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

NIST Cybersecurity Framework 2.0:
Cybersecurity, Enterprise Risk Management, and Workforce Management Quick-Start Guide

U.S. Department of Commerce
Howard Lutnick, Secretary of Commerce

National Institute of Standards and Technology
Craig Burkhardt, Acting Under Secretary of Commerce for Standards and Technology and Acting NIST Director

NIST Special Publication
NIST SP 1308 2pd
https://doi.org/10.6028/NIST.SP.1308.2pd
Please send your comments to csf@nist.gov
November 2025

INTRODUCTION

Purpose of this Guide

This Quick-Start Guide (QSG) draws on concepts and practices from enterprise risk management, cybersecurity risk management, and workforce management **to help organizations improve communication about cybersecurity risks and to plan and implement workforce decisions based upon risk reality and planned risk responses**. The scope of this QSG will vary depending on the user, but generally applies at the organization level, where cybersecurity risks of multiple systems are managed, and at the enterprise level, where senior leaders take on unique risk management responsibilities spanning multiple organizations (see NIST IR 8286 for a discussion of these levels).

Cybersecurity Risk Management (CSRM)

Cybersecurity risks are one of many types of risk that all organizations should manage and integrate into their broader enterprise risk management (ERM) strategy. Potential negative impacts to organizations from cybersecurity risks include higher costs, lost revenue, reputational damage, and reduced innovation. In addition to negative risks, positive risks—where an enterprise asset may constitute an opportunity to realize a benefit or positive impact—should also be considered. **The NIST Cybersecurity Framework (CSF) 2.0 provides guidance for managing cybersecurity risks** by helping organizations understand, assess, prioritize, and communicate consistently about cybersecurity efforts, including those related to the cybersecurity workforce.

Making ERM and CSRM-Informed Risk and Workforce Decisions

Gaps and opportunities related to the sufficiency and competency of an enterprise's cybersecurity workforce are one type of cybersecurity risk. This guide helps organizations make informed workforce and risk decisions based on the integration of ERM, CSRM, and workforce management strategy. For instance, based on the current organizational risk appetite and tolerance, cybersecurity strategy, mission objectives, budget, and existing cybersecurity workforce, an organization might decide they need to hire, upskill, reorganize, or change a risk treatment altogether to effectively address their current cybersecurity risks or to achieve their targeted cybersecurity outcomes. People, processes, and technology combine to achieve acceptable levels of enterprise and cybersecurity risk, and cybersecurity workforce assessment is often made more difficult by disconnects between technical and human resources teams. **The NICE Framework focuses on people**, **providing a common language for describing cybersecurity work, including the Work Roles an organization's cybersecurity staff must perform**.

Key Terms

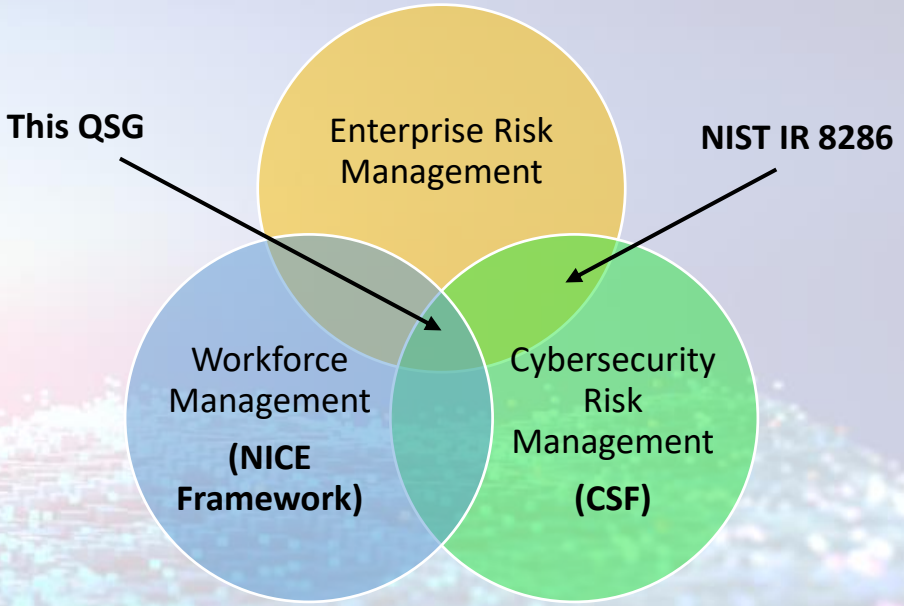
- **Enterprise Risk Management:** An effective organization-wide approach to addressing the full spectrum of the organization's significant risks by understanding the combined impact of risks as an interrelated portfolio rather than addressing risks only within silos [OMB Circular No. A-11].
- **Cybersecurity Risk Management:** Comprises the full range of activities undertaken to protect IT and data from unauthorized access and other cyber threats, to maintain awareness of cyber threats, to detect anomalies and incidents adversely affecting IT and data, and to mitigate the impact of, respond to, and recover from incidents [EO 13800].
- **Cybersecurity Workforce:** Includes individuals and teams whose primary work responsibilities impact an organization's ability to protect its data, technology systems, and operations—both traditional IT security as well as related roles that apply cybersecurity skills and knowledge [NIST SP 800-181].

RESOURCES TO ALIGN CYBERSECURITY, ERM, AND WORKFORCE MANAGEMENT

Three NIST resources enable users to align their cybersecurity, ERM, and workforce management practices in a streamlined process:

- The Cybersecurity Framework (CSF) 2.0 helps organizations—regardless of size, sector, or maturity—**understand and communicate their cybersecurity efforts**. At its most granular level, the CSF defines Categories and Subcategories of specific outcomes of cybersecurity risk management activities. Organizations use those outcomes to construct an Organizational Profile. Communities of interest can also use those outcomes to create a Community Profile, which is a baseline of CSF outcomes that addresses shared interests and goals among a group of organizations.
- The NICE Framework helps organizations **improve cybersecurity capabilities, communicate work responsibilities, and develop training**. Once an organization's current or target cybersecurity posture in terms of CSF cybersecurity outcomes is identified, the NICE Framework can be used to identify how to support or reach that target goal. The most granular elements of the NICE Framework are Task, Knowledge, and Skill (TKS) statements. Work Roles are groups of TKS statements relevant to specific cybersecurity functions.
- The NIST IR 8286 series provides a suite of resources to support improved communication between cybersecurity professionals and organizational leadership and to **align cybersecurity risk management with broader ERM practices**.

Some units within an organization may already use individual resources described above; however, organizations will benefit from using all three together. This QSG connects the three resources and their respective stakeholder groups in a holistic, workforce-focused cybersecurity risk management process.



Questions to Consider

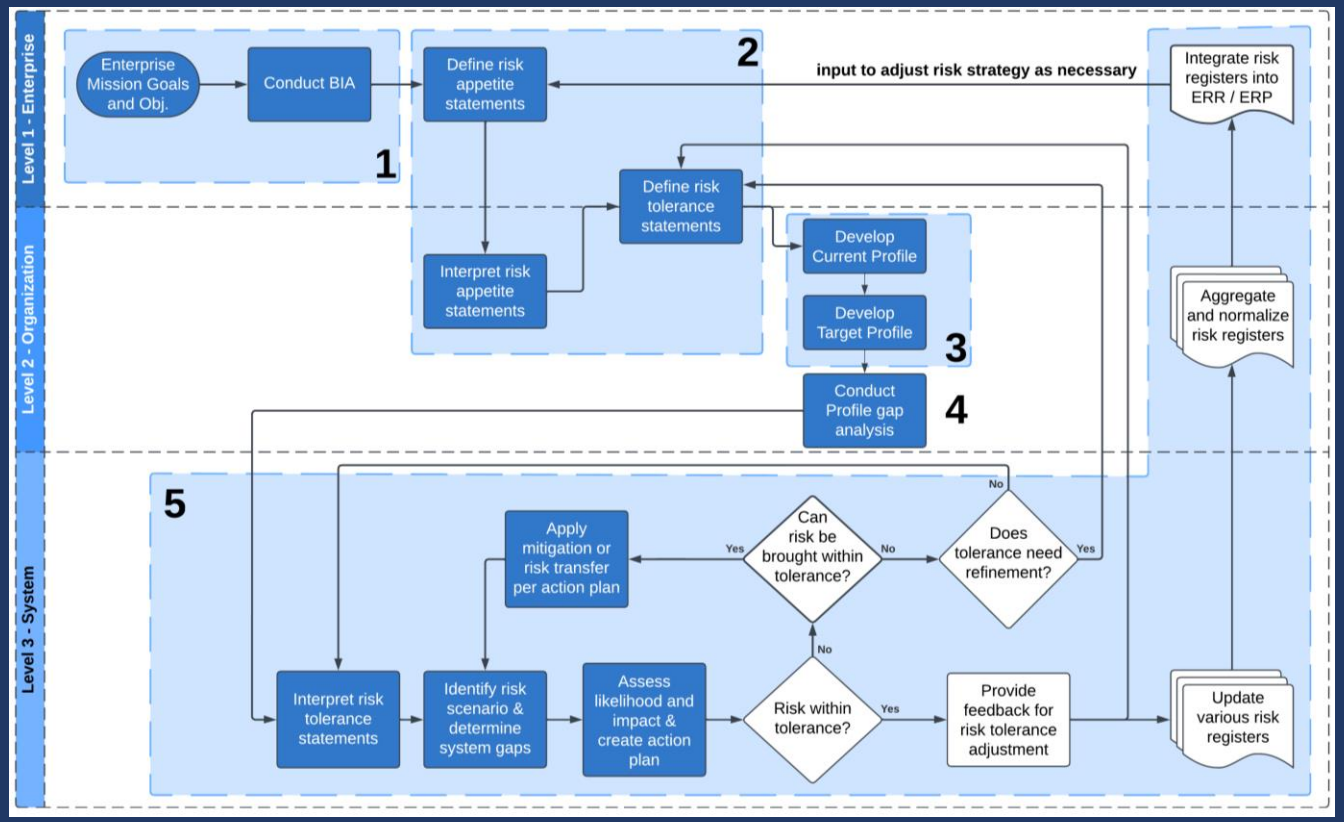
- **How** is the cybersecurity strategy being incorporated into the broader enterprise risk management strategy?
- **How** should information sharing and decision making between ERM, CSRM, and workforce teams take place?
- **What** cybersecurity risks are likely to affect delivery of the organization's mission?
- **What** actions are necessary to mitigate identified cybersecurity risks?
- **Who** within the organization has the skills and knowledge necessary to achieve a given cybersecurity outcome?

NOTIONAL APPLICATION OF THE CSF

The remainder of this guide is organized into five Cybersecurity Framework Profile implementation steps in alignment with CSRM/ERM integration and workforce management.

5 Steps for Creating and Using a CSF Organizational Profile

5 Cybersecurity Framework Profile implementation steps in alignment with CSRM/ERM integration (figure 7, NIST IR 8286C, R1 IPD)



When used together, these steps enable users to align their cybersecurity, ERM, and workforce management practices to adequately address risks and inform continuous improvement of CSRM.

STAGE 1: SCOPE THE ORGANIZATIONAL PROFILE

Overview: The scope defines the high-level facts and assumptions on which the Profiles will be based. The first step is to convene stakeholders from across the enterprise with the perspective and authority to collect risk and workforce data, articulate needs, and execute identified risk responses. The purpose of the group will be to define the scope of the effort, align security risks to the enterprise mission, and make informed risk and workforce decisions based upon current and desired risk context, priorities, budget, etc.

Sample activities in this stage:

1. Identify accountable leads from executive leadership, cybersecurity, enterprise risk management, and workforce management teams and establish an initial process timeline. Depending on scope and context, the process described in this QSG may take a week to several months to complete.
2. Identify the organization's mission, goals, objectives and high-level priorities.
3. Enterprise leaders conduct business impact analysis (BIA), which includes identifying high value assets that are critical to achieving organizational objectives. This information is used to scope the CSF Organizational Profile. The BIA examines the potential impact associated with the loss or degradation of an enterprise's information assets based on a qualitative or quantitative assessment of the criticality and sensitivity of those assets. Learn more in NIST IR 8286D.

Notes:

- A given organization may wish to use several Profiles. Each Profile can have a distinct scope (e.g., enterprise, system), which defines the high-level facts and assumptions on which the Profile is based.
- Depending on the organization, stakeholder teams convened in this stage may or may not have experience working closely together. Efforts should be made to obtain a shared understanding of each unit's roles, responsibilities, and internal processes.
- Organizations may find it beneficial to pilot the process described in this QSG by selecting a subset of CSF outcomes to begin with.

Relevant CSF Core Category: Organizational Context (GV.OC)

The circumstances – mission, stakeholder expectations, dependencies, and legal, regulatory, and contractual requirements – surrounding the organization's cybersecurity risk management decisions are understood.

Key Term: High Value Asset

Information or an information system that is so critical to an organization that the loss or corruption of this information or loss of access to the system would have serious impacts on the organization's ability to perform its mission or conduct business [NIST SP 800-160 Vol. 2 Rev. 1].

STAGE 2: GATHER THE INFORMATION NEEDED TO PREPARE THE ORGANIZATIONAL PROFILE

Overview: Having a clear picture of the organization's current CSRM, ERM, and workforce context and risk environment helps leadership adequately address the most critical risks to an organization's mission.

ERM Information Source Considerations

- Risk appetite and risk tolerance statements, which are used to define parameters for determining acceptable levels of risk
- Business impact registers
- Enterprise risk profiles

CSRM Information Source Considerations

- Cybersecurity requirements and standards followed by the organization
- Organizational policies
- Risk management priorities and resources

Workforce Information Source Considerations

- Workforce planning information, such as organizational charts or lists of filled and unfilled cybersecurity and risk management positions
- Existing recruiting and training programs
- The NICE Framework to CSF 2.0 Crosswalk

Additional Information Source Considerations

- CSF Community Profiles (which can be used as the basis for an organization's own Target Profile)
- NIST Guide to Creating Community Profiles

Relevant CSF Core Category and Subcategories: Risk Management Strategy (GV.RM)

The organization's priorities, constraints, risk tolerance and appetite statements, and assumptions are established, communicated, and used to support operational risk decisions.

- GV.RM-05: Lines of communication across the organization are established for cybersecurity risks, including risks from suppliers and other third parties.
- GV.RM-06: A standardized method for calculating, documenting, categorizing, and prioritizing cybersecurity risks is established and communicated.

Key Term: Business Impact Register

A centralized registry of important asset management information, such as system ownership, contact information for key stakeholders, and characteristics of the physical devices (or services). Since asset management is an important element of cybersecurity risk management, this information is quite valuable for protecting the asset, detecting cyber events, responding quickly to potential issues, and recovering services when necessary. A BIA register is related to but separate from a risk register, which is a repository of risk information including the data understood about risks over time [NIST IR 8286D].

STAGE 3: CREATE THE ORGANIZATIONAL PROFILE

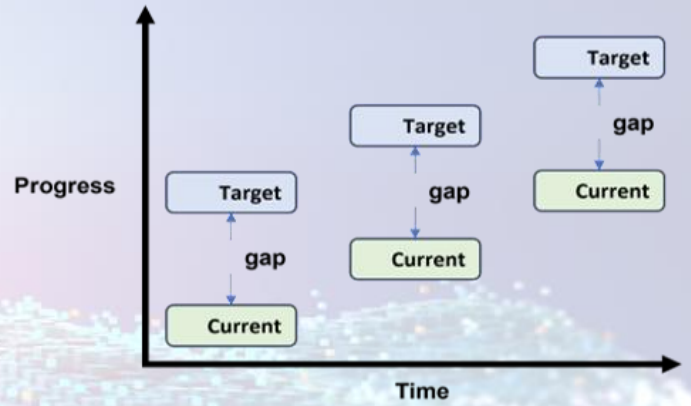
Overview: An Organizational Profile describes an organization's current and/or target cybersecurity posture in terms of cybersecurity outcomes from the Cybersecurity Framework (CSF) Core. Organizational Profiles are used to understand, tailor, assess, and prioritize cybersecurity outcomes based on an organization's mission objectives, stakeholder expectations, threat landscape, and requirements. Organizational Profiles can be categorized as:

- A **Current Profile** that specifies the CSF outcomes an organization currently achieves, and which characterizes how or to what extent each outcome is being achieved.
- A **Target Profile** specifies the desired CSF outcomes an organization has selected and prioritized for achieving its cybersecurity risk management objectives. It considers anticipated changes to the organization's cybersecurity posture, such as: new requirements, new technology adoption, and trends in threat intelligence.
- **Note:** These are viewed side-by-side as one artifact within the CSF Organizational Profile template to help organizations identify and analyze the risks presented within the gap between Current and Target.

Sample activities in this stage:

1. Review the CSF Functions, Categories, and Subcategories to determine outcomes the organization currently achieves, and to what extent. This step provides an opportunity for enterprise stakeholders to review what is currently being done and analyze those activities while considering enterprise risk context and risk strategy (e.g., risk appetite, risk tolerance, compliance requirements).
2. Review the CSF Functions, Categories, and Subcategories to determine target-state outcomes, with a clear understanding of organizational priorities and budget. This step provides an opportunity for cybersecurity risk managers, informed by an understanding of the risk implications defined in the current profile, to determine the desired set of processes and activities that will accomplish stakeholder expectations cost-effectively and efficiently.
3. Throughout each of the above activities, workforce managers, in conjunction with the CSRM and ERM teams, can examine how workforce roles and skills contribute to risk management success, or could be improved to do so.

Drive Progress Over Time with CSF Profiles



Note: The gaps within this graphic are uniform to illustrate the general concept, but gaps between Current and Target state will vary.

Resources

- NIST provides a customizable CSF Organizational Profile template as a spreadsheet. You can download and use it to create Current and Target Profiles for your organization.
- View the CSF 2.0 Profiles page within the CSF 2.0 Resource Library.

STAGE 4: ANALYZE GAPS BETWEEN CURRENT AND TARGET PROFILES AND CREATE AN ACTION PLAN

Overview: Once the team has completed the Current and Target profiles, conduct a gap analysis to identify the risks created by gaps exposed between Current and Target. This analysis will support the development of a prioritized action plan supported by a risk register.

Sample activities in this stage:

1. Using pre-existing risk register (if available) and NIST CSF outcome statements, review known risks and make necessary adjustments to the risk register.
2. Review the risk register to understand which risks are the most critical to achieving the organization's mission and assess who will be the risk owner and risk action owner. This is where focus shifts to analyzing the workforce gap(s) in relation to risk management.
3. Carefully consider and designate risk ownership. Those designated as the risk owners must be constantly knowledgeable about relevant risk conditions and must also have the accountability and authority to manage the risk. Furthermore, a gap analysis between the assigned risk owner and the risk work role can be conducted to see if the practitioner has the competencies necessary to address the problem. Since risk conditions may change as information is aggregated, responsibility and accountability should be periodically reviewed to ensure that the risk owner is appropriate.
4. Complete a gap analysis using a crosswalk between the NICE Framework and the CSF. Does the organization have the requisite staff needed to adequately address the risk? Begin considering whether is it possible to hire or upskill employees to fill identified gaps. Are there other gaps that exist, such as in roles or job descriptions, organizational or reporting structure, etc.?

Relevant CSF Core Category and Subcategories: Roles, Responsibilities, and Authorities (GV.RR)

Cybersecurity roles, responsibilities, and authorities to foster accountability, performance assessment, and continuous improvement are established and communicated.

- GV.RR-01: Organizational leadership is responsible and accountable for cybersecurity risk and fosters a culture that is risk-aware, ethical, and continually improving
- GV.RR-02: Roles, responsibilities, and authorities related to cybersecurity risk management are established, communicated, understood, and enforced
- GV.RR-03: Adequate resources are allocated commensurate with the cybersecurity risk strategy, roles, responsibilities, and policies
- GV.RR-04: Cybersecurity is included in human resources practices

Sample Risk Register

ID	Priority	Risk Description	Risk Category	Current Assessment			Risk Response Type	Risk Response Cost	Risk Response Description	Risk Owner	Risk Action Owner	Status
				Likelihood	Impact	Exposure Rating						

Key Term: Risk Register

OMB Circular A-11 describes a risk register as "a repository of risk information, including the data understood about risks over time. Typically, a risk register 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 [NIST IR 8286].

STAGE 5: IMPLEMENT THE ACTION PLAN AND UPDATE THE ORGANIZATIONAL PROFILE

Overview: At this stage in the CSRM/ERM/workforce alignment process, cybersecurity risk practitioners understand stakeholder expectations, budget, priorities, high value assets, and risks. Equipped with this information, they can now determine the appropriate workforce or risk responses to adequately address the most critical risks to the organization.

Sample activities in this stage:

Convene a team to jointly select workforce response or responses for identified high-priority risks. Workforce responses can include the following, individually or in combination:

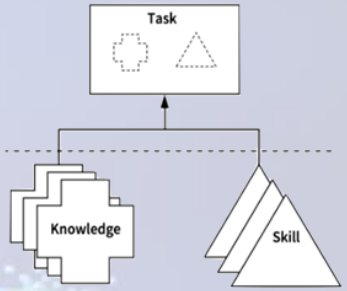
- **Upskill** current employees through professional development, mentorship, or hiring new staff into developmental programs such as internships, apprenticeships, or co-ops.
- **Create new positions**, modify existing ones, or potentially implement a reorganization to address risks.
- **Recruit** fully competent staff to fill a position or positions using the NICE Framework to help identify relevant Work Roles and associated Tasks, Knowledge, and Skills.

1. Workforce management team: Assign estimated costs for workforce responses selected for each Subcategory, and add details related to timeline, metrics, success criteria and implementation considerations for associated people, processes, and technology. Costs and timelines will vary depending on organization characteristics. If the identified risks are positive risks, organizations may wish to consider ways to realize, share, or enhance those opportunities [NIST IR 8286].
2. If workforce-focused risk responses are not possible, consider adjusting risk response. For example, if training and hiring are not viable options for an absent workforce capability, the organization may consider selecting a different mitigation strategy or changing the risk response type to, for example, accept, avoid, or transfer.
3. The Leadership team finalizes and signs off on updated risk register(s).

Key Terms

- **Task:** An activity that is directed toward the achievement of organizational objectives.
- **Knowledge:** A retrievable set of concepts within memory.
- **Skill:** The capacity to perform an observable action.

Relationship Between Task, Knowledge, and Skill Statements.



Credit: NICE Program Office

Resources

- The NICE Framework helps you understand the wide variety of cybersecurity roles and responsibilities that exist across an organization. It can be used to help assess the current workforce as well as identify capability gaps, develop career pathways, create employee upskilling or career plans, and identify courses and training that align with those needs.
- An Employer's Guide to Writing Effective Cybersecurity Job Descriptions provides tips on how to use the NICE Framework when hiring so that you will be equipped to author and communicate about position responsibilities and find the candidate that meets your needs.

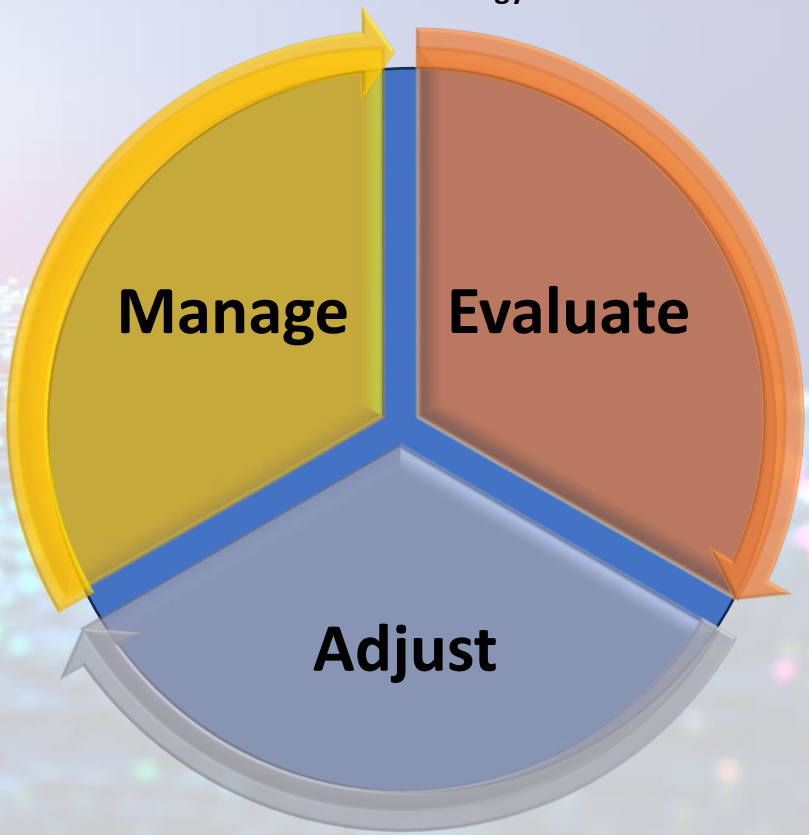
ITERATION

Overview: In the preceding steps, enterprise stakeholders collected risk information, assessed workforce readiness, and identified workforce and risk responses to address high-priority risks. Now begins the task of continuous monitoring.

Sample activities in this stage:

1. **Manage:** Stakeholders implement identified risk responses and, where applicable, incorporate those responses into broader ERM processes. CSRM/ERM/workforce strategies are continuously monitored, evaluated, and adapted to be successful. Stakeholder teams develop plans and processes for continued collaboration to regularly evaluate how effectively risks are being addressed.
2. **Evaluate:** Establish a process for evaluating how effectively planned interventions have addressed risks, including regular check-ins among stakeholder teams working in priority areas. Consider reassessing the risk after the intervention has been in place for a specified timeframe. Ensure the risk register is updated and that cybersecurity risks are incorporated into broader ERM portfolios, if applicable (see NIST IR 8286 for a discussion of risk portfolios). An organization's finance and accounting staff should be involved in this step; if evaluation takes place at the enterprise level, audit committees may be involved as well.
3. **Adjust:** Once stakeholders have evaluated the chosen workforce intervention and other risk interventions to determine whether they have adequately addressed risk to the organization, the next step is to adjust where necessary. Further workforce responses—such as upskilling, reskilling, reassignment of roles or responsibilities—and risk response adjustments may be necessary.

Continuous Monitoring of CSRM, ERM, and Workforce Strategy.



Learn more about the Manage, Evaluate, Adjust (MEA) lifecycle within NIST IR 8286C, Staging Cybersecurity Risks for Enterprise Risk Management and Governance Oversight.

ADDITIONAL RESOURCES

Additional Resources

- **Understanding the Cybersecurity Framework:** Other Quick-Start Guides focused on small businesses, CSF Tiers, ERM, and other subjects are available on the CSF 2.0 Resource Center.
- **Risk identification, analysis, and prioritization:**
  - IR 8286A provides comprehensive information on risk registers and more granular risk detail records.
  - SP 800-30 Rev. 1, SP 800-221, and SP 800-221A discuss risk assessments and the integration of information and communications technology into ERM processes.
  - The NIST Risk Management Framework provides a comprehensive process for managing information security and privacy risks at the system level.
- **Workforce assessment and educational best practices:** The NICE Framework Resource Center provides additional formats for the NICE Framework, in-depth cybersecurity workforce development resources, and information about cybersecurity workforce partnerships, such as the RAMPS communities. Organizations can receive assistance with NICE Framework implementation by emailing NICEframework@nist.gov.
  - Crosswalk for the CSF 2.0 and NICE Framework to help organizations identify priority Work Roles (Note: several Work Roles may map to each CSF Subcategory).
  - NICE Framework Components to explore priority Work Roles and identify relevant Tasks, Knowledge, and Skills to train or recruit for.
  - NIST SP 800-50r1, Building a Cybersecurity and Privacy Learning Program, helps organizations create or mature an organizational learning program in support of an informed and capable cybersecurity and privacy workforce.

Glossary of Acronyms

- **BIA:** Business Impact Analysis
- **CSRM:** Cybersecurity Risk Management
- **CSF:** Cybersecurity Framework
- **ERM:** Enterprise Risk Management
- **QSG:** Quick Start Guide
- **TKS:** Task, Knowledge, and Skill