NIST Special Publication
NIST SP 800-221A

Information and Communications Technology (ICT) Risk Outcomes

Integrating ICT Risk Management Programs with the Enterprise Risk Portfolio

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

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

NATIONAL INSTITUTE OF
STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

NIST Special Publication
NIST SP 800-221A

Information and Communications Technology (ICT) Risk Outcomes

Integrating ICT Risk Management Programs with the Enterprise Risk Portfolio

Stephen Quinn
Applied Cybersecurity Division
Information Technology Laboratory

Nahla Ivy
Enterprise Risk Management Office
Office of Financial Resource Management

Julie Chua
Office of Information Security
Office of the Chief Information Officer (OCIO)
U.S. Department of Health and Human Services

Karen Scarfone
Scarfone Cybersecurity

Matthew Barrett
CyberESI Consulting Group, Inc.

Larry Feldman
Daniel Topper
Greg Witte
Huntington Ingalls Industries

R. K. Gardner
New World Technology Partners

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

November 2023

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology (NIST), nor is it intended to imply that the entities, materials, or equipment 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, Fair Use, and Licensing Statements
NIST Technical Series Publication Identifier Syntax

Publication History

Approved by the NIST Editorial Review Board on 2023-10-18

How to Cite this NIST Technical Series Publication:

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

Author ORCID iDs

Stephen D. Quinn: 0000-0003-1436-684X
Nahla Ivy: 0000-0003-4741-422X
Karen Scarfone: 0000-0001-6334-9486
Matthew Barrett: 0000-0002-7689-427X
Larry Feldman: 0000-0003-3888-027X
Daniel Topper: 0000-0003-2612-7547
Gregory A. Witte: 0000-0002-5425-1097

Contact Information

ictrm@nist.gov

National Institute of Standards and Technology
Attn: Applied Cybersecurity Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930

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

Abstract

The increasing frequency, creativity, and severity of technology attacks means that all enterprises should ensure that information and communications technology (ICT) risk is receiving appropriate attention within their enterprise risk management (ERM) programs. Specific types of ICT risk include, but are not limited to, cybersecurity, privacy, and supply chain. This document provides a framework of outcomes that applies to all types of ICT risk. It complements NIST Special Publication (SP) 800-221, *Enterprise Impact of Information and Communications Technology Risk*, which focuses on the use of risk registers to communicate and manage ICT risk.

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; ICT Risk Outcomes Framework (ICT ROF); 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.

Audience

The primary audience for this publication includes both Federal Government and non-Federal Government professionals at all levels who understand ICT but may be unfamiliar with the details of ERM. The secondary audience includes both Federal and non-Federal Government corporate officers, high-level executives, ERM officers and staff members, and others who understand ERM but may be unfamiliar with the details of ICT.

Acknowledgments

The authors wish to thank all individuals, organizations, and enterprises that contributed to the creation of this document. This includes Jim Foti, Amy Mahn, Matt Scholl, Kevin Stine, and Isabel Van Wyk of NIST and Mat Heyman of Impresa Management Solutions. The authors appreciate the support of the United States Department of Health and Human Services and the

Federal Cyber-ERM Community of Interest, including the following members who provided specific comments: Cedric Carter Jr., L. Dix, Ken Hong Fong, Kim Isaac, Z. Kaptaine, Nnake Nweke, Khairun Pannah, Katherine Polevitzky, Thom Richison, Nicole Rohloff, C. Rosu, Stephanie Saravia, M. Sawyer, and Angelica Stanley. The authors also thank Joel Crook of Consolidated Nuclear Security, LLC; Justin Perkins of CTIA; Kelly Hood of Optic Cyber Solutions; and Matthew Smith of Seemless Transition, LLC; and individual commenters Simon Burson and Chuck Shriver.

Document Conventions

For the purposes of this publication, “assets” are defined as technologies that may compose an information or communications system. The term “asset” or “assets” is used in multiple frameworks and documents. Examples include laptop computers, desktop computers, servers, sensors, data, mobile phones, tablets, routers, and switches. In instances where the authors mean “assets” as they appear on a balance sheet, the word “asset” will be preceded by words such as “high-level,” “balance sheet,” or “Level 1” to differentiate context.

Patent Disclosure Notice

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

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

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

Table of Contents

List of Tables

List of Figures

1. Introduction

The increasing frequency, creativity, and severity of attacks against technology means that all enterprises should ensure that information and communications technology (ICT) risk is receiving appropriate attention within their enterprise risk management (ERM) programs. Specific types of ICT risk include, but are not limited to, cybersecurity, privacy, supply chain, and artificial intelligence risk.

1.1 Purpose and Scope

This document provides a framework of outcomes that applies to all types of ICT risk. It complements NIST Special Publication (SP) 800-221, *Enterprise Impact of Information and Communications Technology Risk* [SP800221], which focuses on the use of risk registers to communicate and manage ICT risk. Before reading this publication, you should first read NIST SP 800-221 so that you understand the concepts and context for the information contained in the framework of outcomes.

NIST has already defined outcome-based frameworks for several types of ICT risk, including the Cybersecurity Framework [CSF], the Privacy Framework [PF], and the Secure Software Development Framework [SSDF]. The outcomes in those frameworks are effectively more specific instances of the outcomes in the more general framework defined in this publication.

1.2 Publication Contents

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

- Section 2 provides an overview of ICT processes as a context for ERM.
- Section 3 defines the framework of ICT risk outcomes and explains the significance of each field within the framework.
- The References section defines the references cited in this publication.
- Appendix A contains acronyms used in the publication.

2. Information and Communications Technology Areas

ERM is the highest terminus of ICT risk management (ICTRM). As with NIST SP 800-221, the processes described within this publication focus on ICTRM within, between, and across ICT areas. ICTRM helps ensure that leaders and stakeholders are supported by a holistic risk risk monitoring and communication model, which is needed for the complexity of risks at the enterprise level.

An ICT Risk Outcomes Framework (ROF) is needed to support ICT risk escalation and elevation, as well as reduce ICTRM complexity. While the focus of many risk management program frameworks is the comprehensiveness of each program's controls, the ICT ROF focuses on the comprehensiveness of overarching risk governance and management. Specifically, the ICT ROF enumerates distinct outcomes associated with the ICTRM process described in NIST SP 800-221 and illustrated in **Fig. 1**.

The **risk governance outcomes** of the ICT ROF are meant to be applied at select levels in a given organization. Typically, risk governance will occur at the enterprise level, and may also occur at the organization level.

The **risk management outcomes** of the ICT ROF may be applied at all levels in a given organization. The risk management outcomes are highly relevant to individual risk management programs and may be used alongside risk management program frameworks.

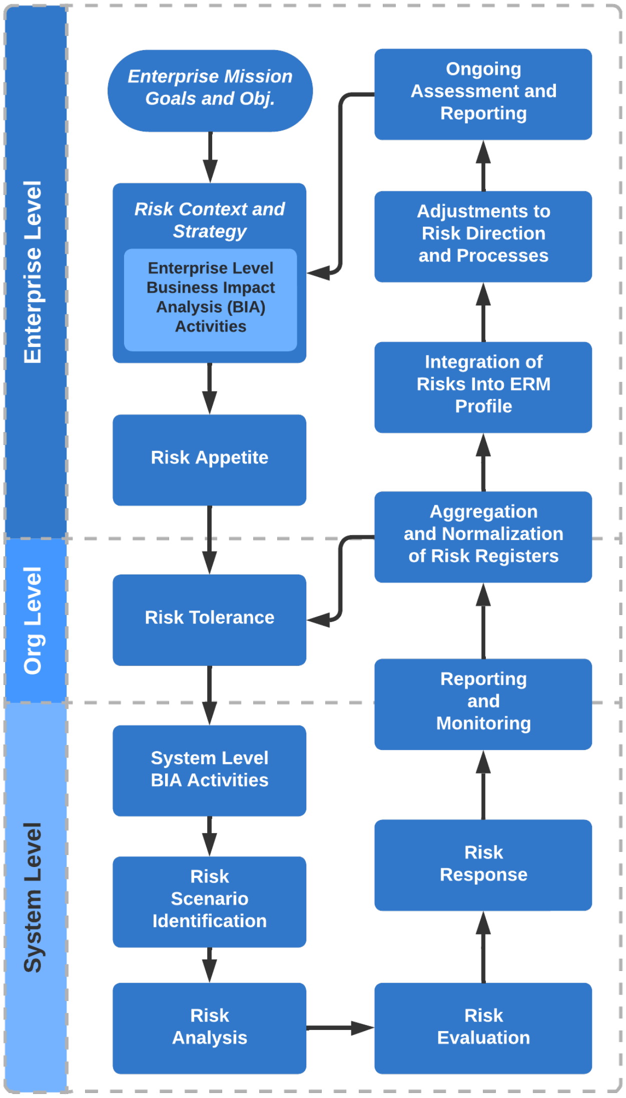
Enterprise Level
Org Level
System Level
Enterprise Mission Goals and Obj.
Risk Context and Strategy
Enterprise Level Business Impact Analysis (BIA) Activities
Risk Appetite
Risk Tolerance
System Level BIA Activities
Risk Scenario Identification
Risk Analysis
Risk Evaluation
Risk Response
Reporting and Monitoring
Aggregation and Normalization of Risk Registers
Integration of Risks Into ERM Profile
Adjustments to Risk Direction and Processes
Ongoing Assessment and Reporting

Fig. 1. ICTRM Process

3. ICT Risk Outcomes Framework (ROF)

This section defines the ICT ROF, a framework for integrating ICT risk with enterprise risk. The ICT ROF is a set of desired outcomes and applicable references that are common across all types of ICT risk. It provides a common language for understanding, managing, and expressing ICT risk to internal and outside stakeholders. It can be used to help identify and prioritize actions for reducing ICT risk, and it is a tool for aligning policy, business, and technological approaches to managing that risk. Using the framework for each type of ICT risk will help organizations improve the quality and consistency of ICT risk information they provide as inputs to their ERM programs. That, in turn, will help organizations address all forms of ICT risk more effectively in their ERM.

The ICT ROF is comprised of the following components:

- **Functions** organize ICT risk outcomes at their highest level. There are two Functions:
    - **Govern (GV):** Develop and implement the organizational business logic for risk management, and ensure risk management is performed according to that business logic.
    - **Manage (MA):** Continuously identify and address risks in accordance with the organization's risk management policies, processes, and priorities.
- **Categories** are the subdivisions of a Function into groups of ICT risk outcomes closely tied to programmatic needs and particular activities. Examples of Categories include:
    - Roles and Responsibilities (GV.RR)
    - Risk Analysis (MA.RA)
    - Risk Monitoring, Evaluation, and Adjustment (MA.RM)
- **Subcategories** further divide a Category into specific outcomes of technical and/or management activities. While not exhaustive, they help support achievement of the outcomes in each Category. Examples of Subcategories include:
    - GV.RR-1: Risk governance roles and responsibilities are established and communicated.
    - MA.RA-1: The likelihood of each risk event is estimated using risk assessment techniques and probability models.
    - MA.RM-4: When risk exceeds risk tolerance, changes to risk responses are identified and planned.
- **Implementation Examples** are one or more notional examples of how tools, processes, or other methods could be used to help achieve a Subcategory. No examples or combination of examples are required, and the stated examples are not the only feasible options. Some examples may not be applicable to certain organizations and situations. Examples of Implementation Examples include:
    - For GV.RR-1: An organization establishes which roles are responsible for documenting risk appetite and policy, as well as performing risk oversight.

  - For MA.RA-1: Bayesian models, event tree analysis, or similar techniques are used to determine the likelihood of a risk, and that information is recorded in the Current Assessment – Likelihood field in a risk register.
  - For MA.RM-4: KRIs are monitored to determine when risk exceeds risk tolerance, resulting in updates to the risk register and planning of a revised risk response, risk response type, risk response cost, and/or risk response description.
- **Informative References** are specific sections of standards, guidelines, and practices that illustrate methods to achieve the outcomes associated with each Subcategory. The Informative References are intended to be illustrative and not exhaustive. To avoid having to re-release this publication every time an Informative Reference is added or updated, Informative References are omitted from this publication. Instead, they will be held in NIST's Online Informative References (OLIR) Catalog.

For ease of use, each Function, Category, and Subcategory is assigned a unique identifier. **Table 1** lists the identifiers for the Functions and Categories to show the framework's overall structure.

Table 1. Function and Category Unique Identifiers

Function	Category
GOVERN (GV)	Context (GV.CT)
	Roles and Responsibilities (GV.RR)
	Policy (GV.PO)
	Benchmarking (GV.BE)
	Communication (GV.CO)
	Adjustments (GV.AD)
	Oversight (GV.OV)
MANAGE (MA)	Risk Identification (MA.RI)
	Risk Analysis (MA.RA)
	Risk Prioritization (MA.RP)
	Risk Response (MA.RR)
	Risk Monitoring, Evaluation, and Adjustment (MA.RM)
	Risk Communication (MA.RC)
	Risk Improvement (MA.IM)

Table 2 defines the Functions, Categories, Subcategories, and Implementation Examples in the ICT ROF and is available for browsing and download at the Cybersecurity and Privacy Tool (CPRT) page. **Table 2** includes only a subset of what an organization may need to do and achieve. The information in the table is space-constrained; much more information can be found from the Informative References in the NIST OLIR Catalog. Note that the order of the Functions, Categories, and Subcategories in the table is not intended to imply the sequence of implementation or the relative importance of any Function, Category, or Subcategory.

Please note that Implementation Examples are offered to provide clarification of the Subcategory. The information in the Implementation Example field represents a way in which the Subcategory might be satisfied but is not exhaustive of all possible ways.

Table 2. ICT Risk Outcomes Framework

Function	Category	Subcategory	Implementation Example
GOVERN (GV): Develop and implement the organizational business logic for risk management, and ensure risk management is performed according to that business logic.	**Context (GV.CT):** The organization's risk context, including mission, mission priorities, stakeholders, objectives, and direction, is understood.	**GV.CT-1:** Organizational mission, vision, and authorities are understood and considered.	An organization builds upon statute and authorities thereof to develop its two-year mission and five-year vision statements.
		GV.CT-2: Internal and outside stakeholder groups that affect or are affected by the organization are identified.	An organization periodically inventories groups of people that affect, and are affected by, the organization.
		GV.CT-3: The priorities, expectations, and effects of internal and external stakeholder groups are understood and considered.	An organization understands and considers stakeholder expectations such as: - Cultural expectations of employees - Achievement expectations of officers and directors - Privacy expectations of customers - Business expectations of partners - Compliance expectations of regulators - Ethics expectations of society
		GV.CT-4: Organizational charter, expectations, and objectives are aligned, prioritized, and communicated.	As part of annual strategic planning, an organization performs a strengths, weaknesses, opportunities, and threats (SWOT) analysis to determine near-term and long-term objectives, risks, and risk appetite. The objectives, risks, and risk appetite are documented and communicated in the form of a strategy.
		GV.CT-5: Mission/business functions and criticality are communicated.	Risk activities account for mission/business impact in the Impact field of the risk register, and account for mission/business criticality in the business impact analysis (BIA).
	Roles and Responsibilities (GV.RR): Positions, duties, and authorities for risk governance and management are established and communicated.	**GV.RR-1:** Risk governance roles and responsibilities are established and communicated.	An organization establishes which roles are responsible for documenting risk appetite and policy, as well as performing risk oversight.
		GV.RR-2: Risk management roles and responsibilities are established and communicated.	An organization establishes which roles are responsible for extending risk appetite into risk tolerance, as well as identifying, prioritizing, responding to, monitoring, evaluating, and adjusting risk.
	Policy (GV.PO): The policies to manage and monitor the organization's regulatory, legal, risk, environmental, and	**GV.PO-1:** Risk management stances, activities, appetites, roles, and authorities are established and communicated.	An organization authors and disseminates a risk management policy that declares stances (what the organization will, and will not, do), activities related to those stances, risk limitations using risk appetite

Function	Category	Subcategory	Implementation Example
	operational requirements are understood.		statements, and expectations and authorities associated with key roles such as the Chief Executive Officer, Chief Financial Officer, Chief Risk Officer, and Chief Information Security Officer.
		GV.PO-2: Organizational stances, activities, roles, and authorities that affect, and are affected by, risk management are aligned with risk policies and appetite.	An organization considers risk policies and risk appetite statements when developing policies that affect/support risk management. When developing policies that are affected by risk management, an organization aligns those policies with risk policies and risk appetite statements.
	Benchmarking (GV.BE): Methods, criteria, and expectations for discovering and distinguishing risk are established, communicated, and followed.	**GV.BE-1:** High-level organizational risks are periodically catalogued, categorized, and communicated.	Annually, an organization uses enterprise risk scenarios as a basis for adjusting the high-level risks represented in a risk breakdown structure.
		GV.BE-2: Risk appetite statements are developed and periodically communicated to risk management programs.	As a part of annual strategic planning, a corporation determines its risk appetite and communicates its risk appetite statements to risk management programs via a strategic plan.
		GV.BE-3: Risk tolerance statements are created as more specific translations of risk appetite statements and communicated to risk management programs as a basis for identifying risk.	An organization translates risk appetite statements into more specific, measurable, and broadly understandable risk tolerance statements in preparation to distribute the labor of risk management across a team of personnel.
		GV.BE-4: Risk scenarios that describe assets, threats, vulnerabilities, probabilities, and impacts are crafted and communicated.	Annually, an organization creates and refines anticipated enterprise risk scenarios as a basis for adjusting the high-level risks represented in a risk breakdown structure.
	Communication (GV.CO): Methods, criteria, and schedules for expressing and explaining risk are established, communicated, and followed.	**GV.CO-1:** Mandatory and voluntary disclosure decisions are informed through an enterprise risk profile and performed on a scheduled or as-needed (e.g., incident disclosure) basis.	Information from the enterprise risk register (ERR) forms the basis for a quarterly enterprise risk profile (ERP) update and informs quarterly and annual public disclosures. A data breach involving protected health information (PHI) triggers mandatory reporting to PHI owners and regulators.
		GV.CO-2: An enterprise risk communication format is established, communicated, and used as the basis for communication with risk management programs.	An ERR and standardized values and instructions for ERR fields are created, occasionally updated, and communicated to risk management programs as the expected risk reporting format.

Function	Category	Subcategory	Implementation Example
		GV.CO-3: Criteria for immediate and periodic escalation and elevation of program risks are established, communicated, understood, and used as the basis for risk communication.	An ERM committee documents and communicates criteria to the risk management programs for periodically and immediately: - communicating risk status of the next Level (i.e., escalation) and - transferring risk ownership to the next Level (i.e., elevation).
	Adjustments (GV.AD): Risk governance is adapted based on changes in organizational objectives, risk exposure, and residual risk.	**GV.AD-1:** Risk appetite is adjusted based on changes in organizational objectives, risk exposure, and residual risk.	An organization's annual strategic planning refines organizational objectives and risk appetite based on known risk exposure and residual risk.
		GV.AD-2: Strategic opportunities (aka positive risks) are adjusted based on changes in organizational objectives, risk exposure, and residual risk.	Among other things, risk exposure and residual risk from the risk register are considered in trade-off analysis with opportunities, and adjustments may be made to opportunity scope.
		GV.AD-3: Strategic priorities are adjusted based on changes in organizational objectives, risk exposure, and residual risk.	Among other things, risk exposure and residual risk from the risk register are considered in trade-off analysis with opportunities, and adjustments may be made to opportunity (i.e., positive risk) priority, timeline, or budget.
	Oversight (GV.OV): Risk is identified and addressed by risk management programs according to the criteria and expectations of risk governance.	**GV.OV-1**: Risk appetite statements and related contextual information are understood and applied by risk management programs.	Portfolio-level personnel verify that risk management programs understand and are applying risk appetite statements appropriately by evaluating what risks are communicated in the risk register.
		GV.OV-2: Assigned roles, responsibilities, and authorities are understood and implemented by risk management programs.	Portfolio-level personnel verify that risk management programs understand and are implementing roles, responsibilities, and authorities appropriately by evaluating that assigned responsibilities are being fulfilled and by whom.
		GV.OV-3: Organizational risk management policy and policies affecting risk management are understood and implemented by risk management programs.	Portfolio-level personnel monitor stances to verify that risk policies and risk-affecting policies are upheld.
		GV.OV-4: Risk tolerance statements are used by risk management program personnel as a basis for identifying risk.	Portfolio-level personnel verify that risk management programs understand and are applying risk tolerance statements appropriately by evaluating what risks are communicated in the risk register.

Function	Category	Subcategory	Implementation Example
		GV.OV-5: Risk is identified, adjudicated, and tracked by risk management programs according to published formats.	A risk management program uses the ERR as a basis for its risk register, and regularly communicates with Level 2 and Level 1 risk personnel using that program risk register.
		GV.OV-6: Risk is communicated and transferred by risk management programs according to published escalation and elevation criteria and process.	A risk management program uses criteria provided by Level 2 risk personnel to escalate risks to the *attention of* Level 2 risk personnel and elevate risks for *management by* Level 2 risk personnel.
		GV.OV-7: Risk management programs provide feedback for adjustment of risk appetite, opportunities, and strategic priorities.	A risk management program provides feedback to Level 2 and Level 1 risk managers when more risks exceed tolerance than current budgets will support.
MANAGE (MA): Continuously identify and address risks in accordance with the organization's risk management policies, processes, and priorities.	**Risk Identification (MA.RI):** Risk events for the organization are catalogued and recorded.	**MA.RI-1**: The assets (data, personnel, devices, systems, facilities, third-party services, etc.) that enable the organization to achieve its objectives are identified along with the assets' relative importance to those objectives and the organization's strategy.	The dependency between facility security and the electronic badge reader technology system is identified in a BIA, and any cyber risk to the electronic badge reader system is recorded in the Risk Description field of a risk register as something that could adversely affect building security.
		MA.RI-2: Threats against the organization's assets are identified and documented.	Threat intelligence sources are monitored for threats that may adversely affect critical assets. Threat modeling techniques are used to determine likely impact. This information is compared to information available from risk assessments and previous risk events. Relevant threat information is recorded in the Risk Description field of a risk register.
		MA.RI-3: Vulnerabilities of the organization's assets are identified and documented.	Vulnerability sources are monitored for vulnerabilities that affect critical assets, and relevant vulnerabilities are recorded in the Risk Description field of a risk register.
		MA.RI-4: Potential consequences are identified for each risk for the organization's assets and documented.	Risk cause and effect are documented as a risk scenario and included in the Risk Description field of a risk register.
		MA.RI-5: Risks are categorized in anticipation of future grouping and combination.	The Risk Category field of a risk register is populated with categories that are meaningful to an organization.
	Risk Analysis (MA.RA): Risk events are assessed for likelihood and impact.	**MA.RA-1**: The likelihood of each risk event is estimated using risk assessment techniques and probability models.	Bayesian models, event tree analysis, or similar techniques are used to determine the likelihood of a risk, and that information is recorded in the Current Assessment – Likelihood field in a risk register.

Function	Category	Subcategory	Implementation Example
		MA.RA-2: The impact of each risk event is estimated using risk assessment techniques that take into consideration both tangible and less tangible impacts, including secondary/cascading impacts, and the estimated impact is recorded.	An organization uses prior event data and the three-point estimate to determine likely single-loss expectancy (SLE) and annualized loss expectancy (ALE) from a risk and records that information in the Current Assessment – Impact field in a risk register.
	Risk Prioritization (MA.RP): Key risks are ranked for response decisions.	**MA.RP-1**: The exposure presented by each risk is determined using qualitative and/or quantitative models and recorded.	An organization assigns a qualitative risk exposure based on risk likelihood and impact and records that determination in the Current Assessment – Exposure Rating field of a risk register.
		MA.RP-2: The risks are prioritized based on exposure and other factors using qualitative and/or quantitative models, and the priorities are recorded.	An organization uses a quantitative model to prioritize its risks and records the priorities in the Priority field of a risk register.
	Risk Response (MA.RR): Risk responses are developed, costed, decided, described, assigned, and executed.	**MA.RR-1**: The exposure associated with each risk is checked against risk tolerance statements to determine which risk response is necessary to achieve information and communications technology objectives.	An organization uses the exposure from a risk register to decide an appropriate risk response.
		MA.RR-2: A risk response that will achieve business objectives and comply with risk guidance from leadership is identified, planned, and recorded, along with the estimated cost of applying the risk response.	An organization chooses a risk response type and estimates its cost, and records those in the Risk Response Type and Risk Response Cost fields, respectively, of a risk register.
		MA.RR-3: A risk owner is assigned for each risk response.	For each risk response in a risk register, a person is assigned responsibility for the risk response action and recorded in the Risk Owner field of the risk register.
		MA.RR-4: Plans for implementing risk responses are documented.	For each risk response in a risk register, a plan is recorded in the Risk Response Description field of the risk register.

Function	Category	Subcategory	Implementation Example
		MA-RR-5: Risk responses that will take an extended period of time or require additional funding to fully enact are recorded and tracked.	A federal agency determines that a risk will take two years to fully address and records the corresponding risk plan in a Plan of Action & Milestones (POA&M) document. A private-sector organization determines that a risk will require funding from next fiscal year to fully address and records the corresponding risk plan in a project plan.
		MA.RR-6: Risk analysis is revised after risk responses are determined to reflect the envisioned reduction of likelihood and impact from each risk response.	An organization updates the Current Assessment – Likelihood, Impact, and Exposure Rating fields of a risk register after the risk responses have been documented.
		MA.RR-7: Controls are implemented or adjusted to perform risk response plans.	An organization implements security controls to enact a risk response, and those actions are recorded in the Risk Response Description field of a risk register.
		MA.RR-8: Residual risk is forecasted for each risk after risk responses are decided.	An organization estimates its residual risk and records it in the Residual Risk field of a risk register.
	Risk Monitoring, Evaluation, and Adjustment (MA.RM): Risks are checked and assessed, and risk responses are adapted as needed.	**MA.RM-1**: Risk conditions are continually monitored against risk tolerance to ensure conditions remain within acceptable levels.	Risks are measured and benchmarked according to key performance indicators (KPIs) and key risk indicators (KRIs), respectively.
		MA.RM-2: The effectiveness of risk responses is evaluated against objectives to identify risk that exceeds acceptable levels.	An organization compares target risks (Target Profile) to current risks (Current Profile) and performs a gap analysis.
		MA.RM-3: Findings from audits and risk assessments are analyzed to identify changes in risk and the effectiveness of risk responses.	A risk management program adjusts some risk responses based on recent audit findings.
		MA.RM-4: When risk exceeds risk tolerance, changes to risk responses are identified and planned.	KRIs are monitored to determine when risk exceeds risk tolerance, resulting in updates to the risk register and planning of a revised risk response, risk response type, risk response cost, and/or risk response description.
		MA.RM-5: Risk tolerance statements and budgets are adjusted as needed to reflect appropriate risk responses.	A risk management program makes budgetary adjustments when it identifies risks that are beyond tolerance and cannot be addressed with current budgets.
		MA.RM-6: Risk response plans are updated as needed to include monitoring and measurement milestones that can	Risk response descriptions are updated in risk registers to note KPIs and KRIs that will result in access to management reserve.

Function	Category	Subcategory	Implementation Example
		trigger the release or repurposing of management reserve resources.	
		MA.RM-7: Controls are adjusted to implement changes to risk response plans.	An organization changes a risk response by implementing security controls, and the updated security controls are recorded in the Risk Response Description field of a risk register.
		MA.RM-8: Changes to risks are identified and tracked.	Changes to risks are identified and recorded in appropriate fields of a risk register.
	Risk Communication (MA.RC): Information on risks is recorded and disseminated.	**MA.RC-1**: Details regarding the considerations, assumptions, and results of risk management activity are documented.	Details about risk assessment and risk response are recorded as supplements to a risk register known as risk assessment reports and risk detail records, respectively.
		MA.RC-2: Risks that match escalation criteria are periodically communicated to higher-level risk managers, and risks that match elevation criteria are transferred to higher-level risk managers.	A risk program… - communicates risk status of the next Level (i.e., escalation) or - transfers risk ownership to the next Level (i.e., elevation) …on a periodic or immediate basis using pre-defined criteria supplied by the ERM committee.
	Risk Improvement (MA.IM): Errors in risk management are reduced through root-cause analysis and refinement implementation.	**MA.IM-1**: Lessons learned while identifying and addressing risks are communicated to leadership.	Risk management programs provide quarterly reports to leadership on their lessons learned and on trends they are seeing.
		MA.IM-2: Risk management is refined based on analysis and feedback of circumstances involving implicit risk acceptance.	Risk management programs are updated to take into account the results of analyzing implicit risk acceptance.

References

[CSF] National Institute of Standards and Technology (2018) Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Cybersecurity White Paper (CSWP) NIST CSWP 6. https://doi.org/10.6028/NIST.CSWP.6

[PF] National Institute of Standards and Technology (2020) NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management, Version 1.0. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Cybersecurity White Paper (CSWP) NIST CSWP 10. https://doi.org/10.6028/NIST.CSWP.10

[SP800221] Quinn SD, Ivy N, Chua J, Barrett M, Feldman L, Topper D, Witte GA, Gardner RK, Scarfone KA (2023) 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 800-221. https://doi.org/10.6028/NIST.SP.800-221

[SSDF] Souppaya M, Scarfone K, Dodson D (2022) Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-218. https://doi.org/10.6028/NIST.SP.800-218

Appendix A. List of Symbols, Abbreviations, and Acronyms

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

BIA
Business Impact Analysis

ERM
Enterprise Risk Management

ERP
Enterprise Risk Profile

ERR
Enterprise Risk Register

ICT
Information and Communications Technology

ICTRM
Information and Communications Technology Risk Management

ICT ROF
Information and Communications Technology Risk Outcomes Framework

KPI
Key Performance Indicator

KRI
Key Risk Indicator

OLIR
Online Informative References

SP
Special Publication