NIST Special Publication 800
NIST SP 800-61r3

Incident Response Recommendations and Considerations for Cybersecurity Risk Management

A CSF 2.0 Community Profile

Alex Nelson
Sanjay Rekhi
Murugiah Souppaya
Karen Scarfone

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-61r3

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

NIST Special Publication 800
NIST SP 800-61r3

Incident Response Recommendations and Considerations for Cybersecurity Risk Management

A CSF 2.0 Community Profile

Alex Nelson
Sanjay Rekhi
Murugiah Souppaya*
Computer Security Division
Information Technology Laboratory

Karen Scarfone
Scarfone Cybersecurity

**Former NIST employee; all work for this publication was done while at NIST.*

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-61r3

April 2025

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

Certain equipment, instruments, software, or materials, commercial or non-commercial, are identified in this paper in order to specify the experimental procedure adequately. Such identification does not imply recommendation or endorsement of any product or service by NIST, nor does it imply that the materials or equipment identified 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, Use, and Licensing Statements
NIST Technical Series Publication Identifier Syntax

Publication History

Approved by the NIST Editorial Review Board on 2025-03-25
Supersedes NIST SP 800-61r2 (August 2012) https://doi.org/10.6028/NIST.SP.800-61r2

How to Cite this NIST Technical Series Publication

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

Author ORCID iDs
Alex Nelson: 0000-0002-3771-570X
Sanjay Rekhi: 0009-0008-8711-4030
Murugiah Souppaya: 0000-0002-8055-8527
Karen Scarfone: 0000-0001-6334-9486

Contact Information
800-61-comments@nist.gov

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

Additional Information
Additional information about this publication is available at https://csrc.nist.gov/pubs/sp/800/61/r3/final, including related content, potential updates, and document history.

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

Abstract

This publication seeks to assist organizations with incorporating cybersecurity incident response recommendations and considerations throughout their cybersecurity risk management activities as described by the NIST Cybersecurity Framework (CSF) 2.0. Doing so can help organizations prepare for incident responses, reduce the number and impact of incidents that occur, and improve the efficiency and effectiveness of their incident detection, response, and recovery activities. Readers are encouraged to utilize online resources in conjunction with this document to access additional information on implementing these recommendations and considerations.

Keywords

cyber threat information sharing; Cybersecurity Framework; cybersecurity incident; cybersecurity risk management; incident handling; incident management; incident response.

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.

Supplemental Content

NIST has established an Incident Response project page that hosts links to resources with additional information on incident response activities. By moving links from this document to a website, NIST can update and expand them as needed without having to release a new version of this publication.

For more information on CSF 2.0 Community Profiles, see the Framework Resource Center.

Audience

The target audience for this publication includes cybersecurity program leadership, cybersecurity personnel, and others who are responsible for preparing for, detecting, responding to, or recovering from cybersecurity incidents. This publication is intended for use by most organizations, regardless of sector, size, or other factors.

Trademark Information

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

Executive Summary

Incident response is a critical part of cybersecurity risk management and should be integrated across organizational operations. All six NIST Cybersecurity Framework (CSF) 2.0 Functions play vital roles in incident response:

- Govern, Identify, and Protect help organizations prevent some incidents, prepare to handle incidents that do occur, reduce the impact of those incidents, and improve incident response and cybersecurity risk management practices based on lessons learned from those incidents.
- Detect, Respond, and Recover help organizations discover, manage, prioritize, contain, eradicate, and recover from cybersecurity incidents, as well as perform incident reporting, notification, and other incident-related communications.

Many individuals, teams, and third parties hold a wide variety of roles and responsibilities across all of the Functions that support an organization's incident response. Organizations have no direct control over the tactics and techniques used by their adversaries, nor are they certain about the timing of a future incident other than knowing that another incident is inevitable. However, organizations can use an incident response life cycle framework or model that best suits them to develop strong cybersecurity risk management practices that reduce their risks to acceptable levels.

This publication uses the CSF 2.0 Functions, Categories, and Subcategories to organize its recommendations, considerations, and other information regarding incident response as a CSF 2.0 Community Profile. Doing so provides a common taxonomy that is already widely used for communicating about incident response and cybersecurity risk management and governance. This also enables organizations to access a range of online resources mapped to each Function, Category, and Subcategory through the NIST Cybersecurity and Privacy Reference Tool (CPRT). These resources include mappings to other incident response and cybersecurity risk management standards and guidance, as well as sources of implementation guidance that organizations can choose to utilize as needed.

Organizations should use the incident response life cycle framework or model that suits them best. The model in this document is based on CSF 2.0 to take advantage of the wealth of resources available for CSF 2.0 and aid organizations that are already using the CSF. Regardless of the incident response life cycle framework or model used, every organization should take incident response into consideration throughout their cybersecurity risk management activities.

1. Introduction

Within this document, an *event* is any observable occurrence that involves computing assets, including physical and virtual platforms, networks, services, and cloud environments. Examples of events are user login attempts, the installation of software updates, and an application responding to a transaction request. Many events focus on security or have security implications. *Adverse events* are any events associated with a negative consequence regardless of cause, including natural disasters, power failures, or cybersecurity attacks. This guide addresses only *adverse cybersecurity events*. Additional analysis is often needed to determine whether adverse cybersecurity events indicate that a cybersecurity incident has occurred.

A *cybersecurity incident* (or simply *incident*) is

> …an occurrence that actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies. [FISMA2014]

Examples of incidents include an attacker:

- Employing a botnet to send high volumes of connection requests to an internet-facing service, making it unavailable to legitimate service users
- Obtaining administrative credentials at a software-as-a-service provider, which puts sensitive tenant data entrusted to that provider at risk
- Intruding upon an organization's business network to steal credentials and use them to instruct industrial control systems to shut down or destroy critical physical components, causing a major service disruption
- Deploying ransomware to prevent the use of computer systems and cause multiple data breaches by copying files from those systems
- Using phishing emails to compromise user accounts and using those accounts to commit financial fraud
- Identifying a new vulnerability in network management appliances and exploiting the vulnerability to gain unauthorized access to network communications
- Compromising a vendor's software, which is subsequently distributed to customers in its compromised state

Because of the damage that cybersecurity incidents can inflict on organizations and their customers, business partners, and others, it is vital to respond quickly and effectively when an incident occurs. Effective implementation of incident response processes enables systematic responses to and recovery from incidents by analyzing information and taking appropriate action. This reduces cybersecurity and enterprise risks by minimizing data loss or theft, the disruption of services, and the overall impact of incidents. Lessons learned from incident response activities and root cause analysis help improve cybersecurity risk management and

governance efforts and ensure that the organization is better prepared to identify its current technology assets and cybersecurity risks, protect its assets, and detect, respond to, and recover from future incidents.

1.1. Purpose and Scope

This publication seeks to help organizations incorporate cybersecurity incident response recommendations and considerations throughout their cybersecurity risk management activities. It also provides a common language that all organizations can use to communicate internally and externally regarding their incident response plans and activities.

The scope of this publication differs significantly from previous versions. Because the details of how to perform incident response activities change so often and vary so much across technologies, environments, and organizations, it is no longer feasible to capture and maintain that information in a single static publication. Instead, this version focuses on improving cybersecurity risk management for all of the NIST Cybersecurity Framework (CSF) 2.0 Functions [CSF2.0] to better support an organization's incident response capabilities.

Readers are encouraged to utilize other NIST resources in conjunction with this document, including the CSF 2.0 publication and supplemental resources, the Incident Response project page, and mappings to additional sources of information on implementing incident response considerations available through the NIST Cybersecurity and Privacy Reference Tool (CPRT). An example of a CPRT mapping is associating CSF 2.0 outcomes with NIST Special Publication (SP) 800-53 controls that can be implemented to help achieve the outcomes. In this way, CSF 2.0 provides a common language that facilitates access to a large number of other resources.

This publication supersedes SP 800-61r2 (Revision 2), *Computer Security Incident Handling Guide* [SP800-61r2].

1.2. Document Structure

The remainder of this document is organized into the following sections and appendices:

- Section 2 discusses how incident response has evolved to become a critical part of cybersecurity risk management, as well as how the concept of the incident response life cycle has changed to reflect that.
- Section 3 presents incident response recommendations and considerations for an organization's cybersecurity risk management practices. They are organized and documented as a CSF 2.0 Community Profile.
- The References section lists references cited throughout this publication.
- Appendix A and Appendix B provide an acronyms list and a glossary, respectively.
- Appendix C contains a change log of the major changes made since the previous revision.

2. Incident Response as Part of Cybersecurity Risk Management

This section explains the fundamental concepts of incident response as an integral part of cybersecurity risk management. Section 2.1 explores the incident response life cycle and proposes a new life cycle model based on CSF 2.0 Functions. Section 2.2 discusses incident response roles and responsibilities both inside and outside an organization. Finally, Section 2.3 briefly examines incident response policies, processes, and procedures.

2.1. Incident Response Life Cycle Model

Fig. 1 depicts the incident response life cycle model illustrated in the previous version of this publication [SP800-61r2].

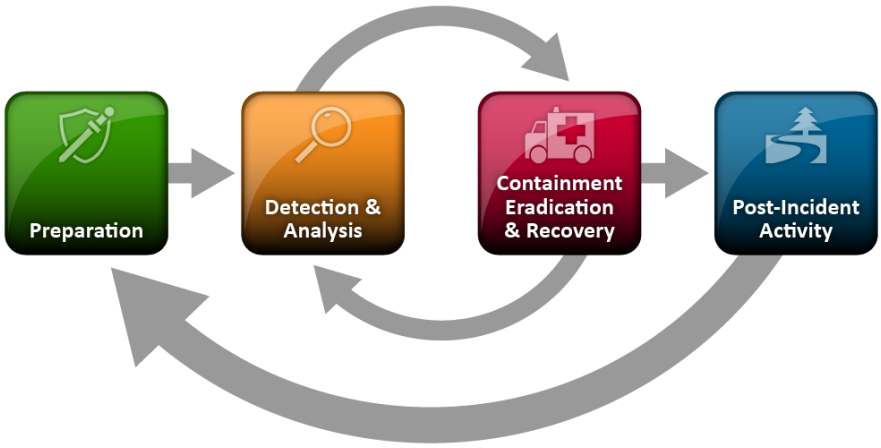

Fig. 1. Previous incident response life cycle model

At that time, incidents were relatively rare, the scope of most incidents was narrow and well-defined, and incident response and recovery was usually completed within a day or two. Under those conditions, it was realistic to treat incident response as a separate set of activities performed by a separate team of personnel and to depict all incident response activities as part of a circular life cycle. Formal post-incident activities would identify needed improvements and feed them into the preparation stage, thus starting the cycle again. Incident response activities were typically intermittent rather than continuous.

However, the current state of incident response has greatly changed since then. Today, incidents occur frequently and cause far more damage. Recovering from them often takes weeks or months due to their breadth, complexity, and dynamic nature. Incident response is now considered a critical part of cybersecurity risk management that should be integrated across organizational operations. The lessons learned during incident response should often be shared as soon as they are identified, not delayed until after recovery concludes. Continuous improvement is increasingly necessary for all facets of cybersecurity risk management in order to keep up with modern threats.

Fig. 2 shows a high-level incident response life cycle model based on the six CSF 2.0 Functions, which organize cybersecurity outcomes at their highest level:

- **Govern (GV):** The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored.
- **Identify (ID):** The organization's current cybersecurity risks are understood.
- **Protect (PR):** Safeguards to manage the organization's cybersecurity risks are used.
- **Detect (DE):** Possible cybersecurity attacks and compromises are found and analyzed.
- **Respond (RS):** Actions regarding a detected cybersecurity incident are taken.
- **Recover (RC):** Assets and operations affected by a cybersecurity incident are restored.

All six Functions have vital roles in incident response. Govern, Identify, and Protect help organizations prevent some incidents, prepare to handle incidents that do occur, reduce the impact of those incidents, and improve incident response and cybersecurity risk management practices based on lessons learned. Detect, Respond, and Recover help organizations discover, manage, prioritize, contain, eradicate, and recover from cybersecurity incidents, as well as perform incident reporting, notification, and other incident-related communications.

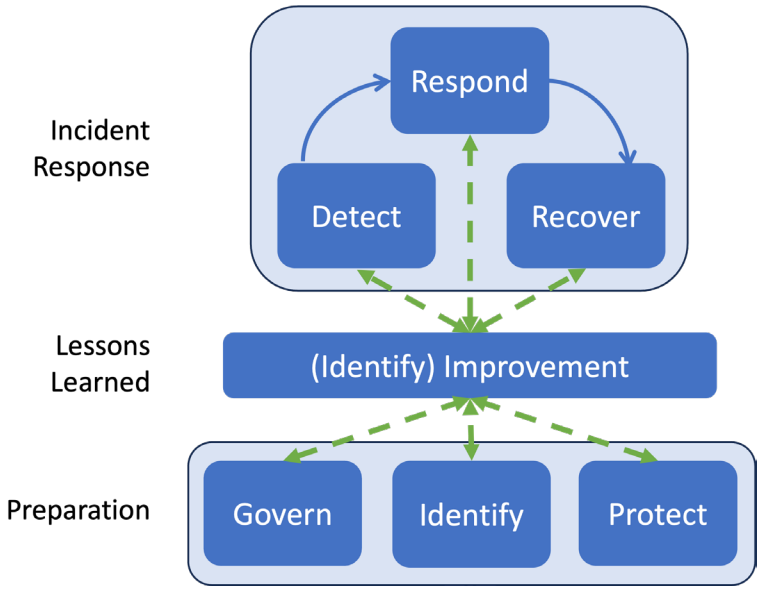

Fig. 2. Incident response life cycle model based on CSF 2.0 Functions

The bottom level reflects that the preparation activities of Govern, Identify, and Protect are not part of the incident response itself. Rather, they are much broader cybersecurity risk management activities that also support incident response. Incident response is shown in the top level of the figure: Detect, Respond, and Recover. Additionally, the need for continuous improvement is indicated as the middle level with the Improvement Category (ID.IM) within the Identify Function and the dashed green lines. Lessons learned from performing all activities in all Functions are fed into Improvement, and those lessons are analyzed, prioritized, and used to inform all of the Functions. This reflects that organizations can learn new lessons at all times

(e.g., detecting the presence of a new threat and characterizing its behavior) and communicate those lessons to the appropriate personnel so that the organization's incident response and other cybersecurity risk management policies, processes, and practices can be adjusted as needed.

Table 1 maps the previous SP 800-61 incident response life cycle model's phases to the corresponding CSF 2.0 Functions used in this document.

Table 1. Previous incident response life cycle model's phases and corresponding CSF 2.0 Functions

Previous Incident Response Life Cycle Model Phase	CSF 2.0 Functions
Preparation	Govern
	Identify (all Categories)
	Protect
Detection & Analysis	Detect
	Identify (Improvement Category)
Containment, Eradication & Recovery	Respond
	Recover
	Identify (Improvement Category)
Post-Incident Activity	Identify (Improvement Category)

Organizations should use the incident response life cycle framework or model that suits them best. The model in this document is based on CSF 2.0 to take advantage of the wealth of resources available for CSF 2.0 and aid organizations that are already using the CSF. The appropriate incident response life cycle framework or model for an organization depends on many factors; for example, larger and more technology-dependent organizations are likely to benefit more from using a framework or model emphasizing continuous improvement than other organizations would. Regardless of the incident response life cycle framework or model used, every organization should take incident response into consideration throughout their cybersecurity risk management activities.

2.2. Incident Response Roles and Responsibilities

In the past, incident response activities were performed almost exclusively by incident handlers from the organization's own incident response team. Today, while incident handlers are still critically important, most organizations increasingly recognize that the success of their incident response efforts depend on the participation of many internal and external parties who hold a wide variety of roles and responsibilities and may be spread around the world. Roles and responsibilities will differ for each organization and may also differ within an organization based on the nature of a particular incident.

Examples of incident response roles and responsibilities include the following:

- **Leadership.** The organization's leadership team oversees incident response, allocates funding, and may have decision-making authority on high-impact response actions, such as shutting down or rebuilding critical services.
- **Incident handlers.** Incident handlers verify that an incident has occurred, collect and analyze data and evidence, prioritize incident response activities, and act appropriately to limit damage, find root causes, and restore operations. Incident handlers also often provide input to others on mitigating cybersecurity issues and improving resiliency. An organization's incident handlers might be:
  - On staff (e.g., an incident response team),
  - On contract (e.g., outsourcing a security operations center [SOC] to a managed security services provider [MSSP] or leveraging a cloud service provider's incident response team when an incident occurs within that provider's cloud), and/or
  - Available when needed (e.g., from a parent organization, a cybersecurity services provider, a business partner, or a law enforcement agency).

  Many organizations may use more than one of these approaches, such as internally performing basic incident response and engaging third-party resources for assistance with certain incidents. Larger organizations may have multiple incident response teams, with each team responsible for a particular logical or physical segment of the organization. When this model is employed, the teams should be part of a single coordinated entity (e.g., a federation) to ensure that incident response processes, procedures, and training are consistent across the organization and that information is shared among teams.
- **Technology professionals.** Cybersecurity, privacy, system, network, cloud, and other technology architects, engineers, and administrators, as well as software developers, may be involved in incident response and recovery efforts.
- **Legal.** Legal experts can review incident response plans, policies, and procedures to ensure compliance with applicable laws and regulations, including the right to privacy. Legal experts can also review contracts with technology suppliers and other third parties when there are incident response implications. In addition, incident responders can seek guidance from their organization's legal department if a particular incident may have legal ramifications, such as the prosecution of a suspect, lawsuits, or situations that require a memorandum of understanding (MOU) or other binding agreement.
- **Public affairs and media relations.** Depending on the nature and impact of an incident, it may be necessary to inform the media and, by extension, the public. Sometimes, the media learns of incidents through alternate sources (i.e., not through public affairs personnel). Having a media engagement strategy in place can greatly aid in this situation.

- **Human resources.** Certain human resources practices should consider cybersecurity risk management, including pre-employment screening and employee onboarding, offboarding, and position changes. Human resources may also be involved if an employee is suspected of intentionally causing an incident.
- **Physical security and facilities management.** Some computer security incidents occur through physical security breaches or involve coordinated logical and physical attacks. The incident response team may also need access to facilities during incident handling (e.g., to access a compromised workstation in a locked office).
- **Asset owners.** Asset owners (e.g., system owners, data owners, and business process owners) may have valuable insights on response and recovery priorities for their affected assets. They also need to be kept up to date on the status of response and recovery efforts.

Third parties may be under contract with an organization to help perform incident response activities. Some third parties may fill a primary role (e.g., an MSSP performing incident detection, response, and recovery activities), while other parties (e.g., cloud service providers [CSPs] and internet service providers [ISPs]) may be involved in certain incident response activities for particular types of incidents. This is a **shared responsibility model** in which the organization transfers some of its responsibilities to a provider. These responsibilities should be clearly defined in a contract, and the incident response team should be aware of the division of responsibilities, including information flows, coordination, and authority to act on behalf of the organization. This also includes restrictions on what the service provider can do, such as sharing sanitized incident information with other customers or making and implementing operational decisions (e.g., immediately deactivating certain services to contain an incident).

A service provider may detect malicious activity sooner than individual organizations would because it can correlate events across its customers. In some situations, a service provider might be able to use knowledge of an incident with one customer to proactively prevent similar incidents with its other customers. Service providers often have privileged access to organizational systems and may also have access to sensitive organizational data. Accordingly, the risk of malicious insiders or the service provider being compromised should be considered and addressed. Non-disclosure agreements (NDAs) and contracting clauses are options for deterring the unauthorized disclosure of sensitive data.

2.3. Incident Response Policies, Processes, and Procedures

Organizations should have policies that govern their cybersecurity incident response. While a policy is highly individualized to the organization, most incident response policies include the same key elements:

- Statement of management commitment
- Purpose and objectives of the policy
- Scope of the policy (i.e., to whom and what it applies and under what circumstances)

- Definition of events, cybersecurity incidents, investigations, and related terms
- Roles, responsibilities, and authorities, such as which roles have the authority to confiscate, disconnect, or shut down technology assets
- Guidelines for prioritizing incidents, estimating their severity, initiating recovery processes, maintaining or restoring operations, and other key actions
- Performance measures

Processes and procedures should be based on the incident response policy and plan. Documented procedures should explain how technical processes and other operating procedures should be performed. Procedures can be tested or exercised periodically to verify their accuracy and can be used to help train new personnel. While it is impossible to have detailed procedures for every possible situation, organizations should consider documenting procedures for responding to the most common types of incidents and threats. Organizations should also develop and maintain procedures for particularly important processes that may be urgently needed during emergency situations, such as redeploying the organization's primary authentication platform.

Many organizations choose to create playbooks as part of documenting their procedures. Playbooks provide actionable steps or tasks for people to perform during various scenarios or situations. Formatting procedures within a playbook instead of another format can improve their usability. See the Cybersecurity and Infrastructure Security Agency (CISA) *Cybersecurity Incident & Vulnerability Response Playbooks* [CISA-PB] for incident response playbook examples.

3. CSF 2.0 Community Profile for Cyber Incident Risk Management

A *CSF Community Profile* is a baseline of CSF outcomes that is created and published to address shared interests and goals for reducing cybersecurity risk among a number of organizations. A Community Profile is typically developed for a particular sector, subsector, technology, threat type, or other use case [CSF2.0].

This section defines NIST's CSF 2.0 Community Profile for cyber incident risk management. It uses the CSF Core as the basis for highlighting and prioritizing cybersecurity outcomes that are important for incident response, makes recommendations, and provides other supporting information for certain CSF outcomes within the context of incident response [CSWP32]. The Community Profile is split into two tables: Table 2 covers Preparation (Govern, Identify, and Protect) and Lessons Learned (Identify-Improvement), while Table 3 covers Incident Response (Detect, Respond, and Recover).

Each CSF 2.0 Function, Category, and Subcategory has its own row in one of the two tables. Each row's relative priority **within the context of incident response** is indicated by one of the following:

- **High:** Functions as a core incident response activity for most organizations
- **Medium:** Directly supports incident response activities for most organizations
- **Low:** Indirectly supports incident response activities for most organizations

These priorities are intended as a starting point for organizations, who are encouraged to customize this Community Profile to reflect their own priorities and needs.

The last column may contain one or more items that recommend what to do or describe additional considerations or supporting information for some rows. Each item in that column has an ID starting with one of the following:

- "R" (recommendation: something the organization should do)
- "C" (consideration: something the organization should consider doing)
- "N" (note: additional information besides recommendations and considerations)

An R, C, or N designation and its number can be appended to the row's CSF ID to create an identifier that is unique within the Community Profile (e.g., "GV.OC-03.R1" is recommendation 1 for CSF Subcategory GV.OC-03).

Recommendations, considerations, and notes made at a higher level of the CSF (Function or Category) also apply to their component elements (Categories or Subcategories).

The recommendations, considerations, and notes supplement what the CSF 2.0 already provides through its documents and online resources. The recommendations, considerations, and notes are not comprehensive, and not all of them will be applicable to every organization. Technologies mentioned in recommendations, considerations, and notes are examples as of this writing and may become outdated.

Some recommendations, considerations, and notes use terms that are not defined in this publication (e.g., "data breach"). Organizations that adopt the Community Profile should define these terms in the context of their own environments, use cases, and applicable laws and regulations. Readers may also choose to consult NIST's glossary, which contains an aggregation of terms and definitions from numerous NIST standards, guidelines, and other publications.

The Community Profile is intended for use by most organizations, regardless of sector, size, or other factors. Additional versions of this Community Profile could be developed for narrower audiences, such as federal agencies, small businesses, or educational institutions. For more information on CSF 2.0 Community Profiles, see the Framework Resource Center.

3.1. Preparation and Lessons Learned

Table 2 contains the first part of the Community Profile: Preparation and Lessons Learned, which both support the Incident Response part of the Community Profile defined in Table 3.

> Note: Most of the CSF elements in this part of the Profile are not specific to executing incident response activities, so they have lower priorities with respect to incident response and do not contain recommendations or considerations. **This does not imply that they are unnecessary for organizations to achieve, but rather that they are outside of the direct scope of responding to incidents.**

Table 2. CSF 2.0 Community Profile part 1: Preparation and Lessons Learned

CSF Element	CSF Element Description	Priority	Recommendations, Considerations, Notes
GV (Govern)	The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored	Low	
GV.OC (Organizational Context)	The circumstances — mission, stakeholder expectations, dependencies, and legal, regulatory, and contractual requirements — surrounding the organization's cybersecurity risk management decisions are understood	Low	
GV.OC-01	The organizational mission is understood and informs cybersecurity risk management	Low	
GV.OC-02	Internal and external stakeholders are understood, and their needs and expectations regarding cybersecurity risk management are understood and considered	Low	
GV.OC-03	Legal, regulatory, and contractual requirements	Medium	**R1:** Cybersecurity requirements should include all requirements related to incident

CSF Element	CSF Element Description	Priority	Recommendations, Considerations, Notes
	regarding cybersecurity — including privacy and civil liberties obligations — are understood and managed		notifications, data breach reporting, and other aspects of incident response.
GV.OC-04	Critical objectives, capabilities, and services that external stakeholders depend on or expect from the organization are understood and communicated	Medium	**N1:** Understanding critical external dependencies on the organization's operations can aid in prioritizing response and recovery efforts.
GV.OC-05	Outcomes, capabilities, and services that the organization depends on are understood and communicated	Medium	**N1:** Understanding critical dependencies on external resources (e.g., cloud-based hosting providers and managed service providers) can aid in prioritizing response and recovery efforts.
GV.RM (Risk Management Strategy)	The organization's priorities, constraints, risk tolerance and appetite statements, and assumptions are established, communicated, and used to support operational risk decisions	Low	
GV.RM-01	Risk management objectives are established and agreed to by organizational stakeholders	Low	
GV.RM-02	Risk appetite and risk tolerance statements are established, communicated, and maintained	Low	
GV.RM-03	Cybersecurity risk management activities and outcomes are included in enterprise risk management processes	Medium	**R1:** Have processes in place so that incident-related decision-making will be informed by other types of risks that the organization faces (e.g., privacy, operational, safety, reputational, AI) and not just cybersecurity risks in isolation.
GV.RM-04	Strategic direction that describes appropriate risk response options is established and communicated	Low	
GV.RM-05	Lines of communication across the organization are established for cybersecurity risks, including risks from suppliers and other third parties	Low	
GV.RM-06	A standardized method for calculating, documenting, categorizing, and prioritizing cybersecurity risks is established and communicated	Medium	**N1:** Having a standardized method for calculating cybersecurity risks can aid in prioritizing response and recovery efforts and in comparing the estimated and actual impacts of incidents. **N2:** Such a method can also be used to establish criteria and inform decision

CSF Element	CSF Element Description	Priority	Recommendations, Considerations, Notes
			making on when to escalate or elevate incident response activities.
GV.RM-07	Strategic opportunities (i.e., positive risks) are characterized and are included in organizational cybersecurity risk discussions	Low	
GV.RR (Roles, Responsibilities, and Authorities)	Cybersecurity roles, responsibilities, and authorities to foster accountability, performance assessment, and continuous improvement are established and communicated	Medium	**R1:** Cybersecurity roles, responsibilities, and authorities should include incident response.
GV.RR-01	Organizational leadership is responsible and accountable for cybersecurity risk and fosters a culture that is risk-aware, ethical, and continually improving	Medium	**R1:** See the recommendation for GV.RR.
GV.RR-02	Roles, responsibilities, and authorities related to cybersecurity risk management are established, communicated, understood, and enforced	Medium	**N1:** Roles and responsibilities that involve cybersecurity incident response typically exist throughout an organization and often include third parties (e.g., those under contract) to help perform incident response activities for the organization. **R1:** All roles and responsibilities involving cybersecurity incident response should be documented in an organization's policies. **R2:** All appropriate individuals or parties should be designated the authority necessary to fulfill their incident response-related responsibilities. **R3:** See the recommendation for GV.RR.
GV.RR-03	Adequate resources are allocated commensurate with the cybersecurity risk strategy, roles, responsibilities, and policies	Low	
GV.RR-04	Cybersecurity is included in human resources practices	Low	
GV.PO (Policy)	Organizational cybersecurity policy is established, communicated, and enforced	High	**R1:** Cybersecurity policies should include an incident response policy.
GV.PO-01	Policy for managing cybersecurity risks is established based on organizational context, cybersecurity strategy, and priorities and is communicated and enforced	Low	
GV.PO-02	Policy for managing cybersecurity risks is reviewed,	Low	

CSF Element	CSF Element Description	Priority	Recommendations, Considerations, Notes
	updated, communicated, and enforced to reflect changes in requirements, threats, technology, and organizational mission		
GV.OV (Oversight)	Results of organization-wide cybersecurity risk management activities and performance are used to inform, improve, and adjust the risk management strategy	Low	
GV.OV-01	Cybersecurity risk management strategy outcomes are reviewed to inform and adjust strategy and direction	Medium	**R1:** Take past cybersecurity incidents into account when adjusting the organization's cybersecurity risk management strategy and direction.
GV.OV-02	The cybersecurity risk management strategy is reviewed and adjusted to ensure coverage of organizational requirements and risks	Medium	**R1:** Take risks from past cybersecurity incidents into account when reviewing the organization's cybersecurity risk management strategy.
GV.OV-03	Organizational cybersecurity risk management performance is evaluated and reviewed for adjustments needed	Low	
GV.SC (Cybersecurity Supply Chain Risk Management)	Cyber supply chain risk management processes are identified, established, managed, monitored, and improved by organizational stakeholders	Low	
GV.SC-01	A cybersecurity supply chain risk management program, strategy, objectives, policies, and processes are established and agreed to by organizational stakeholders	Low	
GV.SC-02	Cybersecurity roles and responsibilities for suppliers, customers, and partners are established, communicated, and coordinated internally and externally	Low	**N1:** See GV.RR-02 for additional information on cybersecurity incident response-related roles and responsibilities for third parties.
GV.SC-03	Cybersecurity supply chain risk management is integrated into cybersecurity and enterprise risk management, risk assessment, and improvement processes	Low	
GV.SC-04	Suppliers are known and prioritized by criticality	Low	

CSF Element	CSF Element Description	Priority	Recommendations, Considerations, Notes
GV.SC-05	Requirements to address cybersecurity risks in supply chains are established, prioritized, and integrated into contracts and other types of agreements with suppliers and other relevant third parties	Medium	**R1:** Cybersecurity supply chain risk management requirements should include cybersecurity performance and vulnerability, threat, and incident disclosure and information sharing.
GV.SC-06	Planning and due diligence are performed to reduce risks before entering into formal supplier or other third-party relationships	Low	
GV.SC-07	The risks posed by a supplier, their products and services, and other third parties are understood, recorded, prioritized, assessed, responded to, and monitored over the course of the relationship	Low	
GV.SC-08	Relevant suppliers and other third parties are included in incident planning, response, and recovery activities	Medium	**N1:** The GV.SC-08 Subcategory is specific to incident planning, response, and recovery. **N2:** See ID.IM-02 for more information on tests and exercises.
GV.SC-09	Supply chain security practices are integrated into cybersecurity and enterprise risk management programs, and their performance is monitored throughout the technology product and service life cycle	Low	
GV.SC-10	Cybersecurity supply chain risk management plans include provisions for activities that occur after the conclusion of a partnership or service agreement	Low	
ID (Identify)	The organization's current cybersecurity risks are understood	Medium	**N1:** All Identify Categories are beneficial for preventing, responding to, and recovering from incidents.
ID.AM (Asset Management)	Assets (e.g., data, hardware, software, systems, facilities, services, people) that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy	Medium	**N1:** All asset management information can be helpful to incident responders in many ways, such as understanding the impact of an incident, identifying other assets that may be targeted, and prioritizing response and recovery efforts.
ID.AM-01	Inventories of hardware managed by the organization are maintained	Medium	**R1:** Make current and automatically updated inventories of the internal and external hardware used by the organization

CSF Element	CSF Element Description	Priority	Recommendations, Considerations, Notes
			available for use in finding and addressing vulnerabilities, monitoring operations and usage to detect adverse cybersecurity events, and identifying "shadow IT" usage.
ID.AM-02	Inventories of software, services, and systems managed by the organization are maintained	Medium	**R1:** Make current and automatically updated inventories of the internal and external software, services, and systems used by the organization available for use in finding and addressing vulnerabilities, monitoring operations and usage to detect adverse cybersecurity events, and identifying "shadow IT" usage.
ID.AM-03	Representations of the organization's authorized network communication and internal and external network data flows are maintained	Medium	**N1:** Maintaining network data flow representations can improve the accuracy of detecting malicious data flows and communication. **C1:** Consider leveraging automation and zero trust architectures to automatically create and maintain network data flow representations.
ID.AM-04	Inventories of services provided by suppliers are maintained	Medium	**R1:** Current and automatically updated inventories of the services provided by the organization's suppliers should be available for use in finding and addressing vulnerabilities, monitoring operations and usage to detect adverse cybersecurity events, and identifying "shadow IT" usage.
ID.AM-05	Assets are prioritized based on classification, criticality, resources, and impact on the mission	Medium	**R1:** Prioritizing the organization's assets — including hardware, software, services, systems, and data — and being aware of the dependencies between those and other assets should help indicate where the organization should focus its resources in terms of protection, detection, response, and recovery.
ID.AM-07	Inventories of data and corresponding metadata for designated data types are maintained	Medium	**R1:** Having data inventories that include data classifications, owners, and logical and physical locations should provide valuable information on what data may have been involved in an incident.
ID.AM-08	Systems, hardware, software, services, and data are managed throughout their life cycles	Medium	**R1:** Managing hardware, software, services, and systems throughout their life cycles should take cybersecurity into consideration, such as configuring them securely, reducing attack surfaces, and updating inventory information as assets are transferred or relocated.
ID.RA (Risk Assessment)	The cybersecurity risk to the organization, assets, and individuals is understood by the organization	Medium	**N1:** Risk assessment practices are critical for reducing the number of incidents that occur and the impacts they cause. Risk assessment is a vast topic that is outside of

CSF Element	CSF Element Description	Priority	Recommendations, Considerations, Notes
			the scope of this Profile other than to summarize its importance for incident response. **N2:** See [SP800-37r2] for more information on cybersecurity risk. **N3:** See [SP800-30r1] for more information on cybersecurity risk assessment.
ID.RA-01	Vulnerabilities in assets are identified, validated, and recorded	Medium	**R1:** Understand current known cybersecurity vulnerabilities to make informed decisions when assessing risks. This should include all types of known cybersecurity vulnerabilities, such as flaws in software (including firmware and software-based services) developed by the organization and third parties, software misconfigurations, network and system design and implementation weaknesses, physical vulnerabilities and resilience issues in facilities that house computing assets, and integrity violations in hardware and software (e.g., counterfeit, evidence of tampering). **N1:** See the notes for ID.RA.
ID.RA-02	Cyber threat intelligence is received from information sharing forums and sources	High	**N1:** Cyber threat intelligence (CTI) is threat information that has been aggregated, transformed, analyzed, interpreted, or enriched to provide the necessary context for decision-making processes. Organizations can receive CTI from automated CTI feeds, information sharing forums, and other sources. **N2:** CTI is useful for incident response and recovery in several ways, including obtaining information on new threats, improving the accuracy of cybersecurity technologies with incident detection or response capabilities, and understanding the tactics, techniques, and procedures (TTPs) used by attackers. TTPs describe the behavior of an actor. Information on threats and their TTPs is widely available through repositories and knowledge bases. **N3:** [SP800-150] provides guidelines on consuming, using, and storing CTIs, as well as establishing CTI relationships. **N4:** See the notes for ID.RA.
ID.RA-03	Internal and external threats to the organization are identified and recorded	Medium	**R1:** Identify internal and external threats during routine operations and from CTI. **N1:** Other possible methods that organizations could consider for identifying

CSF Element	CSF Element Description	Priority	Recommendations, Considerations, Notes
			threats include threat hunting and the use of deception technologies. **N2:** See the notes for ID.RA.
ID.RA-04	Potential impacts and likelihoods of threats exploiting vulnerabilities are identified and recorded	Medium	**N1:** Recording the potential impacts and likelihoods of threats exploiting vulnerabilities is necessary for determining risk. **N2:** See the notes for ID.RA.
ID.RA-05	Threats, vulnerabilities, likelihoods, and impacts are used to understand inherent risk and inform risk response prioritization	High	**R1:** Organizations with mechanisms in place for estimating cybersecurity risk as part of their cybersecurity risk management programs should use those mechanisms for incident response purposes. **C1:** Consider using threat modeling and other methods to inform the understanding of attack vectors, attack surfaces, and lateral paths through organizational assets, among other factors that contribute to risk. **N1:** See the notes for ID.RA.
ID.RA-06	Risk responses are chosen, prioritized, planned, tracked, and communicated	High	**N1:** Risk responses are needed to prevent future incidents from occurring and existing incidents from reoccurring. **R1:** The organization's policies, processes, and procedures should provide guidance (e.g., criteria) for making decisions regarding appropriate risk responses in various situations. **N2:** The four types of risk responses are 1) Accept (accept the risk as is), 2) Mitigate (reduce the risk by eliminating the vulnerabilities and/or deploying additional security controls to reduce vulnerability exploitation), 3) Transfer (reduce the risk by sharing some of the consequences with another party), and 4) Avoid (ensure that the risk does not occur by eliminating the attack surface). **N3:** See [IR8286] for more information on risk responses. **N4:** See the notes for ID.RA.
ID.RA-07	Changes and exceptions are managed, assessed for risk impact, recorded, and tracked	Medium	**N1:** See the notes for ID.RA.
ID.RA-08	Processes for receiving, analyzing, and responding to vulnerability disclosures are established	Medium	**N1:** A vulnerability disclosure is when a third party reports a suspected vulnerability in one of the organization's systems to the organization. **N2:** See [SP800-216] for more information on vulnerability disclosure. **N3:** See Section 4.5.2 of [SP800-150] for guidance on using data formats that may

CSF Element	CSF Element Description	Priority	Recommendations, Considerations, Notes
			assist with maintaining cross-references between asset inventories and sources of vulnerability disclosures. **N4:** See the notes for ID.RA.
ID.RA-09	The authenticity and integrity of hardware and software are assessed prior to acquisition and use	Medium	**N1:** See the notes for ID.RA.
ID.RA-10	Critical suppliers are assessed prior to acquisition	Low	**N1:** See the notes for ID.RA.
ID.IM (Improvement)	Improvements to organizational cybersecurity risk management processes, procedures, and activities are identified across all CSF Functions	Medium	**N1:** See the note for ID.
ID.IM-01	Improvements are identified from evaluations	Medium	**R1:** Periodically evaluate incident response program performance to identify problems and deficiencies that should be corrected. **N1:** Possible evaluation forms include self-assessments, third-party assessments, and independent audits.
ID.IM-02	Improvements are identified from security tests and exercises, including those done in coordination with suppliers and relevant third parties	High	**N1:** Incident response exercises and tests may provide helpful information for program evaluation and prepare staff and involved third parties (e.g., critical service providers and product suppliers) for future incident response activities. **N2:** See [SP800-84] for more information on simulations, tabletop discussions, and other forms of exercises.
ID.IM-03	Improvements are identified from the execution of operational processes, procedures, and activities	High	**N1:** The execution of operational processes, procedures, and activities includes all incident response and recovery efforts. **N2:** Improvements that affect incident response can be made to the incident response program itself (e.g., plan, policy, processes, procedures) or to other aspects of the organization's cybersecurity risk management activities (e.g., identifying TTPs that are not currently being blocked by safeguards or flagged by detection technologies). **N3:** Improvements are often identified when creating follow-up reports for incidents or holding "lessons learned" meetings when an incident's recovery efforts are concluding, especially if the incident was major. This provides an opportunity to review what happened, what actions were taken, and how effective those actions were, as well as hear from all

CSF Element	CSF Element Description	Priority	Recommendations, Considerations, Notes
			parties involved in the incident. Such a meeting can help identify and prioritize potential improvements to the organization's incident response program and cybersecurity risk management efforts.
ID.IM-04	Incident response plans and other cybersecurity plans that affect operations are established, communicated, maintained, and improved	High	**N1:** Several types of cybersecurity plans are relevant to incident response, including 1) incident response plans, which provide the roadmap for implementing the incident response capability; 2) vulnerability management plans, which help identify and assess all types of vulnerabilities and prioritize, test, and implement risk responses; and 3) business continuity plans. **R1:** Synchronize business continuity plans with incident response plans since incidents can undermine business resilience. **R2:** Review and update all cybersecurity plans periodically or when a need for significant improvements is identified. **R3:** Base each cybersecurity plan on the organization's unique requirements, mission, size, structure, and functions. **R4:** Each cybersecurity plan should identify the resources and management support needed to carry it out successfully. **N2:** Business continuity planning professionals who are made aware of cybersecurity incidents and their impacts can fine-tune business impact assessments, risk assessments, and continuity of operations plans. Further, because business continuity planners have extensive expertise in minimizing operational disruption during severe circumstances, they may be valuable in planning responses to specific incident types, such as denial-of-service (DoS) conditions.
PR (Protect)	Safeguards to manage the organization's cybersecurity risks are used	Medium	**N1:** Lowering the number of incidents shortens operational disruptions, allows response teams to focus on high-impact situations, and reduces the impact of incidents that do occur (e.g., by making it harder for attackers to move laterally throughout an environment and, thus, slowing them down). **N2:** Understanding the protection mechanisms in place can help personnel deploy methods to detect protection failures and bypasses.

CSF Element	CSF Element Description	Priority	Recommendations, Considerations, Notes
			N3: It is outside of the scope of this Profile to provide recommendations and considerations on protecting assets, other than a few notes of practices that specifically benefit incident response activities.
PR.AA (Identity Management, Authentication, and Access Control)	Access to physical and logical assets is limited to authorized users, services, and hardware and managed commensurate with the assessed risk of unauthorized access	Medium	**N1:** See the notes for PR.
PR.AA-01	Identities and credentials for authorized users, services, and hardware are managed by the organization	Medium	**N1:** See the notes for PR.
PR.AA-02	Identities are proofed and bound to credentials based on the context of interactions	Medium	**N1:** See the notes for PR.
PR.AA-03	Users, services, and hardware are authenticated	Medium	**N1:** See the notes for PR.
PR.AA-04	Identity assertions are protected, conveyed, and verified	Medium	**N1:** See the notes for PR.
PR.AA-05	Access permissions, entitlements, and authorizations are defined in a policy, managed, enforced, and reviewed, and incorporate the principles of least privilege and separation of duties	Medium	**N1:** See the notes for PR.
PR.AA-06	Physical access to assets is managed, monitored, and enforced commensurate with risk	Medium	**N1:** See the notes for PR.
PR.AT (Awareness and Training)	The organization's personnel are provided with cybersecurity awareness and training so that they can perform their cybersecurity-related tasks	Medium	**N1:** See the notes for PR.
PR.AT-01	Personnel are provided with awareness and training so that they possess the knowledge and skills to perform general tasks with cybersecurity risks in mind	Medium	**N1:** See the notes for PR.
PR.AT-02	Individuals in specialized roles are provided with awareness and training so that they possess the knowledge and skills to perform relevant tasks with cybersecurity risks in mind	Medium	**R1:** Role-based training should include incident-related responsibilities. **N1:** See the notes for PR.

CSF Element	CSF Element Description	Priority	Recommendations, Considerations, Notes
PR.DS (Data Security)	Data are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information	Medium	**N1:** See the notes for PR.
PR.DS-01	The confidentiality, integrity, and availability of data-at-rest are protected	Medium	**N1:** See the notes for PR.
PR.DS-02	The confidentiality, integrity, and availability of data-in-transit are protected	Medium	**N1:** See the notes for PR.
PR.DS-10	The confidentiality, integrity, and availability of data-in-use are protected	Medium	**N1:** See the notes for PR.
PR.DS-11	Backups of data are created, protected, maintained, and tested	High	**N1:** Backups can be particularly important for recovery purposes when data integrity or availability is affected. **N1:** See the notes for PR.
PR.PS (Platform Security)	The hardware, software (e.g., firmware, operating systems, applications), and services of physical and virtual platforms are managed consistent with the organization's risk strategy to protect their confidentiality, integrity, and availability	Medium	**N1:** See the notes for PR.
PR.PS-01	Configuration management practices are established and applied	Medium	**N1:** See the notes for PR.
PR.PS-02	Software is maintained, replaced, and removed commensurate with risk	Medium	**N1:** See the notes for PR.
PR.PS-03	Hardware is maintained, replaced, and removed commensurate with risk	Medium	**N1:** See the notes for PR.
PR.PS-04	Log records are generated and made available for continuous monitoring	Medium	**N1:** Logs are particularly important for recording and preserving information that is vital to incident detection, response, and recovery activities. **N2:** For more information on log management, see [SP800-92r1]. **N3:** See the notes for PR.
PR.PS-05	Installation and execution of unauthorized software are prevented	Medium	**N1:** See the notes for PR.
PR.PS-06	Secure software development practices are integrated, and their performance is monitored throughout the software development life cycle	Medium	**N1:** For more information on secure software development practices, including responding to vulnerabilities or incidents that involve released software, see [SP800-218]. **N2:** See the notes for PR.

CSF Element	CSF Element Description	Priority	Recommendations, Considerations, Notes
PR.IR (Technology Infrastructure Resilience)	Security architectures are managed with the organization's risk strategy to protect asset confidentiality, integrity, and availability, and organizational resilience	Medium	**N1:** See the notes for PR.
PR.IR-01	Networks and environments are protected from unauthorized logical access and usage	Medium	**N1:** See the notes for PR.
PR.IR-02	The organization's technology assets are protected from environmental threats	Medium	**N1:** See the notes for PR.
PR.IR-03	Mechanisms are implemented to achieve resilience requirements in normal and adverse situations	Medium	**N1:** See the notes for PR.
PR.IR-04	Adequate resource capacity to ensure availability is maintained	Medium	**N1:** See the notes for PR.

3.2. Incident Response

Table 3 contains the second part of the Community Profile: Incident Response.

> Note: All of the CSF elements in this part of the Profile are **specific to responding to incidents**, so they have higher priorities with respect to incident response than those in the first part. Accordingly, all CSF elements in this part have recommendations or considerations.

Table 3. CSF 2.0 Community Profile part 2: Incident Response

CSF Element	CSF Element Description	Priority	Recommendations, Considerations, Notes
DE (Detect)	Possible cybersecurity attacks and compromises are found and analyzed	High	**N1:** The Detect Function encompasses all of the monitoring and analysis activities performed to find and characterize potentially adverse events and, in turn, find cybersecurity incidents.
DE.CM (Continuous Monitoring)	Assets are monitored to find anomalies, indicators of compromise, and other potentially adverse events	High	**R1:** Continuous monitoring for unauthorized activity, deviations from expected activity, and changes in security posture should involve the following types of assets at all times: networks and network services; computing hardware and software, runtime environments, and their data; the physical environment; personnel activity and technology usage; and external service provider activities. **C1:** Consider using cyber threat information with continuous monitoring to help identify potentially malicious activities that may have otherwise been considered benign.

CSF Element	CSF Element Description	Priority	Recommendations, Considerations, Notes
			R2: Tune the continuous monitoring technologies to reduce false positives and false negatives to acceptable levels.
DE.CM-01	Networks and network services are monitored to find potentially adverse events	High	**R1:** Monitoring should include wired and wireless networks, network communications and flows, network services (e.g., DNS and BGP), and the presence of unauthorized or rogue networks within facilities.
DE.CM-02	The physical environment is monitored to find potentially adverse events	High	**R1:** Monitoring the physical environment should include all successful and failed access attempts into all controlled areas, the movement of people and equipment into and out of secure areas of facilities, and signs of tampering with physical access controls.
DE.CM-03	Personnel activity and technology usage are monitored to find potentially adverse events	High	**R1:** Monitoring personnel activity and technology usage should include anomalous user activity or unusual patterns of activity, authentication and logical access attempts, and the use of deception technology.
DE.CM-06	External service provider activities and services are monitored to find potentially adverse events	High	**R1:** Monitoring external service provider activities and services should include remote and on-site administration and maintenance activities that providers perform on organizational systems and deviations from expected behavior by cloud-based services, internet service providers, and other service providers.
DE.CM-09	Computing hardware and software, runtime environments, and their data are monitored to find potentially adverse events	High	**R1:** Monitor email, web, file sharing, collaboration services, and other common attack vectors to detect malware, phishing, data leaks, exfiltration, and other adverse events. **R2:** Monitor authentication attempts to identify attacks against credentials and unauthorized credential use. **R3:** Monitor software and hardware configurations for deviations from security baselines. **R4:** Monitor hardware and software, including cybersecurity protection mechanisms, for signs of tampering, failure, or compromise. **R5:** Monitor endpoints for cyber health issues (e.g., missing patches, malware infections, or unauthorized software), and redirect endpoints with issues to a remediation environment before access is authorized.

CSF Element	CSF Element Description	Priority	Recommendations, Considerations, Notes
DE.AE (Adverse Event Analysis)	Anomalies, indicators of compromise, and other potentially adverse events are analyzed to characterize the events and detect cybersecurity incidents	High	**N1:** Adverse event analysis involves studying the data on potentially adverse events collected by continuous monitoring to find possible attacks and compromises and declaring when an incident has occurred so as to initiate incident response activities. **R1:** The volume of potentially adverse events to be analyzed is generally quite high, so organizations should rely on technical solutions that filter large event datasets down to a subset that is suitable for human viewing and analysis. **N2:** The fidelity of events varies based on many factors. Anomalies may have benign or malicious foundations. Some incidents are relatively easy to find amid the noise, while others require deep, specialized technical knowledge and experience. **N3:** CTI can be invaluable in detecting malicious activity early, reducing its impact, and shortening recovery time. Signs of an incident may be more obvious later in the attack life cycle, but the incident's impact and scope may be much larger. **R2:** Organizations should strive to find incidents earlier in the attack life cycle and take a proactive approach to incident detection and response.
DE.AE-02	Potentially adverse events are analyzed to better understand associated activities	High	**R1:** Use tools (e.g., security information and event management [SIEM]; security orchestration, automation, and response [SOAR]) to continuously monitor log events for known malicious and suspicious activity and to generate reports on their findings. **R2:** Utilize up-to-date CTI in log analysis tools to improve detection accuracy and characterize threat actors, their methods, and indicators of compromise. **R3:** Regularly conduct manual reviews of log events for technologies that cannot be sufficiently monitored through automation.
DE.AE-03	Information is correlated from multiple sources	High	**R1:** Constantly transfer the log data generated by other sources to a relatively small number of log servers. **R2:** Use event correlation technology (e.g., SIEM, SOAR) to gather pieces of related data captured by multiple sources. **R3:** Utilize CTI to help correlate events among log sources.

CSF Element	CSF Element Description	Priority	Recommendations, Considerations, Notes
DE.AE-04	The estimated impact and scope of adverse events are understood	High	**R1:** Estimate the impact and scope of adverse events through automated (e.g., SIEM, SOAR) and/or manual means, and review and refine the estimates.
DE.AE-06	Information on adverse events is provided to authorized staff and tools	High	**R1:** Generate alerts and provide them to cybersecurity and incident response tools and staff (e.g., the SOC and incident responders). **R2:** Make log analysis findings accessible to incident responders and other authorized personnel at all times. **R3:** Consider automatically creating and assigning tickets in the organization's ticketing system when certain types of alerts occur.
DE.AE-07	Cyber threat intelligence and other contextual information are integrated into the analysis	High	**R1:** Integrate up-to-date CTI and other contextual information (e.g., asset inventories) into adverse event analysis to improve detection accuracy and characterize threat actors, their methods, and indicators of compromise. **R2:** Rapidly acquire and analyze vulnerability disclosures for the organization's technologies from suppliers, vendors, and third-party security advisories. **N1:** See [SP800-150] for guidelines on consuming, using, and storing CTIs, as well as establishing CTI relationships.
DE.AE-08	Incidents are declared when adverse events meet the defined incident criteria	High	**R1:** Apply incident criteria to known and assumed characteristics of analyzed activity, and consider known false positives to determine whether an incident should be declared.
RS (Respond)	Actions regarding a detected cybersecurity incident are taken	High	**N1:** The Respond Function is at the core of incident response activities.
RS.MA (Incident Management)	Responses to detected cybersecurity incidents are managed	High	**N1:** Incident management involves overseeing responses to all incidents and shifting priorities and resources as needed. Evaluating the overall risk from an incident and applying the appropriate prioritization are perhaps the most critical decision points in the incident response process. **R1:** Because of resource limitations, incidents should not be handled on a first-come, first-served basis. **R2:** Incident triage, prioritization, escalation, and elevation and decisions regarding when to initiate recovery processes should all be based on a set of risk evaluation factors. This set can range

CSF Element	CSF Element Description	Priority	Recommendations, Considerations, Notes
			from simple to incredibly complex, depending on the needs and maturity of an organization. **N2:** Examples of possible risk evaluation factors include asset criticality, functional impact of the incident, data impact of the incident, stage of observed activity, threat actor characterization, and recoverability. **R3:** The incident response status should be tracked for each incident along with pertinent information, such as an incident summary, indicators of compromise related to the incident, the status and expected time frame for each assigned action, and next steps to be taken.
RS.MA-01	The incident response plan is executed in coordination with relevant third parties once an incident is declared	High	**R1:** Detection technologies should automatically report incidents that they have confirmed. **C1:** Consider designating an incident lead for each incident. **R2:** If appropriate, contact the organization's incident response service provider to request assistance. **R3:** Initiate execution of other cybersecurity plans as needed (e.g., business continuity and disaster recovery plans) to support incident response.
RS.MA-02	Incident reports are triaged and validated	High	**R1:** Perform a preliminary review of a new incident report to verify that a cybersecurity incident has occurred, then estimate the severity of the incident and the level of urgency needed to respond to it. **R2:** Have mechanisms in place for third parties to report possible incidents that involve the organization. Reports should be carefully monitored and taken seriously. For example, the organization might be contacted by a party claiming that its systems are being attacked by a system at the organization. External users may report other indicators, such as an unavailable service. Other incident response teams may also report incidents to the organization.
RS.MA-03	Incidents are categorized and prioritized	High	**R1:** Perform a more detailed review of incidents to help categorize them by incident type (e.g., data breach, ransomware, account takeover, denial of service).

CSF Element	CSF Element Description	Priority	Recommendations, Considerations, Notes
			R2: Prioritize how quickly incident response should be performed for each incident based on its scope, likely impact, time-critical nature, and resource availability. **R3:** Select incident response strategies for active incidents by balancing the need to quickly recover from an incident with the need to observe the attacker or conduct a more thorough investigation. **N1:** Every response strategy decision has trade-offs. For example, a strategy that supports observing the attacker's behavior or conducting a more thorough investigation may be at odds with the need to quickly return to normal operations.
RS.MA-04	Incidents are escalated or elevated as needed	High	**N1:** *Escalation* generally refers to increasing resources or time frames, while *elevation* usually indicates involving a higher level of management in the response efforts. **R1:** Track and validate the status of all ongoing incidents so that incidents in need of more response resources or a change in response strategy can be identified and the necessary changes initiated rapidly.
RS.MA-05	The criteria for initiating incident recovery are applied	High	**R1:** Apply incident recovery criteria to known and assumed characteristics of the incident to determine when an incident's recovery processes should be initiated. **R2:** Take the possible operational disruption of incident recovery activities into account to determine when recovery should be initiated.
RS.AN (Incident Analysis)	Investigations are conducted to ensure effective response and support forensics and recovery activities	High	**N1:** The Incident Analysis Category focuses on investigating, determining, and documenting what has happened during an incident, as well as how and why it happened.
RS.AN-03	Analysis is performed to establish what has taken place during an incident and the root cause of the incident	High	**R1:** Determine the sequence of events that have occurred during the incident and which assets and resources were involved in each of those events. **R2:** Attempt to determine what vulnerabilities, threats, and threat actors were directly or indirectly involved in the incident. **R3:** Analyze the incident to find the underlying or systemic root causes. **R4:** Check any deployed cyber deception technology for additional information on attacker behavior.

CSF Element	CSF Element Description	Priority	Recommendations, Considerations, Notes
			N1: This information may also be helpful for identifying weaknesses in cybersecurity risk management that should be addressed to prevent similar incidents from occurring in the future.
RS.AN-06	Actions performed during an investigation are recorded, and the records' integrity and provenance are preserved	High	**N1:** Facts discovered and actions taken during incident response tasks can be recorded by many means, including a paper logbook, audio/video recordings, or automatic session monitoring and logging, as permitted by the organization's incident response plan and policy. **R1:** Safeguard the confidentiality and integrity of incident response records, and ensure that only authorized personnel have access. **N2:** Incident response records can contain sensitive information, such as data on exploited vulnerabilities, recent data breaches, and users who may have performed inappropriate actions. The incident lead is often responsible for ensuring that incident response records are properly safeguarded.
RS.AN-07	Incident data and metadata are collected, and their integrity and provenance are preserved	High	**N1:** Many incident responses involve the collection of incident data and metadata. Formal evidence gathering and handling using chain-of-custody procedures might not be performed for every incident that occurs (e.g., most malware incidents will not result in prosecution). However, collected incident data is still considered evidence, which is defined as "grounds for belief or disbelief; data on which to base proof or to establish truth or falsehood" [SP800-160v1]. **R1:** Collect and retain evidence from an incident in accordance with the organization's evidence preservation procedures and data retention policies, and consider factors such as the possibility of prosecution, and the cost of retaining the data and the hardware and software needed to access the data in the future.
RS.AN-08	An incident's magnitude is estimated and validated	High	**N1:** Determining the incident's magnitude is often one of the most challenging aspects of incident response. **R1:** Look for indicators of compromise, evidence of persistence, and other signs of an incident on both the assets known to be targeted and other potential targets.

CSF Element	CSF Element Description	Priority	Recommendations, Considerations, Notes
			Skipping this activity or performing it in a superficial way may cause underestimation of the incident's magnitude, thus allowing the incident to continue indefinitely on other targets without the organization's knowledge or monitoring.
RS.CO (Incident Response Reporting and Communication)	Response activities are coordinated with internal and external stakeholders, as required by laws, regulations, or policies	High	**N1:** Incident response reporting and communication activities tend to fall into four categories. *Incident coordination* involves communicating current and planned incident response activities for a particular incident among the internal and external parties with incident response roles and responsibilities. *Incident notification* involves formally informing affected customers, employees, partners, regulators, or others about a data breach or other incident. *Public communication* involves communicating to the public about the status of a particular incident, such as responding to media inquiries. *Incident information sharing* involves sharing cybersecurity threat information with others, usually voluntarily, based on activity observed within the organization's technology assets. **R1:** Organizations should have mechanisms in place in advance to coordinate with affected parties about incidents when needed.
RS.CO-02	Internal and external stakeholders are notified of incidents	High	**R1:** When an incident is analyzed and prioritized, the incident response team should coordinate with the appropriate individuals inside and outside of the organization so that all who need to be involved will play their roles. **R2:** Follow established procedures concerning incident coordination that include what must be reported to whom and at what times (e.g., initial notification, regular status updates). **R3:** Perform notifications in compliance with the current incident notification-related laws and regulations that pertain to the organization's sectors, geographic locations, customer locations, and any other characteristics that apply to the organization. Incident notification is an evolving topic, and new laws and regulations are being established frequently.

CSF Element	CSF Element Description	Priority	Recommendations, Considerations, Notes
			R4: Notify affected third parties of data breaches and other cybersecurity incidents in accordance with regulatory, legal, and contractual requirements. **R5:** Notify law enforcement agencies and regulatory bodies of incidents based on criteria in the incident response plan and management approval. Designated individuals should contact these parties in a manner consistent with the requirements of the law and the organization's policies and procedures.
RS.CO-03	Information is shared with designated internal and external stakeholders	High	**N1:** Voluntary incident information sharing is often mutually beneficial because the same threats and attacks simultaneously affect multiple organizations. An example is sharing information about observed TTPs with a sector-specific Information Sharing and Analysis Center (ISAC). **N2:** Sharing defensive tactics between organizations can enhance overall situational awareness and increase the resiliency of all. There is a cost to threat actors to develop or purchase exploits and to deploy them. The effective identification and dissemination of detection techniques lowers the attackers' return on investment and increases their costs. **N3:** Incident handlers might coordinate their efforts with colleagues at partner organizations to share tactical, technical information on mitigating an attack that spans those organizations. The organizations participating in this type of relationship are usually peers without authority over each other. In addition to choosing to share information, they may also pool resources to solve common problems. **R1:** Securely share information with stakeholders consistent with the organization's response plans and information sharing agreements, including contracts with suppliers. **R2:** Regularly update senior leadership on the status of major incidents. **R3:** Notify human resources when malicious insider activity has occurred. **R4:** Establish and follow media communications procedures for incident response that comply with the

CSF Element	CSF Element Description	Priority	Recommendations, Considerations, Notes
			organization's policies on media interaction and information disclosure.
RS.MI (Incident Mitigation)	Activities are performed to prevent expansion of an event and mitigate its effects	High	**N1:** Manually selecting containment and eradication actions may be easier and faster if the organization has criteria and procedures in place. Criteria could take the incident type into account (e.g., a cloud-based services compromise or a user endpoint ransomware infection) and use some of the risk evaluation factors in RS.MA. Another factor to consider is the duration of the containment measure (e.g., an emergency workaround that must be removed within hours, a temporary workaround to be removed within two weeks, or a permanent solution). The eradication measure's duration could be similarly evaluated. **R1:** In some instances, organizations redirect an attacker to a sandbox so that they can monitor the attacker's activity, usually to gather additional evidence. This delays containment and eradication activities. The incident response team should first discuss the feasibility of this strategy with the legal department before executing it. The intentional delay can be dangerous because an attacker could escalate unauthorized access or compromise other systems.
RS.MI-01	Incidents are contained	High	**N1:** *Containment* refers to preventing the expansion of an incident. Containment can prevent additional damage and avoid overwhelming the organization's resources. Most incidents require some form of containment. **C1:** Consider configuring cybersecurity technologies (e.g., antivirus software) and the cybersecurity features of other technologies (e.g., operating systems, network infrastructure devices) to automatically perform some containment actions, like quarantining malware, transferring a compromised endpoint to an isolated remediation network, or halting the execution of an infected container. **C2:** Consider authorizing third parties (e.g., the organization's internet service providers and cloud service providers) to automatically act to contain certain types

CSF Element	CSF Element Description	Priority	Recommendations, Considerations, Notes
			of incidents (e.g., large-scale DDoS attacks) on behalf of the organization. **R1:** Allow incident handlers to manually select and perform containment actions instead of or in addition to automated containment measures.
RS.MI-02	Incidents are eradicated	High	**N1:** *Eradication* refers to mitigating an incident's effects. After containment, eradication may be necessary to eliminate persistence mechanisms and entry points, such as deleting malware, disabling breached user accounts, and identifying and mitigating all exploited vulnerabilities. **R1:** Identify all affected hosts and services within the organization so that all flaws and weaknesses can be remediated. **C1:** Consider configuring cybersecurity technologies and the cybersecurity features of other technologies (e.g., operating systems, network infrastructure devices) to automatically perform some eradication actions. **C2:** Consider authorizing third parties (e.g., the organization's internet service providers and cloud service providers) to automatically act to eradicate certain types of incidents on behalf of the organization. **R2:** Allow incident handlers to manually select and perform eradication actions instead of or in addition to automated eradication measures.
RC (Recover)	Assets and operations affected by a cybersecurity incident are restored	High	**N1:** During incident recovery, personnel restore systems to normal operations, confirm that the systems are functioning normally, and (if applicable) remediate vulnerabilities to prevent similar incidents. **N2:** Recovery operations include restoring systems from clean backups, rebuilding systems, replacing compromised files with clean versions, installing patches, changing passwords, and tightening security controls. In intrusions where the threat actor is highly sophisticated and the full scope of their tactics is not revealed, it may be necessary to go as far as replacing the hardware (e.g., bare metal) of all of the compromised systems. **N3:** For more information on incident recovery, see [SP800-184].

CSF Element	CSF Element Description	Priority	Recommendations, Considerations, Notes
RC.RP (Incident Recovery Plan Execution)	Restoration activities are performed to ensure operational availability of systems and services affected by cybersecurity incidents	High	**N1:** Executing the incident recovery plan involves selecting, prioritizing, and performing recovery actions in a secure manner; verifying the integrity of recovered assets; declaring the end of incident recovery; and completing incident documentation. **N2:** For more information on incident recovery plans and plan execution, see [SP800-184].
RC.RP-01	The recovery portion of the incident response plan is executed once initiated from the incident response process	High	**R1:** Begin recovery procedures during or after incident response processes. **R2:** Inform all individuals with recovery responsibilities about the plans for recovery and the authorizations required to implement each aspect of the plans.
RC.RP-02	Recovery actions are selected, scoped, prioritized, and performed	High	**R1:** Recovery actions should take timeliness, precision, and reliability (e.g., restoring only the affected files versus restoring all files) into account. **R2:** Select recovery actions based on the criteria defined in the incident response plan and available resources. **R3:** Change planned recovery actions based on a reassessment of organizational needs and resources.
RC.RP-03	The integrity of backups and other restoration assets is verified before using them for restoration	High	**R1:** Check restoration assets for indicators of compromise, file corruption, and other integrity issues before use.
RC.RP-04	Critical mission functions and cybersecurity risk management are considered to establish post-incident operational norms	High	**R1:** Validate that essential services are restored in the appropriate order. **R2:** Work with system owners to confirm the successful restoration of systems and the return to normal operations. **R3:** Monitor the performance of restored systems to verify the adequacy of the restoration.
RC.RP-05	The integrity of restored assets is verified, systems and services are restored, and normal operating status is confirmed	High	**R1:** Check restored assets for indicators of compromise, and remediate the root causes of the incident before production use. **R2:** Verify the correctness and adequacy of the restoration actions taken before putting a restored system online.
RC.RP-06	The end of incident recovery is declared based on criteria, and incident-related documentation is completed	High	**R1:** Prepare an after-action report that documents the incident itself, the response and recovery actions taken, and lessons learned.

CSF Element	CSF Element Description	Priority	Recommendations, Considerations, Notes
RC.CO (Incident Recovery Communication)	Restoration activities are coordinated with internal and external parties	High	**N1:** Incident recovery communication is a continuation of the communication activities in RS.CO.
RC.CO-03	Recovery activities and progress in restoring operational capabilities are communicated to designated internal and external stakeholders	High	**R1:** Securely share recovery information, including restoration progress, consistent with response plans and information sharing agreements. **R2:** Regularly update senior leadership on recovery status and restoration progress for major incidents. **R3:** Follow the rules and protocols defined in contracts for incident information sharing between the organization and its suppliers. **R4:** Coordinate crisis communication between the organization and its critical suppliers.
RC.CO-04	Public updates on incident recovery are shared using approved methods and messaging	High	**R1:** Follow the organization's breach notification procedures for recovering from a data breach incident. **R2:** Explain the steps being taken to recover from the incident and to prevent a recurrence.

References

[CISA-PB] Cybersecurity and Infrastructure Security Agency (2021) Cybersecurity Incident & Vulnerability Response Playbooks: Operational Procedures for Planning and Conducting Cybersecurity Incident and Vulnerability Response Activities in FCEB Information Systems. (Cybersecurity and Infrastructure Security Agency, Arlington, VA). Available at https://www.cisa.gov/sites/default/files/publications/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf

[CNSSI-4009] Committee on National Security Systems (2022) Committee on National Security Systems (CNSS) Glossary. (National Security Agency, Ft. Meade, MD). Committee on National Security Systems Instruction (CNSSI) 4009. Available at https://www.cnss.gov/CNSS/issuances/instructions.cfm

[CSF2.0] 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

[CSWP32] Pascoe C, Snyder JN, Scarfone K (2024) NIST Cybersecurity Framework 2.0: A Guide to Creating Community Profiles. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Cybersecurity White Paper (CSWP) NIST CSWP 32. https://doi.org/10.6028/NIST.CSWP.32.ipd

[FISMA2014] Federal Information Security Modernization Act of 2014, Pub. L. 113-283, 128 Stat. 3073. Available at https://www.govinfo.gov/app/details/PLAW-113publ283

[IR8286] Stine KM, Quinn SD, Witte GA, Gardner RK (2020) Integrating Cybersecurity and Enterprise Risk Management (ERM). (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) NIST IR 8286. https://doi.org/10.6028/NIST.IR.8286

[SP800-30r1] Joint Task Force Transformation Initiative (2012) Guide for Conducting Risk Assessments. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-30r1. https://doi.org/10.6028/NIST.SP.800-30r1

[SP800-37r2] Joint Task Force (2018) Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-37r2. https://doi.org/10.6028/NIST.SP.800-37r2

[SP800-61r2] Cichonski PR, Millar T, Grance T, Scarfone KA (2012) Computer Security Incident Handling Guide. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-61r2. https://doi.org/10.6028/NIST.SP.800-61r2

[SP800-84] Grance T, Nolan T, Burke K, Dudley R, White G, Good T (2006) Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-84. https://doi.org/10.6028/NIST.SP.800-84

[SP800-92r1] Scarfone K, Souppaya M (2023) Cybersecurity Log Management Planning Guide. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-92r1 ipd. https://doi.org/10.6028/NIST.SP.800-92r1.ipd

[SP800-150] Johnson CS, Waltermire DA, Badger ML, Skorupka C, Snyder J (2016) Guide to Cyber Threat Information Sharing. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-150. https://doi.org/10.6028/NIST.SP.800-150

[SP800-160v1] 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

[SP800-184] Bartock MJ, Scarfone KA, Smith MC, Witte GA, Cichonski JA, Souppaya MP (2016) Guide for Cybersecurity Event Recovery. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-184. https://doi.org/10.6028/NIST.SP.800-184

[SP800-216] Schaffer KB, Mell PM, Trinh H, Van Wyk I (2023) Recommendations for Federal Vulnerability Disclosure Guidelines. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-216. https://doi.org/10.6028/NIST.SP.800-216

[SP800-218] Souppaya MP, Scarfone KA, Dodson DF (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

CISA
Cybersecurity and Infrastructure Security Agency

CPRT
Cybersecurity and Privacy Reference Tool

CSF
Cybersecurity Framework

CSP
Cloud Service Provider

CTI
Cyber Threat Intelligence

ISAC
Information Sharing and Analysis Center

ISP
Internet Service Provider

MOU
Memorandum of Understanding

MSSP
Managed Security Services Provider

NDA
Non-Disclosure Agreement

SIEM
Security Information and Event Management

SOAR
Security Orchestration, Automation, and Response

SOC
Security Operations Center

SOP
Standard Operating Procedures

TTPs
Tactics, Techniques, and Procedures

Appendix B. Glossary

adverse cybersecurity event
Any event with a potentially negative impact on cybersecurity.

computer security incident
See *cybersecurity incident*.

cyber threat intelligence
Cyber threat information that has been aggregated, transformed, analyzed, interpreted, or enriched to provide the necessary context for decision-making processes. [SP800-150, adapted]

cybersecurity incident
An occurrence that actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies. [FISMA2014]

event
Any observable occurrence involving computing assets, including physical and virtual platforms, networks, services, and cloud environments.

incident
See *cybersecurity incident*.

incident response
The remediation or mitigation of violations of security policies and recommended practices. [FISMA2014]

indicators of compromise
Technical artifacts or observables that suggest that an attack is imminent or is currently underway or that a compromise may have already occurred. [SP800-150, adapted]

tactics, techniques, and procedures
The behavior of an actor. A tactic is the highest-level description of this behavior, while techniques give a more detailed description of behavior in the context of a tactic, and procedures an even lower-level, highly detailed description in the context of a technique. [SP800-150]

threat
Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service. [SP800-30r1]

vulnerability
A weakness in a system, system security procedures, internal controls, or implementation by which an actor or event may intentionally exploit or accidentally trigger the weakness to access, modify, or disrupt the normal operations of a system, resulting in a security incident or violation of the system's security policy. [CNSSI-4009, adapted]

Appendix C. Change Log

This publication revises the previous version, NIST SP 800-61 Revision 2 (2012), as follows:

- Performed a full rewrite of the previous content to improve clarity and usability and to remove outdated material and material addressed in more depth in other NIST publications and other federal agency content
- Shifted the focus of the document from guidelines on detecting, analyzing, prioritizing, and handling incidents to recommendations and considerations for incorporating cybersecurity incident response considerations throughout an organization's cybersecurity risk management activities
- Reorganized the contents to comprise a CSF 2.0 Community Profile
- Moved most hyperlinks to a new SP 800-61 project website to facilitate their maintenance
- Reformatted all content to follow the latest NIST technical report template