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

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 ipd
https://doi.org/10.6028/NIST.SP.1308.ipd
Please send your comments to cyberframework@nist.gov
March 2025

CSF 2.0: CYBERSECURITY, ERM, AND WORKFORCE MANAGEMENT
QUICK START GUIDE

INTRODUCTION

Purpose of this Guide

This Quick Start Guide (QSG) shows how the NICE Workforce Framework for Cybersecurity and the Cybersecurity Framework (CSF) can be used together to **facilitate communication across business units and improve organizational processes where cybersecurity, enterprise risk management (ERM), and workforce management intersect.**

Overview of Risk

Risk is the effect of uncertainty on business objectives. Cybersecurity risk is an important type of risk that all enterprises face, alongside others including financial, legal, reputational, and safety risks. Although cybersecurity risks frequently intersect with additional risk types — in the form of lost revenue or stakeholder trust, for example — some organizations do not conduct cybersecurity risk management with the same consistency and rigor that are applied to other types of risk.

CSF Organizational Profiles

An Organizational Profile describes an organization's current and/or target cybersecurity posture in terms of cybersecurity outcomes from the CSF Core. Organizational Profiles are used to understand, tailor, assess, and prioritize cybersecurity risk based on an organization's mission objectives, stakeholder expectations, threat landscape, and requirements. The organization can then act strategically to achieve those outcomes. Organizational Profiles can also be used to assess progress toward targeted outcomes and to communicate pertinent information to stakeholders. *This QSG assumes that an Organizational Profile has been completed already.*

Integrating Cybersecurity, ERM, and Workforce Management

Once current and/or target cybersecurity posture in terms of CSF cybersecurity outcomes is documented, you can then use the NICE Framework to identify the people and skills needed to implement the outcomes. People, processes, and technology combine to achieve acceptable levels of enterprise and cybersecurity risk. **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.

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

March 2025

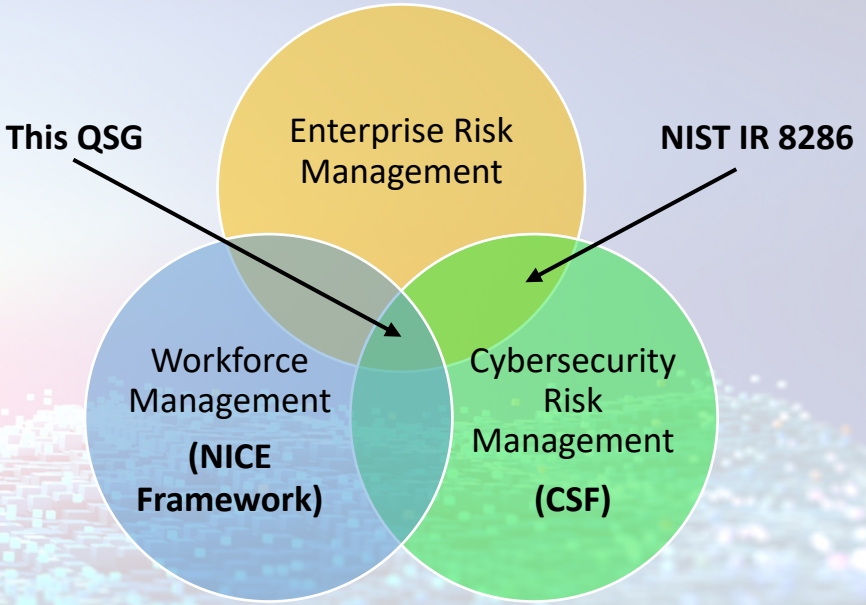
CSF 2.0: CYBERSECURITY, ERM, AND WORKFORCE MANAGEMENT
QUICK START GUIDE

RESOURCES TO ALIGN CYBERSECURITY, ERM, AND WORKFORCE MANAGEMENT

This QSG draws on three key NIST resources to enable users to align their cybersecurity, ERM, and workforce management practices in a streamlined process.

- The Cybersecurity Framework (CSF) 2.0 is voluntary guidance that helps organizations — regardless of size, sector, or maturity — understand and communicate their cybersecurity efforts. At its most granular level, the CSF defines **specific outcomes of cybersecurity risk management** activities called Subcategories. Organizations use Subcategories to construct an Organizational Profile.
- The NICE Framework is a voluntary workforce standard that organizations use to identify gaps in cybersecurity capabilities, communicate work responsibilities, and develop training. The most granular elements of the NICE Framework are Task, Knowledge, and Skill (TKS) statements. This QSG focuses on **Work Roles**, which are groupings of TKS statements that define areas of work for which an individual or team is responsible — such as Cybersecurity Policy and Planning, Software Security Assessment, and Knowledge Management.
- The 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, few are likely to be familiar with all three. This QSG connects the three resources and their respective stakeholder groups in a holistic, workforce-focused cybersecurity risk management process.



Questions to Consider

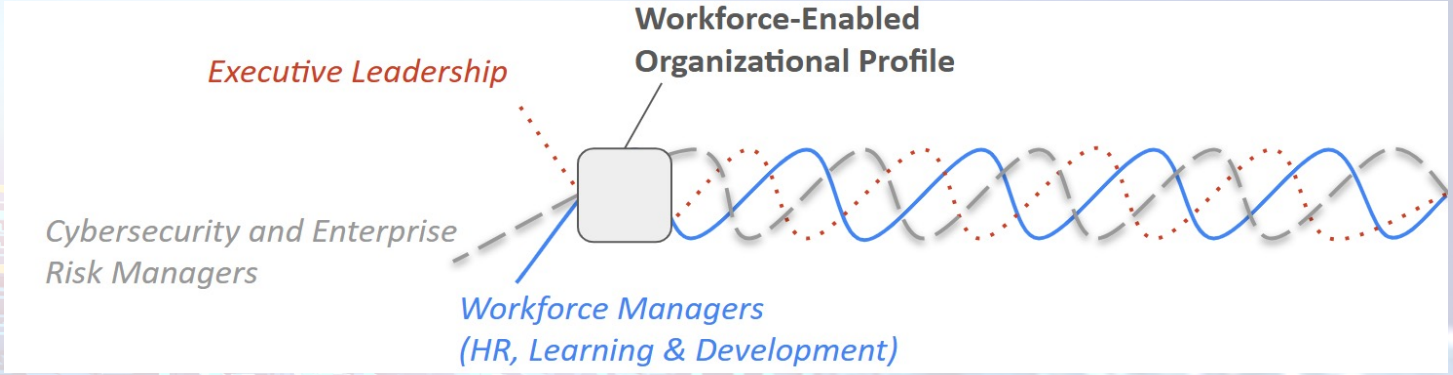
- **How** is cybersecurity being incorporated into our broader enterprise risk management strategy?
- **What** cybersecurity risks are likely to affect our ability to deliver on our organization's mission?
- **What** actions are necessary to mitigate our cybersecurity risks?
- **Who** within the organization has the skills and knowledge necessary to achieve this outcome? Do we have this type of person in our organization? Do we need to upskill or hire individuals? If neither is possible, what are other risk responses or other risk owner assignments?

CSF 2.0: CYBERSECURITY, ERM, AND WORKFORCE MANAGEMENT
QUICK START GUIDE

OVERVIEW

The following pages describe a process for context setting, risk characterization, workforce assessment, response planning, and implementation to enable users to align their cybersecurity, ERM, and workforce management practices in a streamlined process.

1. Identify organizational context
2. Analyze and prioritize risks
3. Conduct workforce assessment
4. Identify and plan workforce responses
5. Implement, evaluate, and adjust responses



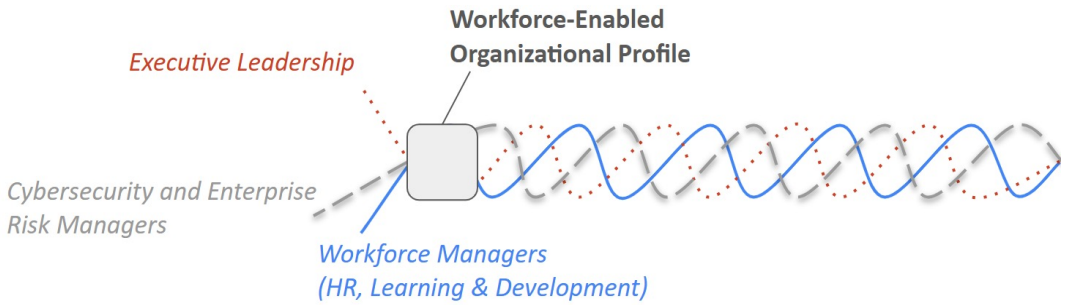
Organizations using this QSG need to convene stakeholder teams with the perspective and authority to collect data, articulate needs, and execute identified responses in each of the areas illustrated above. Necessary organizational inputs include:

- **Workforce planning information** such as organizational charts, lists of filled and unfilled cybersecurity and risk management positions, and existing recruiting and training programs.
- **Asset information** describing hardware, software, data, and other technology assets.
- **Risk context information** related to an organization's unique mission, business, and exposure.

CSF 2.0: CYBERSECURITY, ERM, AND WORKFORCE MANAGEMENT
QUICK START GUIDE

STAGE 1: IDENTIFY ORGANIZATIONAL CONTEXT

Overview: The first step is to convene a planning group with representation drawn from leadership, cybersecurity and ERM, and workforce management teams.



Activities in this stage:

1. Identify accountable leads for each team and establish initial process timeline. Depending on size and context, the process described in this QSG may take a week to several months to complete.
2. Collect and disseminate resources including existing cybersecurity strategy documents, workforce readiness assessments, organizational charts and rosters, and training and hiring documentation.
3. Leads: review collected organizational resources and QSG resources described above.
4. Convene initial discussion(s) to understand current processes and constraints.

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.

Notes

- 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 one or two CSF Functions (Govern, Identify, Protect, Detect, Respond, or Recover) to begin with.

CSF 2.0: CYBERSECURITY, ERM, AND WORKFORCE MANAGEMENT
QUICK START GUIDE

STAGE 2: ANALYZE AND PRIORITIZE RISKS

Overview: The goal of the process described in this QSG is to improve an organization's cybersecurity risk management controls by refining its workforce processes and readiness. A clear picture of the organization's current cybersecurity practices and risk environment is therefore essential. This stage draws on ERM methods and processes detailed in greater depth in the NIST IR 8286 Series.

Activities in this stage:

1. Cybersecurity and ERM team: track and communicate the known system-level threats and vulnerabilities, their impact on business objectives, and the responses taken or planned with a risk register.
2. Leadership team: Review and sign off on the risk register.
3. Both teams: Convene to discuss findings, noting possible barriers and reconciling any differences of opinion.

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

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.

Questions to Consider

- What cybersecurity risks will affect the organization's ability to deliver on its mission?
- What cybersecurity risks are other organizations in this sector experiencing?

Related Resources

- SP 800-221, Enterprise Impact of Information and Communications Technology Risk: Governing and Managing ICT Risk Programs Within an Enterprise Risk Portfolio
- IR 8286A, Identifying and Estimating Cybersecurity Risk for Enterprise Risk Management

STAGE 3: CONDUCT WORKFORCE ASSESSMENT

Overview: Now that you understand what information and technology are most important to the enterprise mission and have defined acceptable levels of risk for those assets (ID.AM, ID.RA), the next step is to identify how personnel in various work roles will be accountable for risk management success (GV.RR). Cybersecurity workforce assessment is a complex process that is often made more difficult by disconnects between technical teams and their human resources counterparts.

Activities in this stage:

1. Workforce management team:
   a) Identify the risk owner for each organizational risk.
   b) Identify the risk action owner who is responsible for carrying out specific actions to mitigate a risk. They may be the same, or different, from the risk owner.
   c) Complete a gap analysis, for example, using the OLIR crosswalk between the NICE Framework and the CSF. **Do the risk owner's skills match what's needed to address the risk?** Do we need to upskill or hire individuals? If neither is possible, what are other risk responses or other risk owner assignments?

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						

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

STAGE 4: IDENTIFY AND PLAN WORKFORCE RESPONSES

Overview: At this stage in the workforce alignment process, an organization should have a common picture of its cybersecurity workforce needs. Next, stakeholders will need to identify appropriate workforce interventions, assign roles and responsibilities, and implement the identified responses.

Activities in this stage:

1. Convene a stakeholder team to debrief and share reflections. Jointly select an achievable response or set of responses for each risk. Responses include:
    - **Hire:** Recruit fully competent staff to fill a position or positions.
    - **Train:** Upskill current employees through professional development or mentorship, or hire new staff into developmental programs such as internships, apprenticeships, or co-ops.
    - **Change risk response**
        - Example 1: If training and hiring are not viable options for an absent workforce capability, the organization may have to consider changing the risk response type to, for example, accept, avoid, or transfer [NIST IR 8286].
        - Example 2: If the identified risks are positive risks, organizations may wish to consider ways to realize, share, or enhance those opportunities [NIST IR 8286].
2. Workforce management team: Assign estimated costs for the responses selected for each Subcategory, and add details related to timeline and possible implementation considerations.

Negative Risks and Positive Risks as Inputs to CSRM

In the CSRM discipline, a significant portion of risk information is collected and reported regarding weaknesses and threats that could result in negative consequences. However, positive risks (opportunities) also inform decisions by senior leaders for setting the risk appetite and tolerance of the enterprise. For example, conducting an analysis that considers strengths and weaknesses as well as opportunities and threats (SWOT) may be a useful exercise.

Learn more: NIST IR 8286, *Integrating Cybersecurity and Enterprise Risk Management*.

Note

Most organizations face a set of common challenges in cybersecurity workforce management. Readers are encouraged to explore opportunities for regional partnership and collaboration by engaging with local colleges, universities, workforce boards, and technology associations.

STAGE 5: IMPLEMENT, EVALUATE, AND ADJUST RESPONSES

Overview: Once target workforce responses have been selected, stakeholder teams can integrate those responses into existing operational practices and work cycles. Workforce interventions require ongoing evaluation and adaptation to be successful, and stakeholder teams are encouraged to develop plans and processes for continued collaboration in the long term.

Activities in this stage:

1. Implement responses, raise awareness, and solicit feedback. Establish regular processes for program evaluations and updates, including regular check-ins among stakeholder teams working in priority areas.
2. If applicable, expand scope of workforce alignment processes to other CSF Functions.

Additional Resources: Practices described in this guide can be enhanced by reference to several additional NIST resources and networks:

- **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.
- **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.