NIST Special Publication
NIST SP 1331 ipd

Quick-Start Guide for Using CSF 2.0 to Improve Management of Emerging Cybersecurity Risks

Initial Public Draft

Stephen Quinn
Computer Security Division
Information Technology Laboratory

Matthew Barrett
CyberESI Consulting Group Incorporated

R. K. Gardner
New World Technology Partners

Kelly Hood
Optic Cyber Solutions

Matthew Smith
Seemless Transition LLC

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.1331.ipd

August 21, 2025

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

Abstract

This Quick Start Guide introduces the topic of emerging cybersecurity risks and illustrates how organizations can improve their ability to address such risks through existing practices within the NIST Cybersecurity Framework (CSF) 2.0. The guide also emphasizes the importance of integrating these practices within the organization's enterprise risk management (ERM) program.

Keywords

Cybersecurity Framework (CSF); cybersecurity risk; emerging risk; enterprise risk management (ERM); systems of systems.

Audience

The audience for this paper is organizations seeking to better understand and mitigate emerging risks, regardless of the maturity of an organization's existing cybersecurity risk management program.

It is assumed that readers have a working knowledge of at least one of the following topics: cybersecurity risk management, enterprise risk management, or systems engineering.

Note to Reviewers

While the goal of this document is to show that preparing for unknown risk can be accomplished through risk planning using the CSF 2.0, NIST is also interested in feedback on this Initial Public Draft (IPD) regarding how this paper characterizes the difference in certain terminology, specifically: the difference in risk response and strategies, and as Appendix A discusses, there are numerous conflicting definitions for the terms "emerging risk" and "emergent risk" within the cybersecurity community and across other scientific and technical communities. Given the potential difference in definition, the implementation of risk management activities may be different. NIST is particularly interested in your experience with both terms, including the definitions you use and how you differentiate the concepts from each other, if at all. For simplicity, NIST is using "emerging risk", as defined in Section 1, as the basis of the guidance.

1. Emerging Cybersecurity Risks

As technologies have increased both in complexity and in the number and nature of their interdependencies with other technologies, their risks have become more difficult to manage. Organizations are not aware, and cannot be aware, of some of the cybersecurity risks they face. There are two types of these risks, better known as *emerging risks*:

- **Emerging risks that are unknown to some organizations and known to others.** These are largely well-understood risks (ransomware, distributed denial of service, phishing, etc.) that some organizations simply do not know about yet. While these risks evolve due to outside factors (new technology, environmental, regulation, etc.), there are known, well-documented mitigations to these risks. An organization that has not identified these risks may incur a large-scale impact if one of these risks is realized. Organizations that bolster their risk identification techniques are likely to be aware of more emerging risks. Example activities for minimizing this type of emerging risk are in Table 1 under ID.RA.
- **Emerging risks that are unknown to all organizations.** These risks have never been seen before. There are no documented risk mitigations, avoidance strategies, or transfer opportunities. At any time, one of these risks may simply be realized, and organizations will be left to their own processes and procedures to handle it.

This paper discusses strategies for handling both types of emerging risks. Emerging risks require more dynamic approaches to cybersecurity risk management (CSRM), such as increasing the resilience of systems to better maintain or restore operations after emerging risks are realized. Furthermore, organizations utilizing a broader coordination across different domains, ERM processes, roles, and responsibilities will improve emerging risk management. Organizations implementing the NIST IR 8286 series of documents would have access to organizational data which would help inform this process:

- A Business Impact Assessment as described in NIST IR **8286D** [9]
- A Risk Register as described in NIST IR **8286A** [6]
- Risk Detail Records as described in NIST IR **8286A** [6]

Many of today's technologies are part of a *system-of-systems*, which is defined as a system whose elements are themselves systems [1]. These heterogeneous, distributed systems often include a mix of information technology (IT), operational technology (OT), and Internet of Things (IoT) capabilities [2]. These systems have become more adaptable due to advances in machine learning (ML) and artificial intelligence (AI). As a result, these systems behave in less predictable ways.

Therefore, it is critical to utilize a multi-disciplinary approach when facing emerging risks. Specifically, organizations should incorporate different disciplines and domains in emerging risk identification, analysis, evaluation, prioritization, and response activities. NIST has many resources which could aid organizations seeking to complement their traditional cybersecurity risk management activities, some examples include:

- NIST SP 800-221 [13]: Enterprise Impact of Information and Communications Technology Risk: Governing and Managing ICT Risk Programs Within an Enterprise Risk Portfolio
- NIST SP 800-221A [14]: Information and Communications Technology (ICT) Risk Outcomes: Integrating ICT Risk Management Programs with the Enterprise Risk Portfolio
- NIST IR 8183r1 [10]: Cybersecurity Framework Version 1.1 Manufacturing Profile
- NIST AI 100-1 [11]: Artificial Intelligence Risk Management Framework (AI RMF 1.0)
- NIST SP 600-1 [12]: Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile

While many organizations face emerging cybersecurity risks, the likelihood of facing them rises when certain factors are present. Those include situations when key business-critical functions, systems, services, and data are dependent upon real-time system interactions or external factors, such as environmental conditions. Therefore, organizations with these factors could benefit greatly from having a BIA as described in NIST IR 8286D [9] to assist in the proactive, preparatory, and forward leaning activities discussed later in this document.

2. Improving the Management of Emerging Cybersecurity Risks

There are two distinct phases for managing emerging cybersecurity risks: prior to such a risk being realized, and after. This delineation between proactive and reactive steps can be organized by the NIST Cybersecurity Framework (CSF) 2.0 [3] Functions. The *Govern*, *Identify*, and *Protect* Functions are mostly used to manage risks before they are realized, and the *Detect*, *Respond*, and *Recover* Functions are mostly used to manage risks after they are realized. Further, the Improvement Category, found in the *Identify* Function, is used to direct lessons learned after the risk is realized. These improvement activities prepare organizations to effectively react to the risk and drive the next iteration of the cycle. Lessons learned from performing all activities in all Functions are fed into Improvement, and those lessons are analyzed, prioritized, and used to inform all Functions. Fig. 2 shows the interactions of the Functions as implemented in this document and NIST Special Publication (SP) 800-61r3, *Incident Response Recommendations and Considerations for Cybersecurity Risk Management* [4].

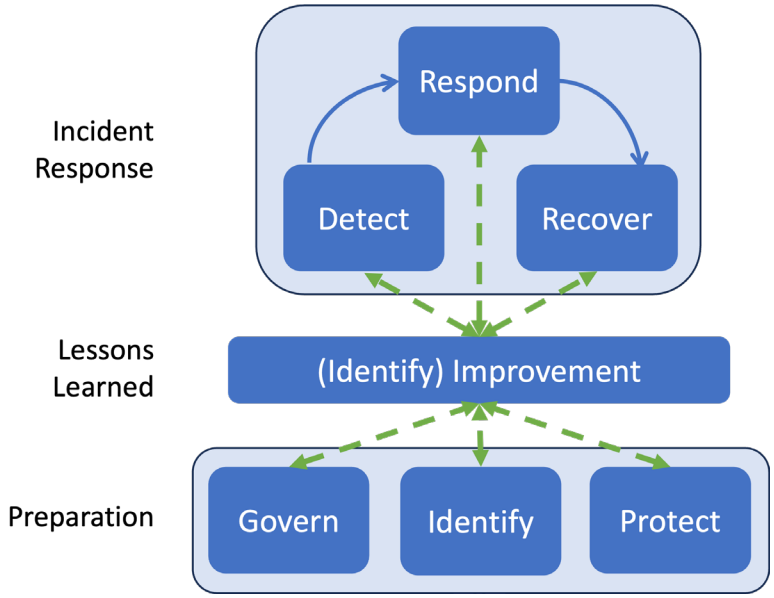

Fig. 1. Incident response life cycle model organized by CSF 2.0 Functions

Organizations can better manage their emerging risks by expanding their organizational view of threats, methods of compromise, and vulnerabilities by adding new disciplines, domains, and stakeholders to risk identification activities. Concurrently organizations should elevate executive-level attention on formal risk treatment. This includes establishing a robust governance structure that aligns with clear business objectives, defining supporting processes, formalizing risk management strategies, and assigning accountability for risk decisions.

Proactively identifying and characterizing emerging risks makes them more manageable through traditional CSRM strategies. System development life cycle (SDLC) management, enterprise risk management (ERM), and complex system behavior analysis provide ways to govern and identify such risks. The NIST Interagency Report (IR) 8286 [5] series of publications

covers the topic of CSRM extensively, providing clear guidance on its implementation and integration with ERM:

- **IR 8286A** [6] details the context, scenario identification, and analysis of cybersecurity risk likelihood and impact. It includes guidance tied to the CSF on identifying potential threat sources and events to aid in identifying and understanding cybersecurity risks.
- **IR 8286B** [7] describes ways to apply risk analysis to help prioritize cybersecurity risk, evaluate and select appropriate risk responses[1], and communicate risk activities as part of an enterprise CSRM strategy.
- **IR 8286C** [8] describes aggregating information from CSRM activities throughout the enterprise. As that information is integrated and harmonized, organizational and enterprise leaders monitor achievement of risk objectives and consider changes to risk strategy.
- **IR 8286D** [9] describes the identification and management of risk as it propagates from system to organization and from organization to enterprise, which in turn better informs Enterprise Risk Management deliberations. NIST IR 8286D expands typical BIA discussions to inform risk prioritization and response by quantifying the organizational impact and enterprise consequences of compromised IT Assets.

Unexpected behaviors are difficult to plan for and react to quickly. The consequences of realized emerging risks can spread instantly, making containment in the moment extremely difficult. Planning for emerging risk is conducted by adequately accounting for these systems and dependencies in governance and management capabilities, as well as ensuring effective safeguards are in place to limit the impact and prevent the cascading effect of emerging behaviors that lead to mission disruption. An organization's quick reaction to execute detection, response, and recovery activities can also help to minimize the disruption.

Preparing for the realization of emerging risks requires organizational resilience and adaptability. The realization of emerging risk requires system level risk mitigation as well as organizational processes to mitigate the impact. Enterprises can implement resilience within their organizational levels by effectively implementing the suggested activities in Table 1.

Table 1 more closely examines how organizations can improve the management of emerging cybersecurity risks. This table, which is organized by CSF 2.0 Functions and Categories, only includes those Functions and Categories with recommendations specific to emerging risks. Generally, organizations seeking to improve the maturity of their management of known cybersecurity risks should devote significantly more resources to known risks than emerging risks. As management of known risks matures, organizations can increase their adoption of recommended actions from Table 1 to better address emerging risks as well.

[1] Response types for negative risks include accepting, avoiding, transferring, or mitigating, while response types for positive risks include exploiting, sharing, enhancing, or accepting, as described in NIST IR 8286B Section 2.3 [7].

144 **Table 1. Recommended actions for improving management of emerging risks**

Function	Category	Recommended Actions	Discussion
Govern (GV)	Organizational Context (GV.OC)	Consider emerging risks as part of the organizational context.	Context should include national and supply chain dependencies that impact an organization's mission and business functions, as well as technological factors such as the presence of systems of systems within the organization's environment.
	Risk Management Strategy (GV.RM)	Adjust the risk management strategy to account for emerging risks.	Consider where increased capital reserves are required to fund *Respond* and *Recover* activities.
	Risk Management Strategy (GV.RM)	Allocate resources to emerging risks.	When discussing risk prioritization, include emerging risks in evaluation criteria.
	Roles, Responsibilities, and Authorities (GV.RR)	Update work roles to include emerging risks.	Include responsibilities for identifying scenarios for emerging risks within cybersecurity risk management roles.
	Policy (GV.PO)	Update policies to include emerging risks.	Account within risk management policies for technologies and scenarios that could trigger emerging risks.
	Oversight (GV.OV)	Update risk analysis processes.	Address emerging risks that affect other types of risk, like operational, financial, and reputational, in risk scenarios used by cross-functional governance teams.
	Cybersecurity Supply Chain Risk Management (GV.SC)	Update ERM risk management processes.	Cascade the above *Govern* practices to the cyber supply chain.
Identify (ID)	Risk Assessment (ID.RA)	Analyze emerging risks through traditional CSRM practices.	Leverage the vulnerability and threat identification techniques outlined in NIST IR 8286A [6], along with system analysis and validation methods such as dependency analysis and stress testing from NIST SP 800-160v1 [2].
	Risk Assessment (ID.RA)	Identify additional emerging risks.	Performing root-cause analysis of the organization's cyber incidents can lead to additional emerging risks being identified. Be aware of emerging risks that are realized by other organizations.
	Improvement (ID.IM)	Improve the current cybersecurity posture.	Bolster the organization's *Respond* posture by focusing on preparatory methods like incident response and disaster recovery planning and exercises, capital reserves corresponding with possible response expenses, and appropriate insurance policies, if applicable.

Function	Category	Recommended Actions	Discussion
Protect (PR)	Technology Infrastructure Resilience (PR.IR)	Implement containment techniques.	Restrict each component of a system to a given function or partition, segmented from other components. When one component fails, the failure is isolated and does not cascade to the other parts of the system, although it can still affect overall system performance. Containment examples include service-oriented architecture, loose coupling, pre-defined segmentation, and dynamic segmentation and isolation consistent with zero-trust principles [1].
	Technology Infrastructure Resilience (PR.IR)	Implement redundancy techniques.	Provide multiple protected instances of critical resources to minimize system downtime and maximize availability. Redundancy is integral to system resilience, but it must be carefully managed to avoid the redundant systems becoming an unintentional risk [1]. Techniques for achieving redundancy include protected backups and restores for data and software; surplus capacity for data storage, processing, and communications; and replicating and synchronizing hardware, data, backups, and functionality in multiple locations, using diverse resources when feasible.
Detect (DE)	Adverse Event Analysis (DE.AE)	Accelerate detection processes.	To detect the realization of emerging risks more rapidly, consider using detection methods that correlate information from numerous sources of alerting and audit data, such as security information and event management (SIEM) or security automation orchestration and response (SOAR).
Respond (RS)	Incident Analysis (RS.AN)	Learn from realized emerging risks.	Conduct root-cause analysis to eradicate conditions that led to the emerging risk so that effective response, recovery, and improvement can happen.
	Incident Mitigation (RS.MI)	Execute crisis response techniques.	If existing containment techniques, as discussed for PR.IR, are not sufficiently effective against a realized emerging risk, consider using additional containment approaches to adequately eliminate or reduce its impact. Examples of stopgap measures include pulling cables, implementing crisis segmentation, or diverting additional resources to the network.
Recover (RC)	Incident Recovery Plan Execution (RC.RP)	Prioritize services for recovery.	In any realized risk, there will be a distinct order in which services should be restored. In the *Identify* phase, include a recovery restoration priority. This activity will accelerate the recovery process.
	Incident Recovery Communication (RC.CO)	Develop alternative communication strategies.	When recovering from a realized emerging risk, there will be a need for communicating internally and externally. Typical communication services may be down. Create alternative strategies and

Function	Category	Recommended Actions	Discussion
			communication plans for if critical services are unavailable. For example, create a call tree with paper copies of names and addresses of key personnel, and hold training sessions for public relations representatives where notes are unavailable.

145

References

[1] Ross RS, Pillitteri VY, Graubart R, Bodeau D, McQuaid R (2021) Developing Cyber Resilient Systems: A Systems Security Engineering Approach. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-160, Vol. 2, Rev. 1. https://doi.org/10.6028/NIST.SP.800-160v2r1

[2] Ross RS, McEvilley M, Winstead M (2022) Engineering Trustworthy Secure Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-160v1r1. https://doi.org/10.6028/NIST.SP.800-160v1r1

[3] National Institute of Standards and Technology (2024) The NIST Cybersecurity Framework (CSF) 2.0. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Cybersecurity White Paper (CSWP) NIST CSWP 29. https://doi.org/10.6028/NIST.CSWP.29

[4] Nelson A, Rekhi S, Souppaya M, Scarfone K (2025) Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-61r3. https://doi.org/10.6028/NIST.SP.800-61r3

[5] Quinn SD, Chua J, Ivy N, Gardner RK, Scarfone K, Smith MC, Witte GA (2025) Integrating Cybersecurity and Enterprise Risk Management (ERM). (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency Report (IR) NIST IR 8286r1 ipd. https://doi.org/10.6028/NIST.IR.8286r1.ipd

[6] Quinn SD, Ivy N, Barrett M, Feldman L, Witte GA, Gardner RK (2025) Identifying and Estimating Cybersecurity Risk for Enterprise Risk Management. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency Report (IR) NIST IR 8286Ar1 ipd. https://doi.org/10.6028/NIST.IR.8286Ar1.ipd

[7] Quinn SD, Ivy N, Barrett M, Witte GA, Gardner RK (2025) Prioritizing Cybersecurity Risk for Enterprise Risk Management. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency Report (IR) NIST IR 8286B-upd1. https://doi.org/10.6028/NIST.IR.8286B-upd1

[8] Quinn SD, Ivy N, Barrett M, Gardner RK, Smith MC, Witte GA (2025) Staging Cybersecurity Risks for Enterprise Risk Management and Governance Oversight. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency Report (IR) NIST IR 8286Cr1 ipd. https://doi.org/10.6028/NIST.IR.8286Cr1.ipd

[9] Quinn SD, Ivy N, Chua J, Barrett M, Feldman L, Topper D, Witte GA, Gardner RK (2025) Using Business Impact Analysis to Inform Risk Prioritization and Response. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency Report (IR) NIST IR 8286D-upd1. https://doi.org/10.6028/NIST.IR.8286D-upd1

[10] Stouffer K, Zimmerman T, Tang C, Pease M, Lubell J, Cichonski J, McCarthy J (2020). Cybersecurity Framework Version 1.1 Manufacturing Profile. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency Report (IR) 8183r1. https://doi.org/10.6028/NIST.IR.8183r1

[11] Tabassi, E. (2023), Artificial Intelligence Risk Management Framework (AI RMF 1.0), NIST Trustworthy and Responsible AI, National Institute of Standards and Technology, Gaithersburg, MD, https://doi.org/10.6028/NIST.AI.100-1

[12] Autio, C. , Schwartz, R. , Dunietz, J. , Jain, S. , Stanley, M. , Tabassi, E. , Hall, P. and Roberts, K. (2024), Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile, NIST Trustworthy and Responsible AI, National Institute of Standards and Technology, Gaithersburg, MD, https://doi.org/10.6028/NIST.AI.600-1

[13] Quinn S, Ivy N, Chua J, Barrett M, Feldman L, Topper D, Witte G, Gardner RK, Scarfone K (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

[14] 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

Appendix A. Emerging vs Emergent Risk

The terms “emerging risk” and “emergent risk” are used interchangeably by some authors and organizations but not by others. This confusion is understandable because the words “emerging” and “emergent” are synonyms in some contexts but not others. For example, the Merriam-Webster dictionary definition of “emerging”[2] duplicates one of its definitions of “emergent”: “newly formed or prominent.” However, “emergent” has several other definitions, including “arising unexpectedly.”[3]

Surveys of the meaning and use of the terms “emerging risk” and “emergent risk” have been conducted across various scientific and technical disciplines.[4] These surveys, as well as NIST’s own survey of recent cybersecurity literature, indicate that while there is no widespread consensus on the meaning of either term, “emerging risk” is more widely used.

We have created a definition of “emerging risk” strictly for the purposes of this document. We are not using the term “emergent risk” at this time. Within cybersecurity, “emergent risk” is sometimes used specifically for unpredictable risks that arise from the behavior of highly complex and interconnected systems. That risk domain is currently being studied within many communities, including the operational research and AI communities. This document may be updated in the future as consensus builds around the meanings of both terms.

[2] https://www.merriam-webster.com/dictionary/emerging
[3] https://www.merriam-webster.com/dictionary/emergent
[4] https://doi.org/10.1016/j.ress.2015.07.008

Appendix B. Acronyms

AI
Artificial Intelligence

CSF
Cybersecurity Framework

CSRM
Cybersecurity Risk Management

ERM
Enterprise Risk Management

IoT
Internet of Things

IR
Interagency Report

ML
Machine Learning

OT
Operational Technology

SDLC
System Development Life Cycle

SP
Special Publication

How to Cite this NIST Technical Series Publication:
Quinn SD, Barrett M, Gardner RK, Hood K, Smith MC (2025) Quick-Start Guide for Using the NIST Cybersecurity Framework 2.0 to Manage Unknown Cybersecurity Risks. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 1331 ipd. https://doi.org/10.6028/NIST.SP.1331.ipd

Author ORCID iDs
Stephen D. Quinn: 0000-0003-1436-684X
Matthew Barrett: 0000-0002-7689-427X
Matthew C. Smith: 0000-0003-1004-7171

Public Comment Period
August 21, 2025 – September 21, 2025

Submit Comments
csf@nist.gov

National Institute of Standards and Technology
Attn: Applied Cybersecurity Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 2000) Gaithersburg, MD 20899-2000

Additional Information
Additional information about this publication is available at https://www.nist.gov/cyberframework, including related content, potential updates, and document history.

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