSO’s key principles: “The organization prioritizes
1426 risks as a basis for selecting responses to risks” [COSOERM].

1427 Table 7 provides a notional Enterprise Risk Profile Supplement, which is a portfolio evaluation
1428 of various organizational risk profiles that inform executive decision-making.

1429 **Table 7. Notional enterprise risk portfolio view for a private enterprise**

Financial Risk Profile						
	Current Period			Previous Period		
	Net Revenue	Capital	Free Cash Flow	Net Revenue	Capital	Free Cash Flow
Enterprise						
Dept A						
Dept B						
...						
Dept N						
Reputation Risk Profile						
	Current Period			Previous Period		
	Public	Regulators	Partners	Public	Regulators	Partners
Enterprise						
Dept A						
Dept B						
...						
Dept N						
Mission Risk Profile						
	Current Period			Previous Period		
	Product/Service Capability	Philanthropy	Share Value	Product/Service Capability	Philanthropy	Share Value
Enterprise						
Dept A						
Dept B						
...						
Dept N						

1430 5. Enterprise Strategy for ICT Risk Coordination

1431 As part of their governance responsibilities, executive leaders should establish clear and
1432 actionable risk management guidance based on the enterprise's mission and business
1433 objectives. They should also plan to continually review and adjust the risk strategy based on an
1434 evolving risk landscape (e.g., due to technological and environmental changes). Additionally, an
1435 enterprise that is subject to external regulation is likely to receive specific guidance regarding
1436 updated federal statutes and directives that must be considered when evaluating acceptable
1437 risk.

1438 5.1. Risk Integration and Coordination Activities

1439 Enterprise leadership may wish to tailor the approach for their unique circumstances. For
1440 example, while risk appetite statements usually originate from the most senior leaders, those
1441 leaders may choose to delegate the creation of ICT risk appetite statements to a senior ICT risk
1442 official.

1443 Table 8 describes the process by which senior leaders express expectations and receive results
1444 about managing ICT risk throughout the enterprise.

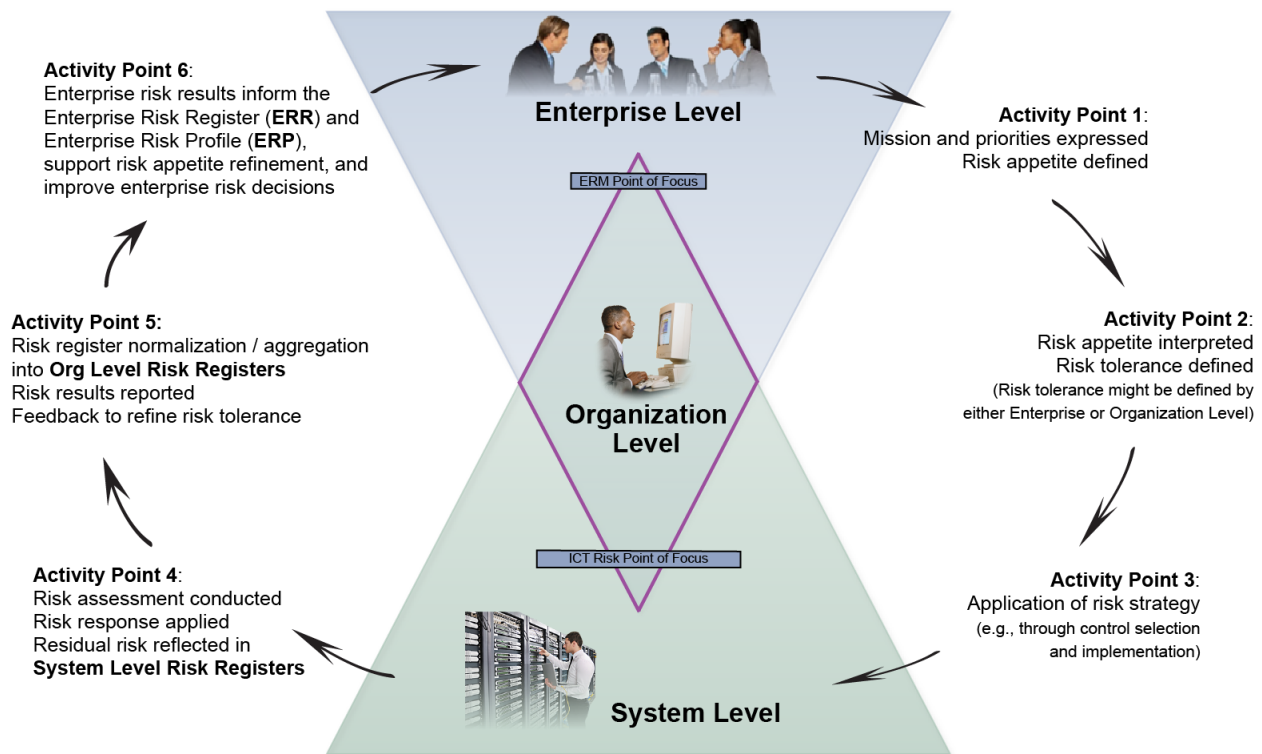
1445 **Table 8. Inputs and outputs for ERM governance and integrated ICTRM**

Activity Point	Inputs	Outputs
Set risk expectations and priorities	Internal and external risk context, enterprise roles and responsibilities, and governance framework and governance systems for managing all types of risks	Documentation of enterprise priorities considering mission objectives and stakeholder values, direction regarding budget (e.g., authorization for capital and operating expenditures), and risk appetite statements pertaining to each risk management discipline, including ICT
Interpret risk appetite to define risk tolerance statements	Enterprise priorities considering mission objectives and stakeholder values, direction regarding budget (e.g., authorization for capital and operating expenditures), and risk appetite statements	Risk tolerance statements (and metrics) to apply risk appetite direction at the organization level and direction regarding methods to apply ICTRM (e.g., centralized services, compliance/auditing methods, shared controls to be inherited and applied at the system level)
Apply risk tolerance statements to achieve system-level ICTRM	Risk tolerance statements, direction regarding shared services and controls, and lessons learned from previous ICTRM implementations.	Inputs to preparatory activities, system categorization, and the selection and implementation of risk management controls
Assess ICT risks and report system-level risk response through risk registers	Security plans, risk responses, and system authorization (or denial of authorization with referral back for plan revision)	Risk assessment results, risk registers describing residual risk and response actions taken, and risk categorization and metrics that support ongoing assessment, authorization, and continuous monitoring
Aggregate organization-level risk registers	Risk registers that show system-level risk decisions and metrics, internal reports from compliance/auditing and monitoring processes to confirm alignment with enterprise risk strategy,	Risk registers aggregated, normalized, and communicated based on enterprise-defined risk categories and measurement criteria and any necessary refinement of risk

Activity Point	Inputs	Outputs
	and observations regarding ICTRM achievement in light of the risk strategy	tolerance statements to ensure balance among value, resources, and risk
Integrate risk registers into ERR and ERP	Normalized and harmonized risk registers from various organization-level ICTRM reports, compliance and audit reports, results from other non-technology risk management activities (e.g., credit risk, market risk, labor risk), and observations regarding ERM and ICTRM achievement	Integrated ERR that aligns ICTRM results with those of other risk categories; the refinement of risk appetite tolerance statements and risk management direction to ensure balance among value, resources, and risk; and ERP for monitoring and reporting overall risk management activities and results

1446

1447 Fig. 13 provides a simplified illustration of risk integration and coordination activities.



1448

1449 Fig. 13. Illustration of enterprise risk management integration and coordination

1450 The processes described here are cyclical. Early iterations may include the definition of terms,
1451 strategies, and objectives. Subsequent iterations may focus on refining those objectives based
1452 on previous results, observations of the risk landscape, and changes within the enterprise.

1453 5.1.1. Detailed Risk Integration Strategy

1454 Fig. 14 illustrates a more detailed information flow of inputs and outputs among ICTRM
1455 participants at the three levels. Senior leaders and business managers define risk tolerance
1456 direction that is applied at the system level. System-level practitioners interpret those risk
1457 tolerance statements and apply ICTRM activities to achieve risk management objectives.



47

Through risk monitoring, results are then reviewed to confirm effectiveness, highlight opportunities for improvement, and identify important trends that might require organization- or enterprise-level action. The output of this activity helps improve communication about performance, risk trends, and opportunities among all levels. Specific process activities are based on the risk management methods applied but will generally include the following:

Risk Context and Strategy Activities

- Based on the enterprise mission, executives identify the systems and services that represent mission- and business-critical functions. Executives then work with senior leaders to identify the enterprise-level assets that enable those functions. Those assets inherit the criticality/priority of the functions they support. Enterprise assets that support those objectives are also identified (e.g., through a BIA).²¹
- As described in Sec. 5.1, leaders at Level 1 (enterprise) and Level 2 (organization) define specific and measurable risk appetite and risk tolerance statements that reinforce enterprise mission objectives and organization goals.
- At Level 3 (system), practitioners interpret the criticality/priority direction expressed in the risk appetite and risk tolerance statements to identify the ICT assets, processes, and activities that support mission-essential delivery operations. System-level assets are categorized based on their sensitivity and criticality to enterprise operations in line with the enterprise-level BIA. Those in various roles (e.g., system owners, security officers) work together to derive system-level requirements and record impact understanding in the system BIA register.

Risk Identification Activities

- The value of each asset (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. Subsequent risk decisions depend on an accurate understanding of the importance of each resource.
- For each of these components, the practitioner identifies threat sources, their potential harmful effects, and the vulnerabilities or conditions that might enable such effects. The scenario is recorded in the risk register's Risk Description column. The category is recorded in the Risk Category column based on enterprise criteria to support risk correlation, aggregation, and reporting.

Risk Analysis Activities

- The practitioner performs risk analysis to determine the likelihood that the threat events and vulnerable conditions would result in harmful impacts to system assets. Similarly, the practitioner analyzes the impact value and calculates the risk exposure using the methodology defined in the enterprise risk strategy.²² The results of these

²¹ For practitioners integrating cybersecurity with ERM, IR 8286D, *Using Business Impact Analysis to Inform Risk Prioritization and Response*, provides additional information about the use of BIA in risk management IR8286D.

²² While this document's discussion of risk as a product of risk likelihood and risk impact is sufficient for many purposes, "likelihood" is itself a compound state of multiple sub-factors, such as adversarial threat, skills, motives, and opportunities.

analyses are recorded in the risk register's Current Assessment column as "Likelihood," "Impact," and "Exposure."

Risk Response Activities

- The determined exposure is compared with the risk tolerance. If exposure is within risk tolerance limits, the risk may be **accepted**.
- If exposure exceeds tolerable levels of risk, practitioners consider whether they can achieve risk tolerance through other forms of risk response. For example:
 - Controls can often be applied to **mitigate** risk by reducing its likelihood or impact to a tolerable level. Controls should be implemented with a corresponding performance scale (i.e., KPI) that is used as the basis for KRIs.
 - Risk response may also include risk **transfer**, also known as risk sharing. For example, an organization might hire an external organization to process sensitive transactions (e.g., payment card transactions), thus reducing the likelihood that such sensitive data would be processed by an in-house system. Another common risk transfer method involves the use of ICT insurance policies that can help reduce the economic impact of an adverse event.
 - Practitioners (e.g., the system owner) may even need to work with Level 2 leaders to **refine the risk direction or the risk tolerance itself** (e.g., through an exception process, an adjustment to the risk tolerance statement, or increased security requirements for the relevant system).
 - If an unacceptable ICT risk cannot be adequately treated in a cost-effective manner, that risk must be **avoided**. Such a condition may require a significant redesign of the system or service. These circumstances should be rare, and they highlight the value of risk coordination early in the system engineering process. Notably, risk avoidance is not the same as ignoring a risk.

5.1.2. Risk Monitoring and Communication Activities

A key purpose of the various risk registers is to enable the ongoing *monitoring* of enterprise risk activities so that risk managers throughout the enterprise can be informed about the objectives, results, priorities, and opportunities identified through the risk responses. Much of that monitoring occurs by analyzing performance metrics, including those that indicate changes in risk. KRIs inform organizations whether controls are adequately addressing risk and whether risks are changing over time. When KRIs fall outside of pre-established thresholds, risk response is beyond acceptable levels. In this case, organizations should evaluate risks and make any necessary adjustments to the controls. Results of risk activities and decisions are recorded in the risk register.

Table 9 provides examples of ICT-related risk appetite, risk tolerance, controls, KPIs, and leading and lagging KRIs, which all support the MEA Cycle (see Fig. 7).

1533

Table 9. Notional ICT-related examples that support the MEA Cycle

	Example 1	Example 2	Example 3
Risk Appetite	Mission-critical systems must be protected from known cybersecurity vulnerabilities.	In keeping with the enterprise designation as a data processor, all personal data are kept confidential, as described in the GDPR (European Union General Data Protection Regulation).	Our customers associate reliability with our company's performance, so outsourced hosting services must minimize outages for any customer-facing websites.
Risk Tolerance	Systems designated as mission-critical must be patched against critical software vulnerabilities (severity score of 10) within 14 days of discovery.	While there may be some tolerance for limited low-risk corporate information disclosures, there is zero tolerance for the disclosure of personally identifiable information (PII).	Regional managers may permit website outages by supply chain partners, but the outages must not exceed two hours and may affect no more than 5 % of customers.
Controls	Periodic vulnerability assessments Patch deployment capabilities	Authentication method PII processing and transparency policy Authority to process PII Audit log alerting/evaluation	Service-level agreements Redundant provider circuits Web load balancers Web servers
KPIs	Percentage of vulnerabilities patched	Days without a loss of PII	Outage time in hours
Leading KRIs	Number of computers with critical vulnerabilities (CVSS score of 10) that have not been patched in 10 days	Failed facility reviews for unprotected physical records Audit log records showing violation of requirements for separation of duties	Outages that have lasted over 1.5 hours and affect more than 5 % of customers Outages that have lasted over two hours and affect fewer than 5 % of customers
Lagging KRIs	Number of computers with critical vulnerabilities that have not been patched in 15 days	One or more violation indications from data loss prevention tools	Current outages that have lasted over two hours and affect more than 5 % of customers

1534 A key purpose of the various risk registers and reporting methods is to make adequate
1535 governance information available to monitor enterprise risk decisions. Enterprise processes
1536 should ensure that the communication of risk has been accepted, which implicitly accepts the
1537 risk itself (e.g., through an exception process).

1538 Risk activities may also be informed by relevant internal and external audit findings. Significant
1539 audit findings often have enterprise-level impacts. However, lower-severity findings may spread
1540 through multiple systems to create risk in aggregate if they are not addressed adequately. The
1541 coordination of audit findings may span multiple levels of the enterprise. For example, as
1542 operational teams address shortcomings or system deficiencies at the system level, key findings
1543 might be communicated and tracked by an audit committee. As responses to findings occur and
1544 are documented (e.g., through a corrective action plan), they assist in the planning of the
1545 subsequent ERM. For some enterprises, the composite set of system risks, responses applied,

and other relevant artifacts will be reviewed by a senior official to confirm that risk decisions and risk responses align with risk tolerance and risk appetite directives.²³

Subsequently, risk registers for various risk management disciplines from throughout the organization level are normalized and aggregated to provide a composite view of the risk posture and decisions for that organization. As Level 2 and 3 managers consider feedback from system-level risk activities, they may decide to refine risk tolerance levels. For example, the aggregate risk across multiple systems may represent too great an exposure and need to be reduced. In other cases, based on successful risk management results, stakeholders may permit more risk in some areas to support mission objectives, save resources, or redirect those resources to other areas. Similar reviews and refinement occur at Level 1 to support enterprise governance and risk management decisions. Some types of enterprises may be required to formally disclose risk factors (e.g., through annual reports), and an aggregated understanding of ICT risks and risk decisions can support their fiduciary responsibilities. These activities may also help others (e.g., federal agencies) comply with mandatory requirements, such as those established by OMB.

At Level 3, practitioners interpret the risk tolerance, develop requirements, and apply controls to achieve an acceptable level of risk in a cost-effective way. For example, consider a global retail firm in which the system owner of a customer-facing website selects controls that will ensure adherence to availability service levels. In deciding which controls to apply, the system owner collaborates with a security team to consider methods for meeting service-level objectives. The team can contact the local power utility supplier to determine electrical availability history and gather other information regarding the likelihood of a loss of power to the website. This additional information might help the system owner decide whether to invest in a backup generator to ensure sufficient power availability.

Results from previous assessments can be useful for estimating the likelihood of achieving risk goals in the future. The team would then move to the next risk scenario (e.g., an internet service outage) and review the history and reliability of the organization's telecommunications provider to ascertain the likelihood and impact of a loss of service. By iterating through each potential risk, as described in Fig. 14, practitioners can develop a risk-based approach to fulfilling risk management objectives based on risk appetite and risk tolerance. This, in turn, helps risk practitioners demonstrate how their actions directly support mission objectives and enterprise success.

5.2. Aggregation and Normalization of Risk Registers

A risk register's precise contents and format will vary by enterprise but will generally follow the structure that has been illustrated throughout this publication. When creating integration processes, practitioners should ensure that the aggregation and communication themselves do not undermine the actual risk management activities (e.g., overwhelming staff with too many

²³ For federal agencies, ICT is typically subject to Federal Information Security Modernization Act (FISMA) privacy and security requirements, so the system authorization process might represent an example of this cycle.

1583 risk scenarios). Instead, a collaborative approach to effectively optimize ICT value, risk, and
1584 resources will help achieve enterprise objectives.

1585 **5.2.1. Aggregation of ICT Risk Information**

1586 The activities described Sec. 4 provide guidelines on how to complete the risk register for a
1587 given system to record information about known risk scenarios, an analysis of their impacts,
1588 and actual or planned activities to respond to those risks.

1589 Aggregation activities are performed among the hierarchical levels shown previously. System-
1590 level risk registers are combined with others from the same lower-level organization (e.g.,
1591 business department, branch office, division). Similarly, the now-combined risk registers at the
1592 organization level (e.g., business unit, government bureau) and enterprise level are aggregated
1593 and normalized. The method for managing the risk identifier (ID) is up to the practitioner, but a
1594 source identifier might be needed to provide traceability to the original register (e.g., "System
1595 A" risk register ID #1 might be tagged as aggregated risk ID A-1).

1596 **5.2.2. Normalization of Risk Register Information**

1597 While aggregation is occurring, the ICT risk manager will also be normalizing the information
1598 contained in the various risk registers. As data points are brought together, there will likely be
1599 some risks that occur so infrequently (or are of low enough consequence) that they do not
1600 merit inclusion in the next-level register. Decisions about what to integrate and how to do so
1601 depend on the use of a common risk rating scheme that enables risk assessments to be
1602 translated and integrated at higher enterprise levels. At a minimum, the normalization process
1603 at the higher level (e.g., for the ERR) should use the same rating criteria to enable comparison
1604 and tracking. This typically includes definitions for how negative (and positive) consequences
1605 and likelihood are to be measured to allow for comparison across assessment results. Risk
1606 criteria may also describe how risk velocity, escalation, and elevation should be considered
1607 when determining risk severity and whether specific ICT risks meet the minimum threshold for
1608 enterprise-level discussion. For example, the enterprise may note shared risks that represent a
1609 broad threat that would benefit from centralized risk mitigation or a reputational risk that
1610 demands immediate preventative action.

1611 During normalization, risk managers review the results from the various risk registers to
1612 support consistent risk treatment and communication. A key element of normalization is the
1613 identification and resolution of cases in which a similar risk scenario is treated differently by
1614 different enterprise participants. The underlying reason should be understood, and the
1615 disparity should be recognized. Some examples of ICT risk normalization are described in Table
1616 10.

1617

Table 10. Examples of ICT risk normalization

Action	Description
De-duplicate and combine identical or similar risks	An external attacker deploys a remote access tool and uses it to exfiltrate the plans for the company's upcoming merger. External threat actors steal information about marketing plans through malicious code deployed in the sales department. Malicious parties plant a web shell in an external site that enables them to access documents stored in the Legal Affairs shared document folder, resulting in the loss of critical corporate information.
Reprioritize according to risk appetite, tolerance, and sensibilities	Since priorities have been established at organization and system levels, it may be necessary to review their collective priority and recommend adjustments to a higher or lower priority.
Resolve risk register disparities	One of two alternatives might be applied: - The combined risk description could be listed in the risk register for each risk response selected by system owners at lower levels. If two system owners had mitigated the above exfiltration risk and one had chosen to accept it, then the risk would appear in the combined risk register twice, with each row indicating the respective response. - The combined ICT risk would be included once in the risk register, with both responses included in the Risk Response Type column.
Adjudicate key risks	Risks that warrant tracking and further communication in the ERR are highlighted and reviewed by enterprise-level risk managers.

1618

1619

1620

1621

1622

1623

1624

1625

1626

1627

1628

1629

1630

The categories of each ICT risk in each register are likely to be limited and consistent, so that column provides a practical key for the initial sorting exercise. After all of the risks at a given level are combined, aggregation is a straightforward activity but may require some manual adjustment. Various risk owners will likely use differing risk descriptions for the same scenario. The risk manager of that business unit would transliterate these ICT risks into a single representative risk on the business unit's risk register, perhaps "External malicious party uses malicious code to exfiltrate sensitive business-related documents." In this case, the risk must describe the type of information that is at risk of theft, since the loss of internal business documents, patient healthcare records, and employee financial information might each represent differing likelihoods and impacts. The criteria for delineating these factors will be determined by each enterprise. For example, if sufficiently detailed risk appetite and risk tolerance statements have been recorded, they might provide input into those risk criteria.

1631

1632

1633

1634

1635

1636

The activities described in this document are solely intended to support public- and private-sector enterprise information gathering and reporting. Actions for an immediate response, escalation, or notification for any particular adverse event should be handled through the enterprise's incident response processes. Similarly, raw risk information from each risk register should be fully available for any manager's review. Aggregated summarization is a valuable reporting tool but should not impede the ability of managers to review specific risk decisions.

1637

1638

1639

1640

1641

Aggregating the risk analysis from multiple risk registers will vary by enterprise. For example, a three-point estimation could be used to complete the likelihood and impact columns on the combined register. The business unit risk manager could calculate these values using the lowest observed value as the best case, the highest value as the worst case, and the mean value of the others as the most likely. That manager could also apply their knowledge of the personnel and

processes used to generate the risk registers, such that if they know that a particularly detailed study had been performed to develop one or more of the estimates, it might influence the understanding of the most likely value.

5.2.3. Integrating Risk Register Details

For some enterprises, the aggregation of these risk analysis and risk response values may be more art than science. Some organizations have skilled practitioners with actuarial experience who can statistically aggregate multiple data points and draw a scientific conclusion about the likelihood and impact (and, therefore, exposure rating) of various risks. Other organizations will simply work to normalize a list of highs and lows, with risk managers using their best judgment to estimate the combined exposure. Because the process of analyzing and responding to risk factors is highly iterative, an enterprise might need to begin with qualitative risk values and identify opportunities to increasingly apply quantitative approaches as more information and history become available.

Information sharing and communications on risk response are vital as risk response could be ongoing, iterative, or span different reporting cycles. The information provides valuable data that will guide enterprise-level risk decisions, but the level of precision needed at higher hierarchical levels will likely be less than what is needed at the system level.

Completion of the remaining columns presents opportunities for enterprise determination as follows:

- For an aggregation of the risk response cost column, an organization-level risk manager may wish to record a statistically weighted average of the risk response costs. In other cases, the manager may wish to provide a total cost allocated across all subsidiary systems and organizations.
- The column for risk owners should indicate an organization-level representative who has the accountability and authority to manage that risk. Risk ownership is a key information point that must be carefully considered and applied. The party designated as the risk owner must be continually knowledgeable about relevant risk conditions and must also have accountability and authority to manage the risk. Since risk conditions may change as information is aggregated, responsibility and accountability should be periodically reviewed to ensure that the risk owner is the appropriate designee.
- The risk status for each aggregated ICT risk should use a consistent set of indicators. Status could be a simple indicator (e.g., open, closed, pending) or provide a more detailed explanation (e.g., "Risk accepted pending review by the Jan. 24 quarterly risk committee meeting").

While the methods and algorithms used will vary by enterprise, there should be a consistent risk aggregation strategy that is expressed as part of a policy within a given enterprise. Given the roll-up process, ICTRM — working in conjunction with enterprise risk managers — can include relevant risk policy statements, such as requirements for registering risks, providing updates regularly, and communicating risk activities with enterprise managers and leadership.

Through these procedures and policy statements, the various ICT risks are integrated into a comprehensive ERR. These processes are described as a bottom-up integration, but real-world scenarios are likely to be interactive and iterative. Integration is important for gathering data and provides opportunities for analysis and adjustment.

5.3. Adjusting Risk Responses

Based on the evaluation, risk managers adjust their risk response approach. In some cases, the evaluation will provide evidence that risk response has been effective and is efficiently achieving the necessary level of risk treatment. In other cases, adjustments may be necessary to risk direction, risk treatment, or both.

The composite set of enterprise risk likelihood and impact is something besides, and not necessarily equivalent to, the sum of the risk analyses described in the various risk registers.

As controls are applied throughout the enterprise and indicators are produced (and reported through metrics), various managers and leaders will consider the evaluation in the previous section. Given the resulting observations, several adjustments may be warranted, as described below:

- **Adjust strategic direction** — Based on collective results, senior leaders may update risk appetite statements to increase or decrease risk limits, including potentially adjusting a specific quantitative direction. In addition to or in place of risk appetite adjustment, risk tolerance interpretation may similarly be adjusted to take advantage of opportunities or to reduce the likelihood or impact of harmful risks.
- **Adjust risk responses** — To address inconsistent responses to risks or to achieve a different result, leaders may choose to direct specific response actions to one or more risk scenarios. For example, if some organizations decided to mitigate a given risk type and others chose to accept it, risk managers may clarify which treatment is the appropriate response (or clarify the criteria by which that decision is made). As with previous discussions, this adjustment may either be to reduce the overall exposure by enacting a more stringent response or to loosen restrictions to gain some advantage in exchange for a measured risk increase. Such changes may occur gradually to ensure sufficient ICTRM at all hierarchical levels.
- **Adjust KPIs and KRIs** — While the enterprise may adjust its specific direction or treatment of risk, the result of the evaluation will often be increased monitoring of the various conditions. Especially when conditions indicate broad variance in resulting metrics, managers may direct changes to the KPIs and KRIs that are monitored to gain better visibility. If changes to impact and likelihood cannot be adequately observed with the current indicators, then different (or additional) metrics may be justified. Increased frequency is indicated when impact and likelihood change more rapidly than the current monitoring interval.

The adjustments described are intended to provide improvements that are directly based on monitoring and evaluating risk results. Additional adjustments may be based on external

direction, such as requirements by a regulator for increased risk management or new reporting criteria (e.g., prohibiting sharing or disclosing information from a smart utility meter about a customer's usage without that customer's consent).

5.3.1. Factors Influencing Prioritization

Numerous factors (e.g., financial loss, enterprise reputation, shareholder sentiment) influence priority and should be included in the enterprise risk strategy. An ICT risk that directly impacts the mission is likely to be a high priority, but many other considerations — such as agency or corporate reputation — may move a particular type of risk to the top of the list. Another consideration could occur if a corporate entity were preparing for a merger. Recent examples that demonstrate the discovery of an ICT risk can affect the valuation of an enterprise and subsequent negotiations. There may also be factors that are not directly related to risk but that could support organizational improvement (e.g., quick wins that build team confidence and gain momentum, risks related to an objective that leaders have established as a key priority). Priority values such as low, moderate, and high are often used as risk prioritization categories. This qualitative approach may be more limiting than quantitative analysis in that it is easier to sort a range of numerical values — even those that are relatively close — than it is to sort a list of risks marked “Very High.” In most enterprises, risk strategy should provide direction for both generalization (e.g., low, moderate, high) and more specific risk prioritization methods.

5.3.2. ICT Risk Optimization

A key goal of ERM/ICTRM coordination is to help enterprise stakeholders collect various risk data for decision support, monitoring, and communications. Several foundational definitions are relevant to properly prioritizing risk at each stage of the life cycle, including aggregating and prioritizing the risk register data discussed in this document:

- **Risk aggregation** — The combination of a number of risks into one risk to develop a more complete understanding of the overall risk [ISO31073]
- **Risk criteria** — Terms of reference against which the significance of a risk is evaluated, such as organizational objectives, internal/external context, and mandatory requirements (e.g., standards, laws, policies) [ISO31073]
- **Risk optimization** — A risk-related process to minimize negative and maximize positive consequences and their respective probabilities; risk optimization depends on risk criteria, including costs and legal requirements

The processes to aggregate, prioritize, and optimize risk will be different at each level of the enterprise based on the risk criteria relevant to that level. At hierarchically lower levels in an enterprise, a certain amount of risk prioritization and treatment authority will have been delegated by the stated risk strategy guidelines to streamline operations, but there may need to be additional collaboration based on observations by those performing oversight at higher levels.

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

- **Fiscal optimization** — A straightforward ranking of risks in descending order from most impactful to least. Risk managers tally the total risk response costs until funding is exhausted.
- **Algorithmic optimization** — The application of mathematical formulas to calculate the aggregate cost-benefit to the enterprise in a purely mechanical approach, given the estimated costs. While risk can rarely be fully addressed only in numerical terms, a practitioner can often conduct an initial sort based on algebraic results, after which the results can be reviewed in context.
- **Operational optimization** — The selection of risks from the register that are most important to operations based on leadership preferences, mission objectives, and stakeholder sentiment. Operational coordination depends on an iterative communications cycle of risk reporting and analytics.
- **Forced ranking optimization** — Prioritizing risks in the way that will best use available resources to achieve the maximum benefit, given specific negative and positive consequences. Various business drivers and risk consequences have different weights for developing a score, helping to move beyond the simplistic “threat multiplied by vulnerability” approach to build business objectives into that equation. Because these factors and their weights are based on business drivers, the factors should be defined by senior stakeholders but can be applied at all levels of the enterprise, subject to adjustment and refinement. While forced ranking is often the default method of optimization, the methods above are equally valid and beneficial to the enterprise.

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

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

1797 **5.3.3. ICT Risk Priorities at Each Enterprise Level**

1798 In support of risk prioritization, as with ICT risks themselves, the ranking factors reflect the
1799 various strata of the enterprise. At the system level, the risk register reflects risk priorities
1800 related to particular systems and technologies. The organization level has priorities based on
1801 unique mission and business unit drivers. The enterprise has overarching ICT priorities that may
1802 not be the same as those at lower technical levels of abstraction, and they can be of varying
1803 priority when considered along with other enterprise risks. This balance is foundational to the
1804 concept of ICTRM as an input to ERM. While risks to institutional information and technology
1805 are critical parts of the enterprise and a primary focus of those charged with leading ICTRM,
1806 corporate officers and fiduciaries have a broad perspective and must balance the dozens of risk
1807 types in the enterprise risk universe. Bidirectional communication is critical, enabling senior
1808 leaders to convey strategy and direction while also enabling system- and business-level
1809 managers to keep leadership informed.

1810 This process does not mean that every system-level risk decision should be elevated to top
1811 leadership but rather that many risk decisions at the system and organization levels should be
1812 considered provisional and that leaders may subsequently recommend a different priority or
1813 approach based on their understanding of the aggregate impact to enterprise factors (e.g.,
1814 revenue, reputation, regulations, politics).

1815 **5.4. Enterprise Adjustments Based on ICT Risk Results**

1816 In many organizations, ICT enables a flexible approach to achieving the enterprise mission and
1817 ensuring stakeholder value. ICT aspects evolve rapidly, as does the ICT risk landscape, so
1818 periodic adjustments to ICTRM are likely to be needed. The Federal Government has observed
1819 that additional technical capabilities are often needed to provide better services to citizens
1820 even as agencies recognize the increased risk presented by the underlying technology. Budgets
1821 may need to be allocated for this emerging technology, and strict guidance on how to manage
1822 risk to that ICT may be provided. Subsequently, the results of previous iterations of the ICTRM
1823 cycle may support management decisions to adjust funding and risk parameters to achieve
1824 enterprise objectives.

1825 **5.4.1. Adjustments to ICT Program Budget Allocation**

1826 In both public- and private-sector enterprises, resource considerations are often described as a
1827 contributing factor for risk. To some extent, the claim that a program “needs more resources” is
1828 justifiable in that there are always more tools, personnel, and services that could be added.
1829 However, effective ICTRM requires a balance among risk optimization, resource optimization,
1830 and the value delivered by the technology being used to support mission objectives. If any of
1831 these three factors results in an imbalance, the solution is untenable. ICTRM informs the
1832 decisions around what areas receive priority within limited budget environments.

For example, because risk decisions are based on stakeholder needs (and the resulting enterprise and alignment objectives), ICT activities can be traced back to mission and business value.

In theory, one can simply build a business case that demonstrates the value proposition of investment in ICT protection, detection, and response resources. In reality, it can be quite challenging to directly report the subsequent return on that investment. One way to address this is by providing detailed risk assessment and reporting activities, such as those described in this document. Quantitative methods offer specific calculations that enable risk practitioners to simulate risk likelihood and financial impact before and after implementation of the ICT improvement. This then drives a straightforward cost-benefit analysis regarding the resource investment.

As managers and leaders review the activities performed and the risk results provided, they may identify opportunities to centrally fund and operate risk management activities that had previously been the responsibility of individual system owners. It might make fiscal sense to combine activities to gain efficiencies or reduce duplication. As such opportunities become apparent during the review of risk register reports and results, leaders may make fiscal adjustments to gain an advantage.

5.4.2. Adjustments to Risk Appetite and Risk Tolerance

Observations made during the life cycle may also provide feedback regarding leaders' risk criteria for risk appetite and tolerance. Fig. 14 illustrates several key decision points, including:

- Risk acceptance at the system level – In selecting the appropriate controls for a given information system (or shared set of controls), is a risk already acceptable, given the applicable risk tolerance statements?
 - If it is not acceptable, the system owner can apply additional risk responses, either through risk sharing or through mitigation by various controls.
 - At times, risk cannot be brought within tolerance through any combination of controls, or the cost of the controls might be unreasonable for the system. There may also be limited ability to adjust risk tolerance. Discussion with decision-makers is necessary to determine the appropriate course of action. That discussion might also support guidance for other enterprise systems facing similar risk scenarios.
- Additional decision points occur after the aggregation and integration of risk registers at various levels. As risk managers review the risk registers and RDRs, risk management results will be compared with stakeholder expectations. Based on the aggregated results, ICT risk managers might need to consider the following questions:
 - Is risk response consistent across various organizational structures and levels? Based on risk analysis, response, and monitoring results, risk managers may determine that additional guidance is needed to better achieve repeatable and reliable risk management activity. Adjustments in policy, procedure, staff

1872 training, and other governance components may be necessary to improve
1873 process maturity.

- 1874 ○ Has the risk environment evolved (e.g., due to new regulations or customer
1875 agreements) to such an extent that risk direction or criteria need to be adjusted?
1876 If so, this provides an opportunity to repeat the cycle.

1877 In addition to these programmatic adjustments, specific risk treatment adjustments might be
1878 identified during continuous monitoring and ongoing assessment activities.

1879 **5.4.3. Reviewing Whether Constraints Are Overly Stringent**

1880 A challenge for senior managers is ensuring that their organizations are permitting enough
1881 beneficial risks (e.g., opportunities, rewards). These introspective questions help those in risk
1882 governance roles identify whether their risk managers are using the risk governance tools and
1883 processes correctly or if those tools and processes need adjustment.

1884 It is rare that an opportunity can be realized without a negative risk. A basic objective of risk
1885 management programs is to identify individual negative risks so that they can be matched to
1886 their corresponding positive risks, enabling trade-off analysis. Once individual negative risks are
1887 identified, the risk program is prepared to move ahead with a risk response should the trade-off
1888 analysis render a decision to proceed with the positive risk.

1889 **5.4.4. Adjustments to Priority**

1890 A final program-level adjustment relates to enterprise priorities. ICT risk decisions flow from the
1891 enterprise mission and priorities. This is illustrated by Activity Point 1 in Fig. 13, where senior
1892 leaders establish the mission and priorities that drive strategic objectives and planning and are
1893 then used to direct ICTRM activities. Subsequently, identified and assessed risks are recorded in
1894 the risk register in accordance with those priorities. The order in which risks are addressed, the
1895 direction of appropriate response, and even the agreement about which risks will be addressed
1896 all derive from the enterprise priorities. For this reason, a key enterprise activity will be a
1897 periodic review of those priorities and the effects that they have on ICTRM. Based on the
1898 results of such reviews, priorities might be adjusted or clarified to ensure continued alignment
1899 between ICTRM activities and mission objectives.

1900

1901 6. Conclusion

1902 Consistent with CSF 2.0 and other federal guidelines, this publication reinforces the role of
1903 governance as the connective tissue between enterprise strategy and risk management
1904 execution. Effective enterprise risk management requires ICT risk to be treated as an integral
1905 component of an organization's broader risk portfolio. This publication has presented a
1906 framework for bridging the gap between ICT risk management disciplines (e.g., cybersecurity,
1907 privacy, supply chain, OT, IoT, SI) and enterprise-level decision-making to help senior leaders
1908 make informed, mission-aligned risk decisions. The document acknowledges the need for
1909 ongoing bidirectional communication between ERM and risk programs and recognizes that the
1910 risk disciplines both inform and receive direction from ERM. It shows that the communication
1911 of *risk appetite* statements from the ERM portfolio is a way for risk programs to better identify
1912 and monitor risks using a variety of related methods, such as *risk tolerance* statements, *key*
1913 *performance indicators*, *key risk indicators*, and *controls*. Similarly, this publication formalizes
1914 the use of *risk registers* to communicate risks and risk responses among program and portfolio
1915 levels. Risk registers are the foundational mechanism for capturing, normalizing, and
1916 aggregating ICT risk information across organizational levels. When maintained and
1917 communicated effectively, these registers provide the information necessary to construct
1918 enterprise risk profiles that reflect a holistic view of negative risks and positive opportunities.

1919 **References**

- 1920 [AIRMF] NIST Artificial Intelligence (AI) Risk Management Framework. Available at
1921 <https://www.nist.gov/itl/ai-risk-management-framework>
- 1922 [COSOERM] Committee of Sponsoring Organizations (COSO) of the Treadway
1923 Commission (2017) Enterprise Risk Management—Integrating with
1924 Strategy and Performance, Executive Summary. Available at
1925 [https://www.coso.org/files/ugd/3059fc_61ea5985b03c4293960642fdce](https://www.coso.org/files/ugd/3059fc_61ea5985b03c4293960642fdce408eaa.pdf)
1926 [408eaa.pdf](https://www.coso.org/files/ugd/3059fc_61ea5985b03c4293960642fdce408eaa.pdf)
- 1927 [CSCRM] The NIST Cybersecurity Supply Chain Risk Management project links and
1928 publication descriptions. Available at [https://csrc.nist.gov/Projects/cyber-](https://csrc.nist.gov/Projects/cyber-supply-chain-risk-management)
1929 [supply-chain-risk-management](https://csrc.nist.gov/Projects/cyber-supply-chain-risk-management)
- 1930 [DTEF] ISACA. (2024). Digital trust ecosystem framework.
1931 <https://www.isaca.org/digital-trust>
- 1932 [GREENBOOK] U.S. Government Accountability Office (GAO) (2014) Standards for
1933 Internal Control in the Federal Government. Available at
1934 <https://www.gao.gov/assets/670/665712.pdf>
- 1935 [IEC31010] International Electrotechnical Commission (IEC) (2019) Risk management
1936 – Risk assessment techniques. IEC 31010:2019. Available at
1937 <https://www.iso.org/standard/72140.html>
- 1938 [IR8170] Marron J, Pillitteri V, Boyens J, Quinn S, Witte G, Feldman L (2020)
1939 Approaches for Federal Agencies to Use the Cybersecurity Framework.
1940 (National Institute of Standards and Technology, Gaithersburg, MD), NIST
1941 Interagency or Internal Report (IR) NIST IR 8170-upd.
1942 <https://doi.org/10.6028/NIST.IR.8170-upd>
- 1943 [IR8286] Quinn SD, Chua J, Ivy N, Gardner RK, Kent KA, Smith MC, Witte GA (2025)
1944 Integrating Cybersecurity and Enterprise Risk Management (ERM).
1945 (National Institute of Standards and Technology, Gaithersburg, MD), NIST
1946 Interagency or Internal Report (IR) NIST IR 8286r1.
1947 <https://doi.org/10.6028/NIST.IR.8286r1>
- 1948 [IR8286A] Quinn SD, Ivy N, Barrett M, Feldman L, Witte GA, Gardner RK (2025)
1949 Identifying and Estimating Cybersecurity Risk for Enterprise Risk
1950 Management. (National Institute of Standards and Technology,
1951 Gaithersburg, MD), NIST Interagency Report (IR) NIST IR 8286Ar1.
1952 <https://doi.org/10.6028/NIST.IR.8286Ar1>
- 1953 [IR8286D] Quinn SD, Ivy N, Chua J, Barrett MP, Feldman L, Topper D, Witte GA,
1954 Gardner RK (2025) Using Business Impact Analysis to Inform Risk
1955 Prioritization and Response. (National Institute of Standards and
1956 Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR)
1957 NIST IR 8286D-upd1. Includes updates as of Feb. 26, 2025.
1958 <https://doi.org/10.6028/NIST.IR.8286D-upd1>
- 1959 [ISACA] “Risk Capacity,” ISACA Glossary. Available at
1960 <https://www.isaca.org/en/resources/glossary#glossr>

1961	[ISO31000]	International Organization for Standardization (ISO) (2018) Risk management— Guidelines. ISO 31000:2018. Available at https://www.iso.org/standard/65694.html
1962		
1963		
1964	[ISO31073]	International Organization for Standardization (ISO) (2022)
1965		Risk management — Vocabulary. ISO 31073:2022.
1966		Available at https://www.iso.org/standard/79637.html
1967	[NISTCSF]	The NIST Cybersecurity Framework for understanding and improving management of cybersecurity risk. Available at https://www.nist.gov/cyberframework
1968		
1969		
1970	[NISTIoT]	The NIST program for the Cybersecurity of the Internet of Things (IoT). Available at https://www.nist.gov/internet-things-iot
1971		
1972	[NISTPF]	The NIST Privacy Framework, a tool to help organizations improve individuals' privacy through enterprise risk management. Available at https://www.nist.gov/privacy-framework
1973		
1974		
1975	[NISTRMF]	The NIST Risk Management Framework (RMF) is available at https://csrc.nist.gov/projects/risk-management
1976		
1977	[OMB-A11]	Office of Management and Budget (2025) OMB Circular No. A-11, Preparation, Submission, and Execution of the Budget. (The White House, Washington, DC), OMB Circular No. A-11, August 2025. Available at https://www.whitehouse.gov/wp-content/uploads/2025/08/a11.pdf
1978		
1979		
1980		
1981	[OMB-A123]	Office of Management and Budget (2016) OMB Circular No. A-123, Management's Responsibility for Internal Control. (The White House, Washington, DC), March 10, 2026. Available at https://www.whitehouse.gov/wp-content/uploads/2026/03/OMB-Circular-No.-A-123-2026.pdf
1982		
1983		
1984		
1985		
1986	[OMB-A130]	Office of Management and Budget (2016) OMB Circular No. A-130, Managing Information as a Strategic Resource. (The White House, Washington, DC), July 28, 2016. Available at https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf
1987		
1988		
1989		
1990		
1991	[OPENFAIR]	The Open Factor Analysis of Information Risk (FAIR) Body of Knowledge is comprised of the Open Group Risk Analysis standard (https://publications.opengroup.org/c13g) and the Open Group Risk Taxonomy (https://publications.opengroup.org/c13k).
1992		
1993		
1994		
1995	[PLAYBOOK]	Chief Financial Officers Council (CFOC) and Performance Improvement Council (PIC) (2022) Playbook: Enterprise Risk Management for the U.S. Federal Government. Available at https://www.agacgfm.org/wp-content/uploads/legacy/Resources/intergov/ERMHub/GuidanceResearch/erm-playbook-2022-update-final-508-compliant.pdf
1996		
1997		
1998		
1999		
2000	[SP80053]	Joint Task Force (2022) Assessing Security and Privacy Controls in Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53A, Rev. 5. https://doi.org/10.6028/NIST.SP.800-53Ar5
2001		
2002		
2003		

2004	[SP800161]	Boyens J, Smith A, Bartol N, Winkler K, Holbrook A, Fallon M (2022) Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-161r1. https://doi.org/10.6028/NIST.SP.800-161r1
2005		
2006		
2007		
2008	[SP800221A]	Quinn S, Ivy N, Chua J, Scarfone K, Barrett M, Feldman L, Topper D, Witte G, Gardner RK (2023) Information and Communications Technology (ICT) Risk Outcomes: Integrating ICT Risk Management Programs with the Enterprise Risk Portfolio. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-221A. https://doi.org/10.6028/NIST.SP.800-221A
2009		
2010		
2011		
2012	[SP1308]	NIST Cybersecurity Framework 2.0: Cybersecurity, Enterprise Risk Management, and Workforce Management Quick-Start Guide. (2024) (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 1308. https://doi.org/10.6028/NIST.SP.1308
2013		
2014		
2015		
2016	[SP80030]	Joint Task Force Transformation Initiative (2012) Guide for Conducting Risk Assessments. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-30, Rev. 1. https://doi.org/10.6028/NIST.SP.800-30r1
2017		
2018		
2019		
2020		
2021		
2022		
2023		

2024 **Appendix A. Acronyms and Abbreviations**

2025 Selected acronyms and abbreviations used in this paper are defined below.

2026 **BIA**

2027 Business Impact Analysis

2028 **CFO**

2029 Chief Financial Officer

2030 **CFOC**

2031 Chief Financial Officers Council

2032 **CISO**

2033 Chief Information Security Officer

2034 **COSO**

2035 Committee of Sponsoring Organizations

2036 **CPRT**

2037 Cybersecurity and Privacy Reference Tool

2038 **C-SCRM**

2039 Cybersecurity Supply Chain Risk Management

2040 **CVSS**

2041 Common Vulnerability Scoring System

2042 **ERM**

2043 Enterprise Risk Management

2044 **ERP**

2045 Enterprise Risk Profile

2046 **ERR**

2047 Enterprise Risk Register

2048 **FAIR**

2049 Factor Analysis of Information Risk

2050 **FISMA**

2051 Federal Information Security Modernization Act

2052 **GAO**

2053 U.S. Government Accountability Office

2054 **GRC**

2055 Governance, Risk, and Compliance

2056 **HVA**

2057 High Value Asset

2058 **ICT**

2059 Information and Communications Technology

2060 **ICTRM**

2061 Information and Communications Technology Risk Management

2062	IEC
2063	International Electrotechnical Commission
2064	IoT
2065	Internet of Things
2066	IR
2067	Interagency or Internal Report
2068	ISO
2069	International Organization for Standardization
2070	ITL
2071	Information Technology Laboratory
2072	KPI
2073	Key Performance Indicator
2074	KRI
2075	Key Risk Indicator
2076	MEA
2077	Monitor-Evaluate-Adjust
2078	NIST
2079	National Institute of Standards and Technology
2080	NOAA
2081	National Oceanic and Atmospheric Administration
2082	OLIR
2083	Online Informative References (Program)
2084	OMB
2085	Office of Management and Budget
2086	OT
2087	Operational Technology
2088	PIC
2089	Performance Improvement Council
2090	PII
2091	Personally Identifiable Information
2092	RDR
2093	Risk Detail Record
2094	SEC
2095	U.S. Securities and Exchange Commission
2096	SP
2097	Special Publication
2098	SWOT
2099	Strengths, Weaknesses, Opportunities, Threats

2100 Appendix B. Notional Example of a Risk Detail Record (RDR)

2101 In support of an ICT risk register, a risk detail record (RDR) enables the communication of
2102 additional information. As shown in the following notional example, an RDR may help provide
2103 information regarding each risk, relevant stakeholders, date and schedule considerations, and
2104 planned activities.

Notional Risk Detail Record		
Risk ID numbers		
System affected		
Organization or business unit		
Risk scenario description		
Assets affected		
Threat sources/actors (with intent? with motivation?)		
Threat vectors		
Threat events		
Vulnerability/predisposing conditions		
Primary adverse impact (be sure to reconcile impact vs. consequences)		
Secondary adverse impacts		
Other scenario details		
Risk category		
Current risk analysis		
Likelihood before controls (%):	Impact before controls (\$):	Exposure rating before controls (\$):
Planned residual risk response	Select all that apply: ☐ Accept ☐ Avoid ☐ Transfer ☐ Mitigate	
Planned risk response description		
Resource requirements for planned risk response		
Planned response cost (\$)		
Likelihood after controls will be (%):	Impact (\$):	Expected exposure rating (\$):
Residual risk response as implemented	Actual response cost (\$):	
After controls are in place, measured likelihood is (%):	Impact (\$):	Final exposure rating (\$):
Risk owner/point of contact		
Date of risk identification		
Source of risk information		
Current status date		
Dependencies		
Follow-up date		
Comments		

Fig. 15. Notional risk detail record

2105
2106 JSON-based digital expressions of the risk register and the RDR notional template with
2107 examples are available as [supplemental material to the NIST IR 8286 series](#).

2108 Appendix C. Federal Agency-Specific Guidelines for ICTRM

2109 OMB Circular A-123 states, “Risk must be analyzed in relation to achievement of the strategic
2110 objectives established in the Agency strategic plan (see OMB Circular No. A-11, Section 230), as
2111 well as risk in relation to appropriate operational objectives. Specific objectives must be
2112 identified and documented to facilitate identification of risks to strategic, operations, reporting,
2113 and compliance” [OMB-A123].

2114 Table 11 illustrates similarities among several common risk management models, including
2115 establishing context, identifying risks, analyzing risks, estimating risk importance, determining
2116 and executing risk response, and monitoring and responding to changes over time.

2117 **Table 11. Similarities among selected ERM and risk management documents**

ERM Playbook	COSO ERM Framework	ISO 31000:2018		OMB A-123	GAO Green Book
Identify the Context	Governance and Culture Strategy and Objective Setting	Establish External Context (5.3.2), Establish Internal Context (5.3.3)		Establish Context	Define objectives and risk tolerances (6.01)
Identify the Risks	Performance Review and Revision Information, Communication, and Reporting	Risk Assessment	Risk Identification (5.4.2)	Identify Risks	Identification of Risks (7.02)
Analyze the Risks			Risk Analysis (5.4.3)	Analyze and Evaluate	Analysis of Risks (7.05)
Assess Likelihood			Calculate Level of Risk		Management estimates the significance of a risk and considers the magnitude of impact, the likelihood of occurrence, and the nature of the risk
Assess Impact					
Prioritize Risks					
Calculate Exposure		Risk Evaluation (5.4.4)	Develop Alternatives		
Plan and Execute Response Strategies				Risk Treatment (5.5)	
Monitor, Evaluate, and Adjust	Performance Review and Revision Information, Communication, and Reporting	Monitoring and Review (5.6)		Monitor and Review	Identification of Change (9.02)
					Analysis of and Response to Change (9.04)

2118
2119 The entries in Table 11 indicate the identifier or section number from the source material in
2120 parentheses, whenever available. Table 11 provides a high-level comparison and is not
2121 intended to be a crosswalk for relationships among the models but rather show that risk

2122 management disciplines that aggregate into the ERM process follow similar steps to manage
2123 risk.

2124 The resources in Table 11 are from:

- 2125 • Committee of Sponsoring Organizations of the Treadway Commission (COSO) *Enterprise*
2126 *Risk Management – Integrating with Strategy and Performance* Framework [COSOERM]
- 2127 • International Organization for Standardization (ISO) 31000, *Risk Management* standard
2128 [ISO31000]
- 2129 • U.S. Office of Management and Budget (OMB) *Circular No. A-123 – Management’s*
2130 *Responsibility for Internal Control* [OMB-A123]
- 2131 • U.S. Chief Financial Officers Council (CFOC) and Performance Improvement Council (PIC)
2132 *Playbook: Enterprise Risk Management for the U.S. Federal Government (or ERM*
2133 *Playbook)* [PLAYBOOK].

2134 This document uses the processes of the ERM Playbook (column 1 in Table 11) as a basis for
2135 describing the ICTRM life cycle and explaining how ICTRM integrates with ERM at a high level.
2136 This is not meant to imply that all enterprises should use these steps; enterprises should
2137 determine and apply the appropriate approach to achieve ICTRM/ERM integration,
2138 communication, and monitoring.

Appendix D. Change Log

Table 12. Changes from the Original Publication

EDIT TYPE	CHANGE	LOCATION
Revision	Revised the Executive Summary for brevity and to reflect updated content from throughout the publication.	Executive Summary
Revision	Updated references to U.S. Office of Management and Budget documents, to OMB Circular A-123.	All
Addition	New paragraph inserted on CSF 2.0 alignment: document updated to align with NIST CSF 2.0 and its new Govern function, governance central to risk management. Also added pointers to the NIST Online Informative Reference (OLIR) resources.	Sec. 1.1
Revision	Added “safety” to the sentence describing ERM’s primary purpose	Sec. 2.1, last paragraph
Deletion	Removed Table 1 ("Similarities among selected ERM and risk management documents") and its surrounding material. Sec. 2.2 now opens directly with the six-step life cycle.	Sec. 2.2
Revision	"Based on this guidance, each discipline..." → "Based on these guidelines, each discipline..."	Sec. 2.3
Addition	Clarified examples of emerging conditions: "such as increased use of SI, increased dependence on external service providers, and integration of automated sensor systems further increase this complexity."	Sec. 2.4.1
Revision	Sec. 2.4.6 regarding positive risk has been retitled and largely rewritten for clarity.	Sec. 2.4.6 heading
Addition	Updated Sec. 3.1.1 to reflect the increased governance outcomes in NIST CSF 2.0.	Sec. 3.1.1
Addition	Added a new Sec. 3.2, "Risk Culture"	Sec. 3.2 (new)
Addition	New paragraph on risk capacity inserted, with COSO definition and quote.	Sec. 3.2.1
Addition	New paragraph on workforce considerations citing NIST SP 1308 (CSF 2.0 Workforce Management Quick-Start Guide) and using the register for workforce/gap analysis.	Sec. 3.3.5
Addition	Added a new Appendix C to detail some ERM aspects that specifically apply to Federal agencies. Moved numerous references to federal-specific considerations to the new Appendix.	Appendix C
Addition	Added Change Log	Appendix D