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

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

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

NIST Special Publication
NIST SP XXXX
This publication is available free of charge from:
DOI LINK GOES HERE

NIST Cybersecurity Framework: Enterprise Risk Management Quick-Start Guide

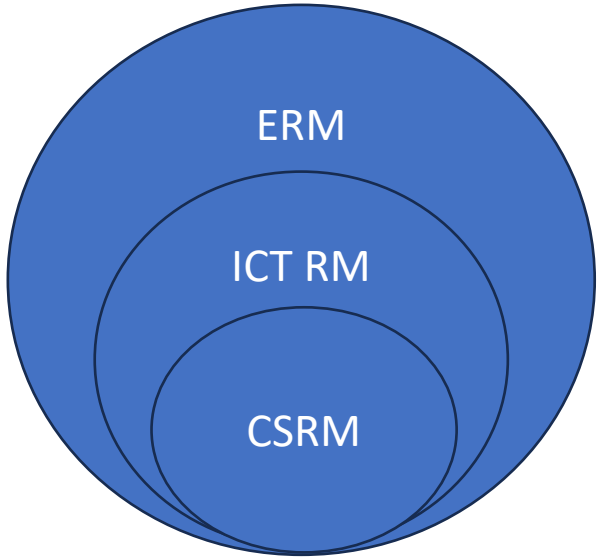
This guide provides an introduction to using the NIST Cybersecurity Framework (CSF) 2.0 for planning and integrating an enterprise-wide process for integrating cybersecurity risk management information, as a subset of information and communications technology (ICT) risk management, into enterprise risk management (ERM). The use of CSF common language and outcomes supports the integration of risk monitoring, evaluation, and adjustment across various organizational units and programs.

Enterprise Risk Management (ERM)

When we use the word enterprise in an organizational context, we mean all aspects of that organization, spanning the entire breadth and depth of that org chart. ERM exists at the top level of the organizational hierarchy and spans risk considerations such as mission, financial, reputation, and technical risks thereof. ERM calls for understanding the core risks that an enterprise faces, determining how best to address those risks, and ensuring that the necessary actions are taken. An ERM program allows enterprises to aggregate, prioritize, and analyze risks from across the enterprise in a common risk register format. **Risk appetite** expressed by the ERM program helps inform **risk identification**.

Information and Communications Technology (ICT) Risk Management

The information and communications technology (ICT) on which an enterprise relies is managed through a broad set of risk disciplines that include privacy, supply chain, and cybersecurity. ICT extends beyond traditional information technology (IT) considerations. Many entities rely on operational technology (OT) and IoT (Internet of Things) devices' sensors or actuators to bridging physical and digital environments. Increasingly, artificial intelligence (AI) factors into enterprise risk. NIST SPs 800-221 and 800-221A provide more information.



Cybersecurity Risk Management (CSRM)

Cybersecurity risks are a fundamental type of risk for all organizations to manage. Potential negative impacts to organizations from cybersecurity risks include higher costs, lower revenue, reputational damage, and the impairment of innovation. Cybersecurity risks also threaten individuals' privacy and access to essential services and can result in life-or-death consequences. Risk appetite expressed at other levels of risk management get translated into more specific CSRM **risk tolerance**, such that cyber risks can be more easily identified.

CSF 2.0 provides guidance for reducing cybersecurity risks by helping organizations discuss, organize, and address gaps in their **cybersecurity program** in a standard way. The cybersecurity outcomes described in CSF effect cybersecurity, ICT, and enterprise risks. Understanding these dependencies is an essential activity in CSRM, ICT RM, and ERM. The Cybersecurity Risk Register (CSRR) described in the NISTIR 8286 series of publications enables organizations to identify, manage, and monitor the relationships between discrete risks and aspects of a CSF-based cybersecurity program that address those risks. The CSRR allows organizations to identify, organize, analyze, and report on cybersecurity risks at the system level. CSF Profiles are a natural byproduct of a comprehensive CSRR, because the relative priority of CSF outcomes becomes apparent based on how significant the impacts of identified cybersecurity risks might be to the organization's priorities, such as its strategic objectives, products and services, or customers.

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

February 2024

NIST Cybersecurity Framework: Enterprise Risk Management Quick-Start Guide

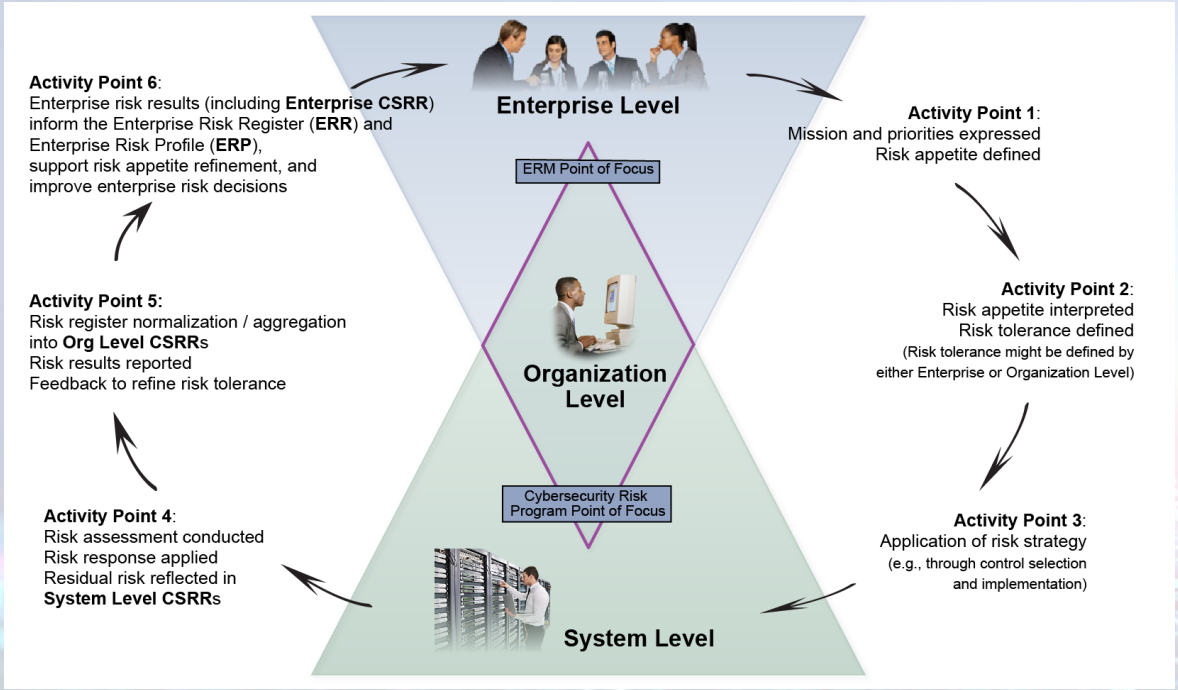


Illustration of enterprise risk management integration and coordination
From NIST SP 800-221

CSF 2.0, as part of a holistic ERM approach, helps ensure that leaders continually have the information they need for making informed business/agency decisions.

CSF 2.0 Supports Six Activity Points For Informing, Implementing, and Monitoring ERM

CSF 2.0 is a valuable guide for helping to review and improve security and privacy considerations as part of a holistic enterprise risk approach. CSF is most helpful when it is paired with other ERM elements. For example, as agency officials and corporate boards of directors provide oversight of all relevant risks, the CSF process helps ensure that cybersecurity strategy is well-executed. Managers plan and implement risk treatment based on that strategy, record and report progress, and provide agency / business leaders with information needed for effective operations and mission success.

The **Activity Points**, which will be further described in subsequent pages, include:

- 1 – Leaders **define and record** enterprise mission, priorities, and risk appetite. **Accountability** is assigned for managing both **positive and negative types of risk**. (GV.OC, GV.RM, GV.SC)
- 2 – Organization-level managers interpret **risk appetite** into specific guidance regarding security and privacy requirements, and associated **risk tolerance**. (GV.RR, GV.PO, ID.RA)
- 3 – **Risk strategy and requirements** aid implementation of shared security solutions and system-level controls to achieve an acceptable level of risk. (PROTECT, DETECT, RESPOND, and RECOVER)
- 4 – Risk response outcomes are reflected as residual risk in **system-level risk registers** as part of **ongoing assessment** and **continuous monitoring** activities. (ID.RA, ID.IM, GV.OV)
- 5 – **Risk registers are normalized and aggregated** at the organization unit level, supporting reporting, analysis, and organization-level adjustment. (ID.IM, GV.OV)
- 6 – Combined risk results from the enterprise are used to maintain an **enterprise-level risk register and risk profile**, supporting enterprise business decisions and any **adjustments** needed for the risk strategy. (GV.PO, GV.OV)

Supporting Resources:

- SP 800-221, *Enterprise Impact of Information and Communications Technology Risk: Governing and Managing ICT Risk Programs Within an Enterprise Risk Portfolio*
- SP800-221A - *Information and Communications Technology (ICT) Risk Outcomes: Integrating ICT Risk Management Programs with the Enterprise Risk Portfolio*

NIST Cybersecurity Framework: Enterprise Risk Management Quick-Start Guide

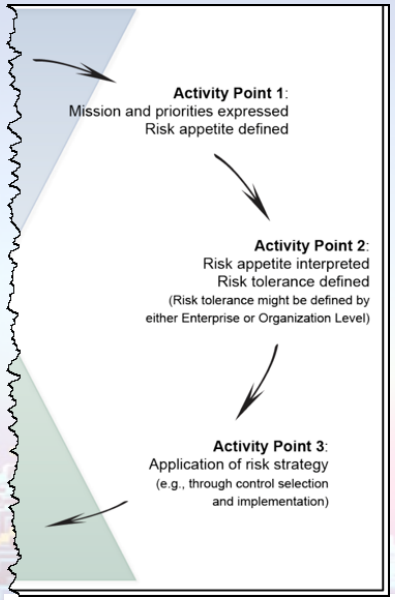
Aligning enterprise priorities with strategic activity

As senior leaders and organizational managers observe and discuss **risk management strategy** (to take advantage of opportunities and to avoid known threats), they develop a plan for managing risk to the optimal level.

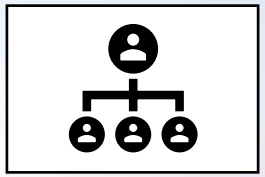
The outcomes in the CSF Govern function (GV) specifically drive **actionable planning** about how to best manage various enterprise risks to ICT, including privacy, supply chain, AI, IoT, and operational technology on which the entity depends.

Beginning with an understanding of what information and technology are most important to the **enterprise mission**, leaders define **acceptable levels of risk** for those assets and describe how personnel in various work roles will be **accountable** for risk management success. (ID.AM, ID.RA)

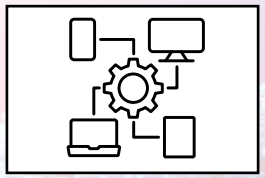
This actionable and proactive strategizing also makes clear to customers and other stakeholders that effective risk management is a priority, that clear and accountable plans are in place to achieve that management, and that monitoring processes are continually identifying opportunities for improvement. These plans specifically apply the outcomes described in the CSF Organizational Profile(s), in particular the PROTECT, DETECT, RESPOND, and RECOVER functions.



Based on internal and external organizational context, leaders use governance systems to set risk priorities, risk appetite, and risk strategy. This understanding sets the tone for how the enterprise conducts, measures, and reports risk management activities and performance. Actions include processes for aligning priorities and risk direction for business partners and other members of the organization's cybersecurity supply chain.



Understanding of objectives and risk appetite enables managers to interpret how to apply those for their organizational units (OUs). Managers create risk tolerance statements and metrics, defining a "target state" that will achieve stakeholder objectives such as through secure shared infrastructure (e.g., organizationally-tailored control baselines, common controls, and monitoring strategy).



The direction from leadership and OU management is applied in an operational context, supporting system-level risk assessment, requirements definition and allocation. These enable effective categorization, control selection/implementation, and ongoing system-level authorization/monitoring.

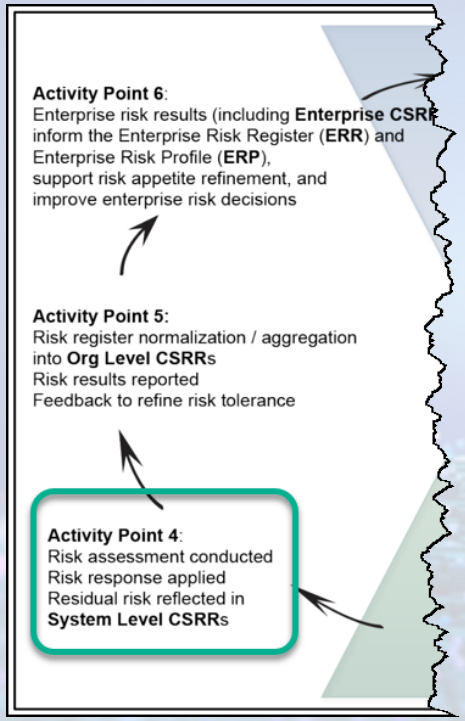
Questions to Consider

- ? **Activity Point 1**: Where do you draw the mission and strategic priorities of the organization from?
  Do you have a process for defining and expressing Risk Appetite?
- ? **Activity Point 2**: How is Risk Appetite translated into Risk Tolerance?
  Are cybersecurity risk management strategy outcomes reviewed to inform and adjust strategy and direction?
- ? **Activity Point 3**: How are organizational priorities, definition of acceptable risk, and performance requirements embedded in your system-level risk activities?
  Are these translated into control selection, system constraints, reporting requirements, and anomaly detection?

Related Resources

- NIST Risk Management Framework (RMF) for Information System and Organizations - a comprehensive, flexible, repeatable, and measurable process to manage information security and privacy risk
- NISTIR 8286 series – Specifically NISTIR 8286A - *Identifying and Estimating Cybersecurity Risk for ERM*
- NIST SP800-30 Rev1 – *Guide for Conducting Risk Assessments*

NIST Cybersecurity Framework: Enterprise Risk Management Quick-Start Guide



Risk Assessment, Risk Treatment and Information Sharing Ensure Value and Risk Optimization

Select Risk Response

After selecting and implementing controls and other methods of risk treatment, system-level personnel assess the effectiveness and efficiency of that treatment (e.g., through the Assess step of the NIST Risk Management Framework). Risk managers evaluate threats and opportunities, in alignment with risk strategy and direction from enterprise- and organization-level guidance. They determine the benefits of the following responses: Mitigate, Accept, Avoid, Transfer for negative risks; Realize, Share, Enhance, and Accept for positive risks.

Analyze & Prioritize Risks

There are benefits to both qualitative and quantitative risk analysis methodologies and even the use of multiple methodologies, based on enterprise strategy, organization preference, and data availability. (ID.RA) The relative priority of various types of risk must be decided upon by those with appropriate authority, usually through guidance provided through the risk management strategy (GV.RM).

Communicate Risk Findings and Decisions

The cybersecurity risk register (CSRR) provides a location to record and communicate the known system-level threats and vulnerabilities, their impact on business objectives, and actions taken or planned. Risk managers share information about residual risk, including metrics that support ongoing assessment and authorization, and plans of actions & milestones for maintaining the appropriate level of risk based on stakeholders' expectations (as expressed in the target state of the Organizational Profiles, especially the GOVERN and IDENTIFY functions).

Notional Cybersecurity 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											

Continually Communicate, Learn, and Update

Questions to Consider

- ? How do CSF Target Profile outcomes (organizational agreement on how to best protect, detect, respond and recover) inform system-specific risk assessment and treatment?
- ? How can we estimate likelihood and impact of those risks given the planned outcomes and knowledge from previous results?
- ? Is our risk response proportionate to the exposure?

Related Resources

- NIST Risk Management Framework (RMF) for Information System and Organizations
- NISTIR 8286A – Identifying and Estimating Cybersecurity Risk for Enterprise Risk Management
- **Risk Detail Schema** **Risk Detail** **CSRR Schema**

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

February 2024

NIST Cybersecurity Framework: Enterprise Risk Management Quick-Start Guide

CSF outcomes (planned and current) support a Monitor-Evaluate-Adjust cycle for achieving ERM objectives.

As risk management is applied through various controls (as described above) the results are continually evaluated for effectiveness. CSF provides examples of how to do this through CSF Informative References, described at the Online Informative References (OLIR) web site.

At the organization level, the results of various system-level activities and results (as reflected in CSRRs) are aggregated and normalized. Managers monitor how well the cyber risk strategy is being implemented, evaluate indicators to confirm performance goals and highlight potential changes in the risk landscape, and then make any adjustments necessary to accentuate achievement of opportunities (positive risk) and reduce impactful threat conditions to acceptable level.

This cycle enables creation and maintenance of an organization-level CSRR, and updates to the Organizational Profiles to reflect refined current state and adjusted Target State.

MONITOR

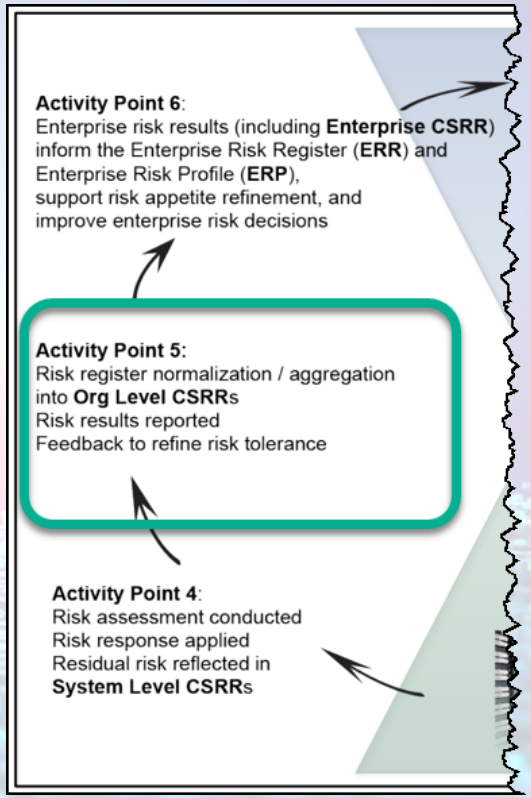
- Measure *whether* controls are still implemented and effective
- Measure the *extent to which* controls are implemented without impairing organizational operations and efficiency

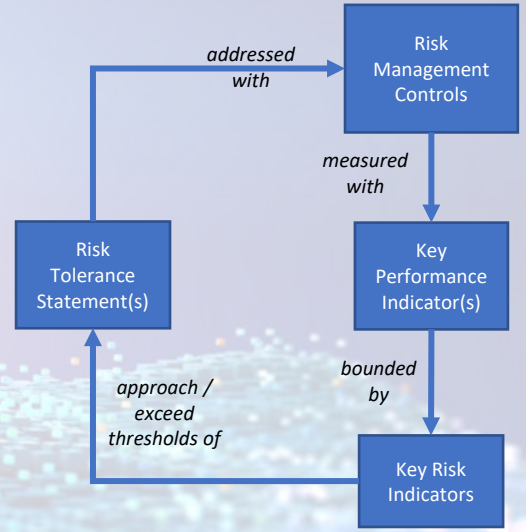
EVALUATE

- Assess if organizational controls are achieving the desired risk results
- Assess if risk management activities are keeping risk within tolerance (e.g., evaluating key risks and key performance indicators)
- Compare current outcomes to the target state described in Organizational Profiles

ADJUST

- Implement additional controls and enhancement as needed
- Implement alternative controls to enhance opportunity





Monitor-Evaluate-Adjust Cycle (from NIST SP 800-221)

Risk registers are aggregated, normalized, and shared based on enterprise-defined risk categories and measurement criteria. Risk tolerance statements are refined, if needed, to ensure balance among ICT value, organizational resources, and optimal risk.

Supporting Resources

- NISTIR 8286C – *Staging Cybersecurity Risks for ERM and Governance Oversight*

NIST Cybersecurity Framework: Enterprise Risk Management Quick-Start Guide

Feedback from CSF Informative References and the MEA cycle help monitor and adjust risk response, appetite/tolerance, and policy.

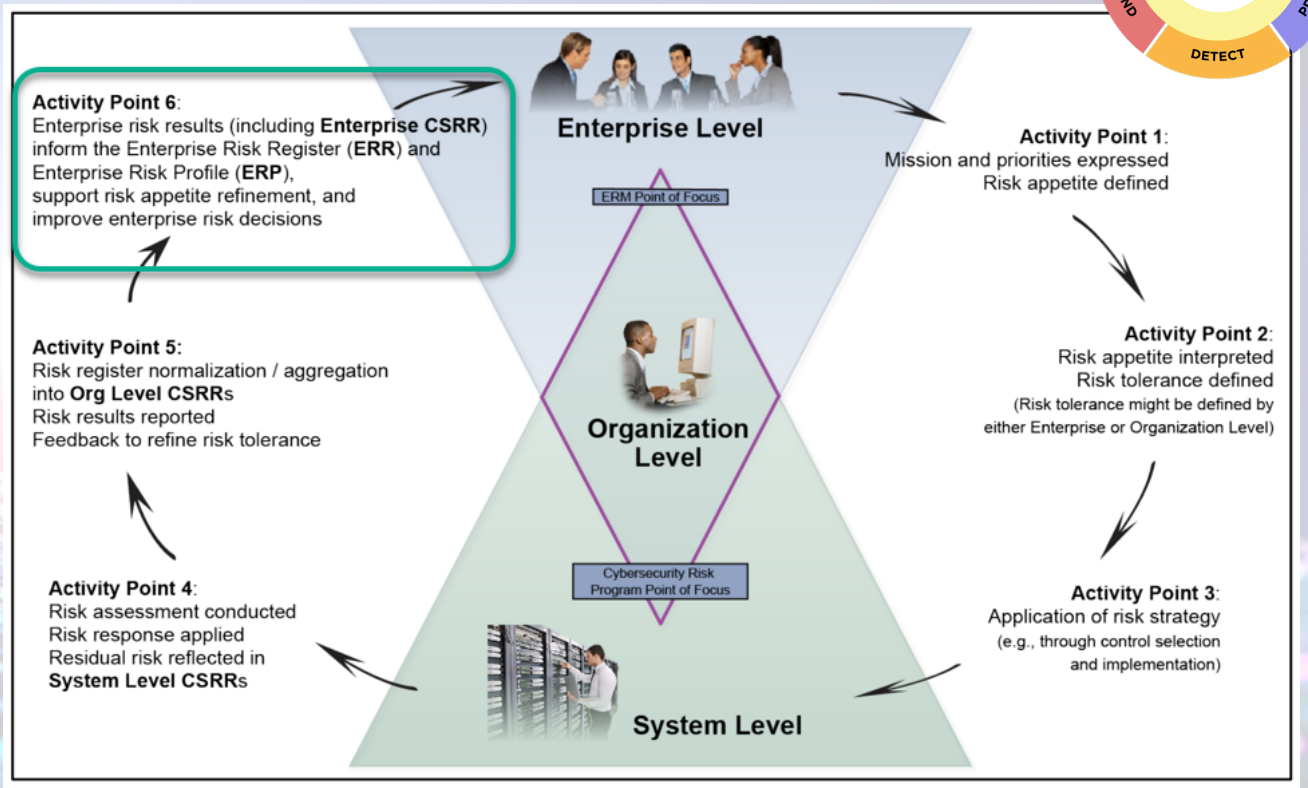
As risk management controls are operated, performance is evaluated and adjusted to improve effectiveness and efficiency. Feedback from the MEA cycle sometimes results in more than just adjustments to controls and other Informative References. Feedback may lead to adjustments in:

- CSF Profile
- Risk Detail Record
- Risk Response Description
- Risk Response
- Risk Tolerance
- Risk Appetite
- Policy
- Strategy

This helps report results back to management and enterprise leadership. Results that particularly reflect operational achievement (key performance indicators, or KPIs) confirm conformance with the strategy. (GV.RM, GV.SC) This also supports personnel performance monitoring and reporting (GV.RR, GV.PO)

Managers integrate data from normalized and harmonized risk registers, from organization-level reports, compliance and audit reports. These are considered in light of non-technology risk management activities (e.g., credit risk, market risk, labor risk). Considering composite outcomes of positive and negative risk management enables effective balance among investments in and results of risk management activity. Results are reflected in an **enterprise risk register (ERR)** and **an enterprise risk profile (ERP)** that provides a prioritized ERR.

In this way, CSF helps to guide the selection, implementation, and monitoring of specific controls (such as those in the informative references), and the results ensure an effective and ongoing holistic ERM solution for all types of risk.



Questions to Consider

- ? How are top cybersecurity risks identified for leadership and recorded in the enterprise risk register?
- ? Are escalation criteria defined to ensure accountability and information sharing? (NISTIR 8286C)
- ? Are processes in place to marry system/organization-level risk to enterprise level considerations?
- ? How are enterprise security and privacy risks (including opportunities) aligned with other risk types?

NIST Cybersecurity Framework: Enterprise Risk Management Quick-Start Guide

What We Learned*

Risk Appetite – a general way of defining risk you can accept

Risk Tolerance – a specific way of defining risk you cannot accept

Risk Identification – the process of understanding your risks

Enterprise Risk Management – the process of managing general high-level risk

Information and Communications Technology Risk Management - the process of managing various ICT risks

Cybersecurity Risk Management - the process of managing specific cybersecurity risks

CSF Govern – one of six high-level outcomes expressed in CSF; oversight to ensure cybersecurity is managed

Negative Risks – things that are weaknesses or threats

Positive Risks – things that are strengths or opportunities

Cybersecurity Risk Register – a list of your high priority risks

Risk Response Description – the place in the CSRR where you note CSF outcomes and Informative Reference implementations

Cybersecurity Framework Outcome – what cybersecurity you are trying to achieve

Informative Reference Implementation - how you implement cybersecurity

Online Informative References – a catalog of Informative References hosted at a NIST web site

SP 800-53 Control – a security or privacy control from the NIST Special Publication 800-53 controls catalog

Monitor, Evaluate, Adjust – how you actualize cybersecurity; in a Deming Cycle, this is the do, check, act

Feedback Loop – how you make adjustments and improvements

*Descriptions provided are intended as plain language. Please see the NIST Glossary for official NIST definitions.

EXPLORE MORE CSF 2.0 RESOURCES

CSF web site for more on CSF Govern and CSF Profiles

OLIR web site for more Informative References

SP 800-53 page for more on security and privacy controls

IR 8286 page – for more on risk identification and analysis

IR 8286A for more on risk registers

IR 8286B for more on risk detail records