Check for updates

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

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

Check for updates

NIST 特别出版物 800
NIST SP
800-61r3

网络安全事件响应建议与考虑

风险管理

CSF 2.0 社区概况

亚历克斯·纳尔逊桑杰
·雷基
穆鲁吉亚·苏帕亚
凯伦·斯卡弗恩

本出版物可从以下网址免费获取：
https://doi.org/10.6028/NIST.SP.800-61r3

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

本译本由机器翻译生成，供快速理解条文与内部培训使用；
涉及合规判断或法律适用时，请咨询专业顾问，并以官方英文文本为准。
翻译您自己的文件，请选择桐鸾译馆 · https://www.ivyivy.com.cn
扫码关注服务号

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

NIST 特别出版物 800
NIST SP
800-61r3

网络安全事件响应建议与考虑

风险管理

CSF 2.0 社区概况

亚历克斯·纳尔逊
桑杰·雷基
穆鲁吉亚·苏帕亚*
计算机安全部
信息技术实验室

凯伦·斯卡弗恩
*Scarfone*网络安全

*前NIST员工；所有相关工作均为此该出版物是在NIST任职期间完成的。

本出版物可从以下网址免费获取：
https://doi.org/10.6028/NIST.SP.800-61r3

2025年4月



美国商务部
霍华德·卢特尼克，商务部长

美国国家标准与技术研究院
Craig Burkhardt，代理商务部负责标准与技术事务副部长兼代理*NIST*主任

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

本文中标识了某些商业或非商业设备、仪器、软件或材料，以便充分说明实验过程。此类标识并不意味着NIST对任何产品或服务的推荐或认可，也不意味着所标识的材料或设备必然是该用途下的最佳可用选择。

本出版物中可能引用了NIST正在根据其法定职责制定的其他出版物。本出版物中的信息，包括概念和方法，即使在这些配套出版物完成之前，联邦机构也可以使用。因此，在每份出版物完成之前，现有的要求、指南和程序(如存在)仍然有效。出于规划和过渡目的，联邦机构可能希望密切关注NIST这些新出版物的制定进展。

鼓励各组织在公开评论期内审阅所有草案出版物并向NIST提供反馈。除上述出版物外，许多NIST网络安全出版物可在https://csrc.nist.gov/publications.获取

权限
本出版物由NIST根据2014年《联邦信息安全管理现代化法案》(FISMA)、44 U.S.C.3551 et seq.、公法(P.L.)113-283赋予的法定职责制定。NIST负责制定信息安全标准和指南，包括联邦信息系统的最低要求，但此类标准和指南未经对此类系统行使政策权限的适当联邦官员明确批准，不得适用于国家安全系统。本指南符合管理和预算办公室(OMB)A-130号通告的要求。

本出版物中的任何内容均不得被视为与商务部长根据法定权限对联邦机构作出的强制性且具有约束力的标准和指南相矛盾。这些指南也不应被解释为改变或取代商务部长、OMB主任或任何其他联邦官员的现有权限。本出版物可由非政府组织自愿使用，在美国不受版权保护。但NIST希望在使用时予以注明出处。

NIST 技术系列政策
版权、使用和许可声明
NIST技术系列出版物标识符语法

出版历史
NIST编辑审查委员会于2025-03-25批准
取代 NIST SP 800-61r2(2012年8月) https://doi.org/10.6028/NIST.SP.800-61r2

如何引用本 NIST 技术系列出版物
Nelson A, Rekhi S, Souppaya M, Scarfone K(2025)《网络安全风险管理的事件响应建议与考量：CSF 2.0 社区概况》(美国国家标准与技术研究院，马里兰州盖瑟斯堡),NIST 特别出版物(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).

作者 ORCID iD
亚历克斯·纳尔逊：0000-0002-3771-57
桑杰·雷基：0009-0008-8711-4030
穆鲁吉亚·苏帕亚：0000-0002-8055-8527
凯伦·斯卡弗恩：0000-0001-6334-9486

comments@nist.gov

美国国家标准与技术研究院
收件人：计算机安全部，信息技术实验室 100 Bureau Drive(Mail Stop 8930) Gaithersburg, MD 20899-8930

附加信息
有关本出版物的更多信息可在https://csrc.nist.gov/pubs/sp/800/61/r3/final，获取，包括相关内容、可能的更新和

所有评论均可能根据《信息自由法》(FOIA)予以公开。

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.

摘要

本出版物旨在帮助组织按照NIST网络安全框架(CSF)2.0所述，将网络安全事件响应建议和考虑因素纳入其整个网络安全风险管理活动。这样做可以帮助组织为事件响应做好准备，减少所发生事件的数量和影响，并提高其事件检测、响应和恢复活动的效率和有效性。鼓励读者结合本文档利用在线资源，获取有关实施这些建议和考虑因素的更多信息。

关键词

网络威胁信息共享；网络安全框架；网络安全事件；网络安全风险管理；事件处置；事件管理；事件响应。

计算机系统技术报告

美国国家标准与技术研究院(NIST)的信息技术实验室(ITL)通过为国家的测量和标准基础设施提供技术领导，促进美国经济和公共福利。ITL开发测试、测试方法、参考数据、概念验证实现和技术分析，以推进信息技术的发展和高效利用。ITL的职责包括制定管理、行政、技术和物理标准与指南，以实现联邦信息系统中除国家安全相关信息之外的其他信息的成本效益安全性和隐私性。800系列特别出版物报告了ITL在信息系统安全方面的研究、指南和外联工作，以及与行业、政府和学术组织的合作活动。

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

All registered trademarks belong to their respective organizations.

补充内容

NIST已建立事件响应项目页面，其中托管了指向包含事件响应活动更多信息之资源的链接。通过将链接从本文档移至网站，NIST可按需更新和扩展这些链接，而无需发布本出版物的新版本。

有关CSF 2.0社区概况的更多信息，请参见框架资源中心。

受众

本出版物的目标受众包括网络安全项目领导层、网络安全人员以及其他负责为网络安全事件做准备、检测、响应或恢复的人员。本出版物适用于大多数组织，无论其行业、规模或其他因素如何。

商标信息

所有注册商标均属于其各自的组织。

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.

专利披露声明

注意：ITL已要求，其使用可能为遵守本出版物的指南或要求所必需的专利权利要求持有人向ITL披露此类专利权利要求。但是，专利持有人没有义务回应ITL的专利征集，ITL也未进行专利检索以确定是否有任何专利可能适用于本出版物。

截至出版之日，在征集可能为遵守本出版物的指南或要求所必需之专利权利要求的标识之后，未向ITL标识出任何此类专利权利要求。

ITL未作出或暗示任何陈述，表明在使用本出版物时无需许可即可避免专利侵权。

Table of Contents

Executive Summary **1**
1. Introduction **2**
1.1. Purpose and Scope 3
1.2. Document Structure 3
2. Incident Response as Part of Cybersecurity Risk Management **4**
2.1. Incident Response Life Cycle Model 4
2.2. Incident Response Roles and Responsibilities 6
2.3. Incident Response Policies, Processes, and Procedures 8
3. CSF 2.0 Community Profile for Cyber Incident Risk Management **10**
3.1. Preparation and Lessons Learned 11
3.2. Incident Response 23
References **36**
Appendix A. List of Symbols, Abbreviations, and Acronyms **38**
Appendix B. Glossary **39**
Appendix C. Change Log **40**

List of Tables

Table 1. Previous incident response life cycle model's phases and corresponding CSF 2.0 Functions **6**
Table 2. CSF 2.0 Community Profile part 1: Preparation and Lessons Learned **11**
Table 3. CSF 2.0 Community Profile part 2: Incident Response **23**

List of Figures

Fig. 1. Previous incident response life cycle model **4**
Fig. 2. Incident response life cycle model based on CSF 2.0 Functions **5**

目录

执行摘要 1
1. **引言** 2
1.1. Purpose and Scope 3
1.2. Document Structure 3
2. **作为网络安全风险管理组成部分的事件响应** 4
2.1. Incident Response Life Cycle Model 4
2.2. Incident Response Roles and Responsibilities 6
2.3. Incident Response Policies, Processes, and Procedures 8
3. **CSF 2.0 网络事件风险管理社区概况** 10
3.1. Preparation and Lessons Learned 11
3.2. Incident Response 23
参考文献 36
附录 A.符号、缩写和首字母缩略语列表 38
附录 B.术语表 39
附录 C.变更日志 40

表清单

表1. 以往事件响应生命周期模型的阶段及对应的CSF 2.0功能 6
表2. CSF 2.0社区概况第1部分：准备与经验教训 11
表 3. CSF 2.0 社区概况第 2 部分：事件响应 23

图目录

图1. 以往事件响应生命周期模型 ..... **4** **图2. 基于CSF 2.0功能的事件响应生命周期模型** **5**

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.

执行摘要

事件响应是网络安全风险管理的关键组成部分，应贯穿组织各项运营进行整合。NIST网络安全框架(CSF) 2.0的全部六个功能在事件响应中都发挥着至关重要的作用：

- 治理、识别和保护帮助组织预防某些事件、为处置确实发生的事件做好准备、减轻这些事件的影响，并基于这些事件的经验教训改进事件响应和网络安全风险管理实践。
- 检测、响应和恢复帮助组织发现、管理、优先处理、遏制、根除网络安全事件并从中恢复，以及执行事件报告、通知和其他与事件相关的沟通。

许多个人、团队和第三方在支持组织事件响应的所有功能中承担着各种各样的角色和职责。组织无法直接控制对手使用的战术和技术，也无法确定未来事件的发生时间，只知道另一起事件不可避免。然而，组织可以使用最适合自身的事件响应生命周期框架或模型，制定强有力的网络安全风险管理实践，将风险降低到可接受的水平。

本出版物使用 CSF 2.0 的功能、类别和子类别，作为 CSF 2.0 社区概况来组织其关于事件响应的建议、考虑事项和其他信息。这样做提供了一个通用分类法，该分类法已被广泛用于事件响应以及网络安全风险管理和治理方面的沟通。这也使组织能够通过 NIST 网络安全和隐私参考工具(CPRT)访问映射到每个功能、类别和子类别的一系列在线资源。这些资源包括与其他事件响应和网络安全风险管理标准及指南的映射，以及组织可根据需要选择使用的实施指南来源。

组织应使用最适合自身的事件响应生命周期框架或模型。本文档中的模型基于 CSF 2.0，以利用 CSF 2.0 可用的丰富资源，并帮助已在使用 CSF 的组织。无论使用何种事件响应生命周期框架或模型，每个组织都应在整个网络安全风险管理活动中考虑事件响应。

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

1. 引言

在本文件中，事件是任何涉及计算资产的可观察发生，包括物理和虚拟平台、网络、服务和云环境。事件的示例包括用户登录尝试、软件更新的安装以及应用程序对事务请求的响应。许多事件关注安全或具有安全影响。不利事件是任何与负面后果相关的事件，无论原因如何，包括自然灾害、电力故障或网络安全攻击。本指南仅涉及不利网络安全事件。通常需要额外分析以确定不利网络安全事件是否表明已发生网络安全事件。网络安全事件(或简称事件)是

> .....在无合法授权的情况下，实际或即将危及信息或信息系统的完整性、保密性或可用性的发生；或构成对法律、安全策略、安全程序或可接受使用策略的违反或即将违反的威胁。[FISMA2014]

事件示例包括攻击者：

- 利用僵尸网络向面向互联网的服务发送大量连接请求，使其无法为合法服务用户所用
- 获取软件即服务提供商的行政凭据，使委托给该提供商的敏感租户数据面临风险
- 侵入组织的业务网络以窃取凭据，并利用这些凭据指示工业控制系统关闭或破坏关键物理组件，造成重大服务中断
- 部署勒索软件以阻止计算机系统的使用，并通过从这些系统复制文件造成多起数据泄露
- 使用网络钓鱼电子邮件入侵用户账户，并利用这些账户实施金融欺诈
- 识别网络管理设备中的新脆弱性，并利用该脆弱性未经授权访问网络通信
- 入侵供应商的软件，该软件随后以被入侵状态分发给客户

由于网络安全事件可能对组织及其客户、业务合作伙伴和其他方造成损害，因此在事件发生时快速有效地响应至关重要。有效实施事件响应流程，可以通过分析信息并采取适当行动，实现对事件的系统性响应和恢复。这通过最大限度地减少数据丢失或被盗、服务中断以及事件的总体影响，降低网络安全风险和企业风险。从事件响应活动和根本原因分析中获得的经验教训有助于改进网络安全风险管理并

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.

治理工作，并确保组织更好地准备识别其当前技术资产和网络安全风险，保护其资产，并检测、响应和恢复未来的事件。

1.1. 目的与范围

本出版物旨在帮助组织将网络安全事件响应建议和考虑事项纳入其整个网络安全风险管理活动。它还提供了一种通用语言，所有组织都可以使用它在内部和外部就其事件响应计划和活动进行沟通。

本出版物的范围与以往版本有显著不同。由于事件响应活动的具体实施方式变化频繁，且因技术、环境和组织而异，在单一静态出版物中捕获并维护这些信息已不再可行。因此，本版本侧重于改进 NIST 网络安全框架(CSF)2.0 所有功能[CSF2.0]的网络安全风险管理，以更好地支持组织的事件响应能力。

鼓励读者结合本文件使用其他NIST资源，包括CSF 2.0出版物及补充资源、事件响应项目页面，以及通过NIST网络安全和隐私参考工具(CPRT)可获得的关于实施事件响应考虑的其他信息源的映射。CPRT映射的一个示例是将CSF 2.0结果与NIST特别出版物(SP)800-53控制措施相关联，这些控制措施可实施以帮助实现这些结果。通过这种方式，CSF 2.0提供了一种共同语言，便于访问大量其他资源。本出版物取代SP 800-61r2(第2版),计算机安全事件处置指南[SP800-61r2]。

1.2. 文档结构

本文档的其余部分组织为以下章节和附录：

- 第 2 节讨论事件响应如何演变为网络安全风险管理的关键部分，以及事件响应生命周期的概念如何变化以反映这一点。
- 第 3 节提出针对组织网络安全风险管理实践的事件响应建议和考虑事项。它们作为 CSF 2.0 社区概况进行组织和记录。
- 参考文献部分列出了本出版物中引用的参考文献。
- 附录 A 和附录 B 分别提供缩略语列表和术语表。
- 附录 C 包含自上一修订版以来所做重大更改的变更日志。

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].

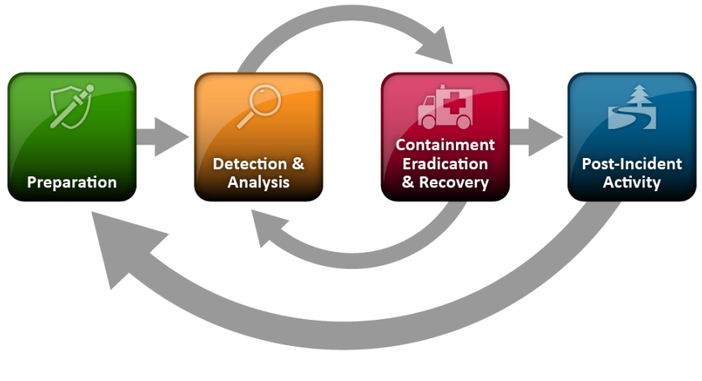


Fig. 1. Previous incident response life cycle model

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.

2. 事件响应作为网络安全风险管理的一部分

本节解释事件响应作为网络安全风险管理组成部分的基本概念。第 2.1 节探讨事件响应生命周期，并提出基于 CSF 2.0 功能的新生命周期模型。第 2.2 节讨论组织内部和外部的事件响应角色和职责。最后，第 2.3 节简要考察事件响应策略、过程和程序。

2.1. 事件响应生命周期模型

图 1 描绘了本出版物上一版本中说明的事件响应生命周期模型[SP800-61r2]。

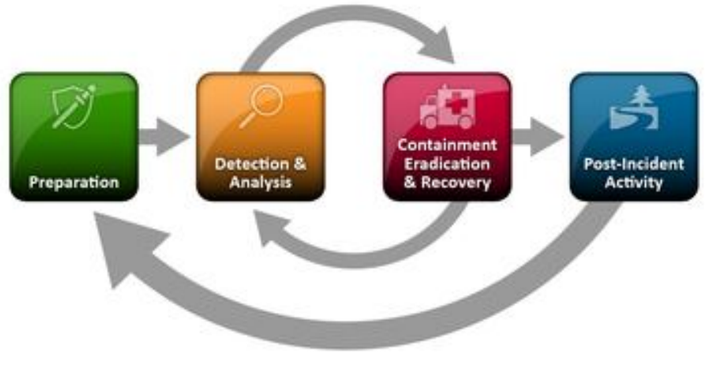


图 1. 以往的事件响应生命周期模型

当时，事件相对罕见，大多数事件的范围狭窄且界定明确，事件响应和恢复通常在一两天内完成。在那种条件下，将事件响应视为由专门人员团队执行的一套独立活动，并将所有事件响应活动描述为循环生命周期的一部分，是切合实际的。正式的事件后活动会识别所需的改进并将其反馈到准备阶段，从而重新开始循环。事件响应活动通常是间歇性的，而非持续性的。

然而，自那时以来，事件响应的现状已发生巨大变化。如今，事件频繁发生并造成远更大的损害。由于其广度、复杂性和动态性质，从中恢复往往需要数周或数月。事件响应现在被视为网络安全风险管理的关键组成部分，应整合到组织运营的各个方面。事件响应期间获得的经验教训往往应在识别后尽快共享，而不是延迟到恢复结束后。为了跟上现代威胁，网络安全风险管理的各个方面越来越需要持续改进。

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.

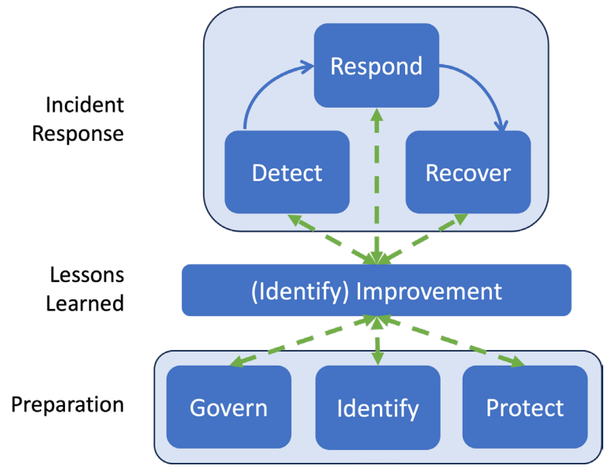


Fig. 2. Incident response life cycle model based on CSF 2.0 Functions

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

图 2 显示了基于六个 CSF 2.0 功能的高级事件响应生命周期模型，这些功能在最高层级组织网络安全结果：

- **治理(GV):**组织的网络安全风险管理策略、期望和政策得以建立、传达和监控。
- **识别(ID):**组织当前的网络安全风险得到理解。
- **保护(PR):**使用保障措施来管理组织的网络安全风险。
- **检测(DE):**发现并分析可能的网络安全攻击和入侵。
- **响应(RS):**针对检测到的网络安全事件采取行动。
- **恢复(RC):**受网络安全事件影响的资产和运营得到恢复。所有六个功能在事件响应中都发挥着至关重要的作用。治理、识别和保护帮助组织预防某些事件、为处置确实发生的事件做好准备、减少这些事件的影响，并基于经验教训改进事件响应和网络安全风险管理实践。检测、响应和恢复帮助组织发现、管理、优先排序、遏制、根除网络安全事件并从中恢复，以及执行事件报告、通知和其他与事件相关的通信。

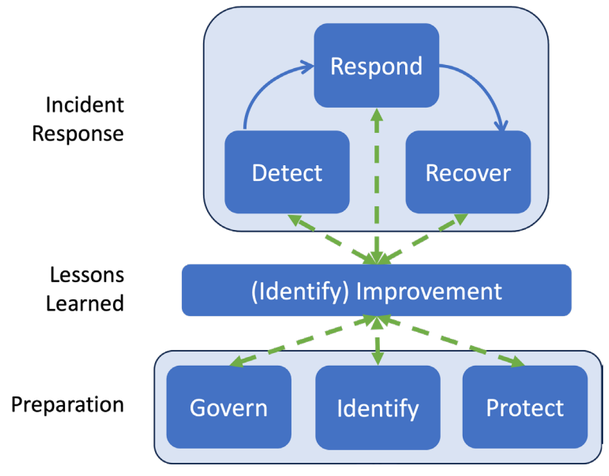


图2. 基于CSF 2.0功能的事件响应生命周期模型

底层反映的是治理、识别和保护中的准备活动不属于事件响应本身。相反，它们是更广泛的网络安全风险管理活动，同时也支持事件响应。事件响应显示在图的顶层：检测、响应和恢复。此外，持续改进的需求以中间层表示，即识别功能中的改进类别(ID.IM)和绿色虚线。从执行所有功能中的所有活动中获得的经验教训被输入到改进中，这些经验教训被分析、确定优先级，并用于为所有功能提供信息。这反映出组织可以在任何时候学到新的经验教训

(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.

(例如，检测新威胁的存在并描述其特征)并将这些经验教训传达给适当人员，以便组织的事件响应和其他网络安全风险管理策略、过程和实践可按需调整。

表 1 将先前 SP 800-61 事件响应生命周期模型的阶段映射到本文档中使用的相应 CSF 2.0 功能。

表1. 以往事件响应生命周期模型的阶段及对应的CSF 2.0功能

先前的事件响应生命周期模型阶段	CSF 2.0 功能
准备	治理
	识别(所有类别)
	保护
检测与分析	检测
	识别(改进类别)
遏制、根除与恢复	响应
	恢复
	识别(改进类别)
事件后活动	识别(改进类别)

组织应使用最适合自己的事件响应生命周期框架或模型。本文档中的模型基于CSF 2.0，以利用CSF 2.0可用的丰富资源，并帮助已经在使用CSF的组织。适合组织的事件响应生命周期框架或模型取决于许多因素；例如，规模较大且更依赖技术的组织可能比其他组织更能从强调持续改进的框架或模型中受益。无论使用何种事件响应生命周期框架或模型，每个组织都应在整个网络安全风险管理活动中考虑事件响应。

2.2. 事件响应角色与职责

过去，事件响应活动几乎完全由组织自身事件响应团队的事件处理人员执行。如今，尽管事件处理人员仍然至关重要，但大多数组织日益认识到，其事件响应工作的成功取决于许多内部和外部方的参与，这些方承担着各种各样的角色和职责，并且可能分布在世界各地。每个组织的角色和职责会有所不同，并且根据特定事件的性质，组织内部也可能有所不同。

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.

事件响应角色和职责的示例包括以下内容：

- **领导层。**组织的领导团队监督事件响应、分配资金，并可能对高影响的响应行动(如关闭或重建关键服务)拥有决策权。
- **事件处置人员。**事件处置人员核实事件是否已发生，收集和分析数据与证据，确定事件响应活动的优先级，并采取适当行动以限制损害、查找根本原因并恢复运营。事件处置人员还经常就缓解网络安全问题和提高韧性向他人提供意见。组织的事件处置人员可能是：
  o 内部员工(例如，事件响应团队),o 合同人员(例如，将安全运营中心[SOC]外包给托管安全服务提供商[MSSP]，或在该提供商的云内发生事件时借助云服务提供商的事件响应团队)，和/或
  o 需要时可用(例如，来自上级组织、网络安全服务提供商、业务合作伙伴或执法机构)。

  许多组织可能使用这些方法中的不止一种，例如在内部执行基本事件响应，并在某些事件中聘请第三方资源提供协助。较大的组织可能有多个事件响应团队，每个团队负责组织特定的逻辑或物理部分。当采用这种模式时，各团队应属于一个单一协调实体(例如，联邦)，以确保整个组织的事件响应流程、程序和培训保持一致，并且团队之间共享信息。
- **技术专业人员。**网络安全、隐私、系统、网络、云及其他技术架构师、工程师和管理员，以及软件开发人员，可能参与事件响应和恢复工作。
- **法律。**法律专家可以审查事件响应计划、政策和程序，以确保符合适用的法律和法规，包括隐私权。当涉及事件响应影响时，法律专家还可以审查与技术供应商和其他第三方的合同。此外，如果特定事件可能具有法律后果，例如起诉嫌疑人、诉讼或需要谅解备忘录(MOU)或其他有约束力协议的情况，事件响应人员可以寻求组织法律部门的指导。
- **公共事务与媒体关系。**根据事件的性质和影响，可能有必要告知媒体，并进而告知公众。有时，媒体通过其他来源(即并非通过公共事务人员)获悉事件。制定媒体接触策略可在这种情况下大有助益。

- **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)

- **人力资源。**某些人力资源实践应考虑网络安全风险管理，包括入职前筛查以及员工入职、离职和岗位变动。如果怀疑员工故意造成事件，人力资源部门也可能参与其中。
- **物理安全与设施管理。**某些计算机安全事件通过物理安全漏洞发生，或涉及有协调的逻辑和物理攻击。事件响应团队在事件处置期间也可能需要进入设施(例如，访问锁闭办公室内受入侵的工作站)。
- **资产所有者。**资产所有者(例如，系统所有者、数据所有者和业务流程所有者)可能对其受影响资产的响应和恢复优先级有宝贵见解。他们也需要及时了解响应和恢复工作的状态。

第三方可能与组织签订合同以帮助执行事件响应活动。一些第三方可能承担主要角色(例如，MSSP执行事件检测、响应和恢复活动)，而其他方(例如，云服务提供商[CSP]和互联网服务提供商[ISP])可能参与针对特定类型事件的某些事件响应活动。这是一种**共享责任模型**，其中组织将其部分责任转移给提供商。这些责任应在合同中明确界定，事件响应团队应了解责任分工，包括信息流、协调以及代表组织行事的权限。这还包括对服务提供商可以做什么的限制，例如与其他客户共享经过净化的

服务提供商可能比单个组织更早检测到恶意活动，因为它可以关联其客户之间的事件。在某些情况下，服务提供商可能能够利用与一个客户发生事件的知识，主动预防其其他客户发生类似事件。服务提供商通常对组织系统拥有特权访问权限，也可能访问敏感的组织数据。因此，应考虑并应对恶意内部人员或服务提供商被攻陷的风险。保密协议(NDA)和合同条款是阻止未经授权披露敏感数据的选项。

2.3. 事件响应策略、流程和程序

组织应制定治理其网络安全事件响应的策略。虽然策略高度因组织而异，但大多数事件响应策略都包含相同的关键要素：

- 管理层承诺声明
- 策略的目的和目标
- 策略的范围(即适用于谁、适用于什么以及在何种情况下适用)

- 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.

- 事件、网络安全事件、调查及相关术语的定义
- 角色、职责与权限，例如哪些角色有权没收、断开或关闭技术资产
- 用于确定事件优先级、估计其严重性、启动恢复流程、维持或恢复运营以及其他关键行动的指南
- 绩效度量

流程和程序应基于事件响应策略和计划。文档化的程序应说明应如何执行技术流程和其他操作程序。程序可以定期测试或演练，以验证其准确性，并可用于帮助培训新人员。虽然不可能为每种可能的情况制定详细的程序，但组织应考虑记录响应最常见类型的事件和威胁的程序。组织还应制定和维护特别重要流程的程序，这些流程在紧急情况下可能需要紧急使用，例如重新部署组织的主要身份验证平台。

许多组织选择创建行动手册，作为记录其程序的一部分。行动手册为人们在各种场景或情况下执行提供了可操作的步骤或任务。将程序格式化在行动手册中而不是其他格式中，可以提高其可用性。有关事件响应行动手册的示例，请参见网络安全和基础设施安全局(CISA)网络安全事件与脆弱性响应行动手册[CISA-PB]。

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.

3. CSF 2.0 网络事件风险管理社区概况

*CSF*社区概况是CSF结果的基线，其创建和发布旨在应对多个组织之间降低网络安全风险的共同利益和目标。社区概况通常针对特定部门、子部门、技术、威胁类型或其他用例而制定[CSF2.0]。

本节定义了 NIST 的 CSF 2.0 网络安全事件风险管理社区概况。它使用 CSF 核心作为基础和优先考虑对事件响应重要的网络安全结果，提出建议，并在事件响应的背景下为某些 CSF 结果提供其他支持信息[CSWP32]。社区概况分为两个表格：表 2 涵盖准备(治理、识别和保护)和经验教训(识别-改进)，而表 3 涵盖事件响应(检测、响应和恢复)。

每个 CSF 2.0 功能、类别和子类别在两张表格之一中各有自己的行。每一行在事件响应背景下的相对优先级由以下之一表示：

- **高：**作为大多数组织的核心事件响应活动
- **中：**直接支持大多数组织的事件响应活动
- **低：**间接支持大多数组织的事件响应活动

这些优先级旨在作为组织的起点，鼓励组织自定义此社区概况以反映其自身的优先级和需求。

最后一列可能包含一个或多个项目，这些项目建议做什么或描述某些行的额外考虑因素或支持信息。该列中的每个项目都有一个ID，以以下之一开头：

- "R"(建议：组织应做的事情)
- "C"(考虑：组织应考虑采取的行动)
- "N"(注：除建议和考虑因素之外的附加信息)R、C或N标识及其编号可以附加到该行的CSF ID上，以创建在社区概况中唯一的标识符(例如，"GV.OC-03.R1"是CSF子类别GV.OC-03的建议1)。

在CSF较高层级(功能或类别)提出的建议、考虑因素和注释也适用于其组成元素(类别或子类别)。

建议、考虑因素和注释补充了CSF 2.0已通过其文档和在线资源提供的内容。建议、考虑因素和注释并非详尽无遗，并非所有内容都适用于每个组织。建议、考虑因素和注释中提到的技术是撰写本文时的示例，可能会过时。

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

一些建议、考虑事项和注释使用了本出版物中未定义的术语(例如，“数据泄露”)。采用社区概况的组织应在其自身环境、用例以及适用法律法规的背景下定义这些术语。读者也可以选择查阅NIST 的术语表，其中包含来自众多 NIST 标准、指南和其他出版物的术语和定义的汇总。社区概况旨在供大多数组织使用，无论其行业、规模或其他因素如何。可以针对更窄的受众(例如联邦机构、小型企业或教育机构)开发此社区概况的其他版本。有关 CSF 2.0 社区概况的更多信息，请参阅框架资源中心。

3.1. 准备与经验教训

表2包含社区概况的第一部分：准备和经验教训，二者均支持表3中定义的社区概况的事件响应部分。

> 注：概况这一部分中的大多数CSF要素并非特定于执行事件响应活动，因此它们相对于事件响应的优先级较低，并且不包含建议或考虑事项。**这并不意味着组织不需要实现它们，而是说它们超出了响应事件的直接范围。**

表2. CSF 2.0社区概况第1部分：准备与经验教训

CSF 要素	CSF 要素说明	优先级	建议、考虑事项、说明
治理(Govern)	组织的网络安全风险管理策略、期望和策略已建立、传达并 已监控	低	
GV.OC （组织 背景）	情况--任务， 利益相关者期望， 依赖性以及法律、监管和合同要求--围绕组织网络安全风险管理决策的--是 已理解	低	
GV.OC-01	组织使命被理解并为网络安全风险管理提供信息	低	
GV.OC-02	内部和外部 利益相关方已被理解，其需求 与 关于.....的期望 网络安全风险管理已被理解和考虑	低	
GV.OC-03	法律、监管和 合同要求	中	**R1:**网络安全要求应 纳入所有与事件相关的要求

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 要素	CSF 要素说明	优先级	建议、考虑事项、说明
	关于网络安全—— 包括隐私和公民 自由义务--被理解并加以管理		通知、数据泄露报告以及事件响应的其他方面。
GV.OC-04	关键目标、能力和 外部利益相关方依赖或 以及恢复工作。 期望组织 被理解并 结果、能力和	中	**N1:**理解关键外部 对组织运营的依赖关系有助于确定响应的优先次序 已传达
GV.OC-05	组织所依赖的 服务已被理解并 管理 结果、能力和	中	**N1:**理解关键依赖关系 外部资源(例如，基于云的托管提供商和托管服务提供商)可以帮助确定响应和恢复工作的优先级。
GV.RM(风险战略） 决策	组织的优先事项， 约束、风险容忍度和 风险偏好声明和假设已建立、 传达并用于支持运营风险 网络安全风险管理	低	
GV.RM-01	风险管理目标已建立并经组织利益相关方同意	低	
GV.RM-02	风险偏好和风险容忍度声明已建立、传达并维护	低	
GV.RM-03	活动和结果被 纳入企业风险 管理流程 战略方向	中	**R1:**制定相应流程，以便 与事件相关的决策将参考组织面临的其他类型风险(例如，隐私、运营、安全、声誉、AI)，而不仅仅是孤立的网络安全风险。
GV.RM-04	一种标准化方法，用于 描述适当的风险响应选项已建立 并传达	低	
GV.RM-05	为网络安全风险(包括来自供应商和其他第三方的风险)建立了跨组织的沟通渠道	低	
GV.RM-06	计算、记录、 分类和优先排序 计算、记录、分类和优先排序 网络安全风险已建立 并传达	中	**N1:**拥有一种标准化方法用于 计算网络安全风险有助于确定响应和恢复工作的优先级，并比较估计的和实际的 事件的影响。 **N2:**此类方法还可用于建立标准并为决策提

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 要素	CSF 要素说明	优先级	建议、考虑事项、说明
			制定何时升级或提升事件响应活动的决策。
GV.RM-07	战略机遇(即正向风险)得到描述并纳入组织网络安全风险讨论	低	
GV.RR(角色，职责、和权限）	网络安全角色、职责和权限以促进问责、绩效评估和持续改进已建立并传达	中	**R1:**网络安全角色、职责、和权限应包括事件响应。
GV.RR-01	组织领导层对网络安全风险负责并承担责任，并培育一种风险意识强、合乎道德且持续改进	中	**R1:**参见 GV.RR 的建议。
GV.RR-02	角色、职责和与以下相关的权限网络安全风险管理已建立、传达、理解并执行	中	**N1:**涉及以下方面的角色与职责网络安全事件响应通常存在于整个组织中，并且通常包括第三方(例如合同方)来帮助为组织执行事件响应活动。 **R1:**所有涉及网络安全事件响应的角色和职责应记录在组织的策略中。**R2:**所有适当的个人或方应被授予履行其事件响应相关职责所需的权限。 **R3:**参见 GV.RR 的建议。
GV.RR-03	充足的资源分配与网络安全风险策略、角色、职责和政策	低	
GV.RR-04	网络安全已纳入人力资源实践	低	
GV.PO(策略)	组织网络安全政策已建立、传达并强制执行	高	**R1:**网络安全政策应包括事件响应政策。
GV.PO-01	管理政策网络安全风险基于组织背景、网络安全策略和优先级建立，并得到传达和执行	低	
GV.PO-02	管理政策网络安全风险得到审查，	低	

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 要素	CSF 要素说明	优先级	建议、考虑事项、说明
	更新、传达和执行，以反映需求、威胁、技术和组织 使命		
GV.OV(监督)	组织范围内网络安全风险管理活动和绩效的结果用于为风险管理提供信息、改进和调整 战略	低	
GV.OV-01	活动和结果被 战略结果经过审查 以指导和调整战略 和方向	中	**R1:**将过去的网络安全事件纳入 在调整组织的网络安全风险管理策略时予以考虑 和方向。
GV.OV-02	网络安全风险 管理策略 经过审查和调整，以 确保覆盖 组织要求与风险	中	**R1:**承担过往网络安全带来的风险 在审查组织的网络安全风险时，将事件纳入考量 管理策略。
GV.OV-03	组织网络安全风险管理绩效经过 评估和审查以确定所需的调整	低	
GV.SC （网络安全 供应链风险 管理）	网络供应链风险 管理流程是 已识别、已建立， 由组织进行管理、监控和改进 利益相关方	低	
GV.SC-01	网络安全供应链风险管理计划、策略、目标、策略和流程由组织建立 并达成一致 利益相关方	低	
GV.SC-02	供应商的网络安全角色和 职责， 客户和合作伙伴 建立、传达并 内部协调并 外部	低	**N1:**参见 GV.RR-02 获取更多信息 有关网络安全事件响应相关角色和职责的信息 对于第三方。
GV.SC-03	网络安全供应链风险管理被整合 到网络安全和企业风险管理、风险评估和改进中 流程	低	
GV.SC-04	供应商已知，并按关键性 排定优先级	低	

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 要素	CSF 要素说明	优先级	建议、考虑事项、说明
GV.SC-05	应对供应链中网络安全风险的要求 已建立、 优先排序并整合到 合同和其他类型的 和信息共享中。 与供应商及其他相关第三方的协议	中	**R1:**网络安全供应链风险 管理要求应包括网络安全绩效以及脆弱性、威胁和事件披露 关系
GV.SC-06	在签订正式供应商或其他第三方 之前进行规划和尽职调查以降低 风险 相关供应商和其他	低	
GV.SC-07	供应商、其产品和服务以及其他第三方带来的风险在关系过程中得到理解、记录、优先排序、评估、响应和监控	低	
GV.SC-08	第三方被纳入 事件规划、响应 和恢复活动 测试和演练。	中	**N1:** GV.SC-08 子类别具体针对 事件规划、响应和恢复。**N2:**有关更多信息，i 测试和演练。
GV.SC-09	供应链安全实践被整合到网络安全和企业风险管理计划中，其绩效在整个技术产品和服务生命周期中得到监控	低	
GV.SC-10	网络安全供应链风险管理计划包括在合作伙伴关系或服务结束后发生的活动的规定 协议	低	
ID(识别)	组织当前的 网络安全风险 已理解	中	**N1:**所有识别类别均有益于 预防、响应和恢复 来自事件。
ID.AM(资产管理）	资产（例如，数据、硬件、 软件、系统、设施、 服务、人员），这些资产使 组织能够实现 业务目的，已被识别 并与.....保持一致地管理 它们对组织目标和组织风险策略的相对重要性	中	**N1:**所有资产管理信息均可 对事件响应人员有许多帮助 方式，例如了解事件的影响、识别可能成为目标的其他资产以及确定响应的优先级 已传达
ID.AM-01	由组织管理的硬件 清单 得到维护	中	**R1:**使当前状态和自动 组织使用的内部和外部硬件的更新清单

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 要素	CSF 要素说明	优先级	建议、考虑事项、说明
			可用于发现和解决脆弱性、监控操作和使用以检测不利网络安全事件以及识别“影子 IT”使用。
ID.AM-02	由组织管理的软件、 服务和系统 的清单 得到维护	中	**R1:**使当前状态和自动 组织使用的内部和外部软件、服务和系统的更新清单，可用于发现和解决脆弱性、监控操作和使用以检测不利网络安全事件以及识别“影子 IT”使用。
ID.AM-03	组织授权的 网络通信和 通信的表示 内部和外部网络 表示。	中	N1： 维护网络数据流 表示可以提高检测恶意数据流的准确性，并且 数据流得到维护 **C1:**考虑利用自动化和零信任架构来自动创建和维护网络数据流 由供应商提供的
ID.AM-04	服务清单 得到维护	中	**R1:**当前且自动更新 组织供应商提供的服务清单应可用于发现和解决脆弱性、监控操作和使用以检测不利网络安全事件以及识别“影子 IT”使用。
ID.AM-05	资产根据 分类、关键性、 资源以及对 使命	中	**R1:**确定组织资产的优先级 - 包括硬件、软件、服务、系统和数据--并了解这些资产与其他资产之间的依赖关系，应有助于指明组织在保护、检测、响应和恢复方面应集中资源的地方。
ID.AM-07	数据和 相应元数据的清单，针对 指定数据类型的 得到维护	中	**R1:**拥有包含以下内容的数据清单： 数据分类、所有者和逻辑与物理位置应提供有关事件中可能涉及哪些数据的宝贵信息。
ID.AM-08	系统、硬件、软件、 服务和数据在其整个 生命周期内得到管理	中	**R1:**管理硬件、软件、服务， 及其整个生命周期中的系统 应将网络安全纳入 考虑因素，例如安全配置它们、减少攻击面以及在资产转移或迁移时更新清单信息。
ID.RA(风险评估）	对以下方面的网络安全风险 组织、资产和 个人受到的风险被 组织所理解	中	**N1:**风险评估实践至关重要 用于减少以下事件的数量： 发生及其造成的影响。风险评估是一个广泛的议题，超出了

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 要素	CSF 要素说明	优先级	建议、考虑事项、说明
			本概况的范围，而非概述其对事件的重要性 响应。 **N2:**有关网络安全风险的更多信息，请参见[SP **N3:**有关网络安全风险评估的更多信息，请参见
ID.RA-01	资产中的脆弱性被 识别、验证并 记录	中	R1：理解当前已知 网络安全漏洞，以便在评估风险时做出明智的决策。这应包括所有类型的已知网络安全漏洞，例如组织或第三方开发的软件(包括固件和基于软件的服务)中的缺陷、软件配置错误、网络和系统设计与实现弱点、容纳计算资产的设施中的物理漏洞和韧性问题，以及硬件和软件中的完整性违规(例如，假冒、篡改证据)。 **N1:**参见 ID.RA 的注释。
ID.RA-02	网络威胁情报从信息 共享论坛和来源 获取	高	**N1:**网络威胁情报(CTI)是威胁 经过聚合、转换、分析、解释或丰富以提供决策过程所需上下文的信息。组织可以从自动化CTI馈送、信息共享论坛和其他来源接收CTI。 **N2:** CTI 在多个方面对事件响应和恢复有用，包括获取有关新威胁的信息、提高具有事件检测或响应能力的网络安全技术的准确性，以及了解攻击者使用的战术、技术和程序(TTP)。TTP 描述行为者的行为。有关威胁及其 TTP 的信息可通过存储库和知识库广泛获取。**N3:**[SP800-150] 提供了关于消费、使用和存储 CTI 以及建立 CTI 关系的指南。**N4:**参见 ID.RA 的注释。
ID.RA-03	对组织的内部和外部威胁 被识别 并记录	中	**R1:**识别内部和外部威胁 在常规操作期间以及从CTI中。**N1:**组织在识别时可考虑的其他可能方法

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 要素	CSF 要素说明	优先级	建议、考虑事项、说明
			威胁包括威胁狩猎和欺骗技术的使用。**N2:**参见 ID.RA 的注释。
ID.RA-04	潜在影响和 威胁被利用的可能性 脆弱性被识别并 记录	中	**N1:**记录潜在影响及 确定威胁利用漏洞的可能性对于判断是必要的 风险。 **N2:**参见 ID.RA 的注释。
ID.RA-05	威胁、脆弱性、 可能性和影响被 用于理解固有 风险并为风险响应 优先级排序提供依据	高	**R1:**已建立机制的组织 用于在其网络安全风险管理计划中估算网络安全风险，应使用这些机制来 事件响应目的。 **C1:**考虑使用威胁建模和其他方法，以帮助理解攻击向量、攻击面以及通过组织资产的横向路径等有助于风险的因素。**N1:**参见 ID.RA 的注释。
ID.RA-06	风险响应被选择、 优先级排序、规划、跟踪、 并传达	高	**N1:**需要风险响应来防止 防止未来事件发生以及现有 事件再次发生。 **R1:**组织的策略、过程和程序应提供指导(例如，标准)，以便在各种情况下就适当的风险响应做出决策。 **N2:**四种风险响应类型是 1) 接受(按原样接受风险),2) 缓解(通过消除脆弱性和/或部署额外的安全控制以减少脆弱性利用来降低风险),3) 转移(通过与另一方分担部分后果来降低风险)，以及 4) 避免(通过消除攻击面确保风险不发生)。 **N3:**有关风险响应的更多信息，请参见[IR8286]。 **N4:**参见 ID.RA 的注释。
ID.RA-07	变更和例外是 已管理、评估风险影响、记录并跟踪	中	**N1:**参见 ID.RA 的注释。
ID.RA-08	接收、 分析和响应 脆弱性披露的流程已 建立	中	**N1:**漏洞披露是指当 第三方向组织报告组织某一系统中疑似脆弱性 组织。 **N2:**有关漏洞披露的更多信息，请参见[SP800-216]。 **N3:**关于使用可能的数据格式的指导，参见[SP800-150] 第 4.5.2 节

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 要素	CSF 要素说明	优先级	建议、考虑事项、说明
			协助维护资产清单与脆弱性披露来源之间的交叉引用。**N4:**参见 ID.RA 的注释。
ID.RA-09	关键供应商的真实性和完整性 在获取和使用之前，对硬件和软件进行评估	中	**N1:**参见 ID.RA 的注释。
ID.RA-10	得到评估 在获取之前	低	**N1:**参见 ID.RA 的注释。
ID.IM （改进）	组织改进 在所有 CSF 功能中识别网络安全风险管理过程、程序和活动	中	**N1:**见 ID 的注释。
ID.IM-01	改进被识别 来自评估	中	**R1:**定期评估事件响应 计划绩效以识别应纠正的问题和缺陷。**N1:**可能的评估形式包括自评估、第三方评估和独立审计。
ID.IM-02	改进被识别 来自安全测试和 演练，包括与供应商 和 相关第三方协调进行的	高	**N1:**事件响应演练与测试 可为计划评估提供有用信息，并使员工和相关第三方(例如，关键服务提供商和产品供应商)为未来的事件响应活动做好准备。 **N2:**关于模拟、桌面讨论和其他形式演练的更多信息，参见[SP800-84]。
ID.IM-03从操作过程、	程序和活动的执行中识别改进	高**N1:**操作过程、程序和活动的执行包括所有事件响应和恢复工作。**N2:**影响事件响应的改进可以针对事件响应计划本身(例如，计划、策略、过程、程序)或组织网络安全风险管理活动的其他方面(例如，识别当前未被保障措施阻止或未被检测技术标记的 TTP)。 **N3:**改进通常是在为事件创建后续报告或在事件恢复工作结束时召开"经验教训"会议时识别的，特别是如果事件是重大事件。这提供了一个机会来审查发生了什么、采取了哪些行动以及这些行动的有效性，并听取所有	

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 要素	CSF 要素说明	优先级	建议、考虑事项、说明
			参与事件的各方意见。此类会议有助于识别组织事件响应计划和网络安全风险管理工作的潜在改进并确定其优先级。
ID.IM-04	事件响应计划和其他影响运营的网络安全计划已建立、传达、维护和改进	高	**N1:**存在多种类型的网络安全计划与事件响应相关，包括 1) 事件响应计划，其为实施事件响应能力提供路线图；2) 脆弱性管理计划，其帮助识别和评估所有类型的脆弱性，并确定风险响应的优先级、测试和实施；以及 3) 业务连续性计划。**R1:**将业务连续性计划与事件响应计划同步，因为事件可能削弱业务韧性。**R2:**定期或在识别出需要重大改进时审查和更新所有网络安全计划。**R3:**每个网络安全计划应基于组织独特的需求、使命、规模、结构和功能。**R4:**每个网络安全计划应识别成功执行该计划所需的资源和管理支持。**N2:**了解网络安全事件及其影响的业务连续性规划专业人员可以微调业务影响评估、风险评估和运营连续性计划。此外，由于业务连续性规划人员在严苛情况下最大限度减少运营中断方面拥有广泛专业知识，他们在规划对特定事件类型(如拒绝服务(DoS) 状况)的响应时可能很有价值。
PR(保护)	管理组织网络安全风险的保障措施被使用	中	**N1:**降低事件数量缩短运营中断时间，使响应团队能够专注于高影响情况，并减少确实发生的事件的影响(例如，通过使攻击者更难在环境中横向移动，从而减缓其速度)。 **N2:**了解已实施的保护机制可以帮助人员部署检测保护失效和绕过的方法。

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 要素	CSF 要素说明	优先级	建议、考虑事项、说明
			N3:提供有关保护资产的建议和考虑事项超出了本概况的范围，除了少数特别有利于事件响应的实践说明 活动。
PR.AA(身份管理、 身份验证、 和访问 控制）的访问	对物理和逻辑 资产仅限于授权用户、服务和硬件，并根据评估的未授权访问风险进行管理	中	**N1:**参见 PR 的注释。
PR.AA-01	身份和凭证用于 授权用户、服务和硬件由以下管理： 组织所理解	中	**N1:**参见 PR 的注释。
PR.AA-02	身份经过验证并 基于交互上下文绑定到凭证	中	**N1:**参见 PR 的注释。
PR.AA-03	用户、服务和硬件 已通过身份验证	中	**N1:**参见 PR 的注释。
PR.AA-04	身份断言被 受保护、传达和 验证	中	**N1:**参见 PR 的注释。
PR.AA-05	访问权限， 权限和授权在策略中定义、管理、执行和审查，并纳入最小权限和职责分离原则	中	**N1:**参见 PR 的注释。
PR.AA-06	对资产的物理访问是 受到管理、监控和执行，并与……相称 风险	中	**N1:**参见 PR 的注释。
PR.AT(意识 和培训）	组织的人员 获得网络安全意识与培训，以便他们能够执行与网络安全相关的任务	中	**N1:**参见 PR 的注释。
PR.AT-01	人员被提供 意识与培训，以便他们具备在考虑网络安全风险的情况下执行一般任务的知识和技能	中	**N1:**参见 PR 的注释。
PR.AT-02	专业角色中的个人 被提供意识 和培训，以便他们 具备在考虑网络安全风险的情况下执行 相关任务的知识和技能	中	**R1:**基于角色的培训应包括 与事件相关的职责。 **N1:**参见 PR 的注释。

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 要素	CSF 要素说明	优先级	建议、考虑事项、说明
PR.DS(数据安全）	数据被一致地管理 与组织的风险策略一致，以保护信息的保密性、完整性和可用性	中	**N1:**参见 PR 的注释。
PR.DS-01	保密性、完整性， 以及静态数据的可用性得到保护	中	**N1:**参见 PR 的注释。
PR.DS-02	保密性、完整性， 并保护传输中数据的可用性	中	**N1:**参见 PR 的注释。
PR.DS-10	保密性、完整性， 保护使用中数据的可用性	中	**N1:**参见 PR 的注释。
PR.DS-11	数据备份被创建、 保护、维护和 测试	高	**N1:**备份可能尤为重要 用于恢复目的当数据完整性 或可用性受到影响。 **N1:**参见 PR 的注释。
PR.PS(平台安全）	硬件、软件（例如， 固件、操作系统、应用程序)以及物理和虚拟平台的服务按照组织的风险策略进行管理，以保护其保密性、完整性和可用性	中	**N1:**参见 PR 的注释。
PR.PS-01	配置管理 实践已建立并 应用	中	**N1:**参见 PR 的注释。
PR.PS-02	软件被维护， 根据风险进行替换和移除	中	**N1:**参见 PR 的注释。
PR.PS-03	硬件被维护， 根据风险进行替换和移除	中	**N1:**参见 PR 的注释。
PR.PS-04	日志记录被生成并 可用于持续 监控	中	**N1:**日志对于以下方面尤为重要： 记录和保存对事件检测、响应和恢复活动至关重要的信息。 **N2:**关于日志管理的更多信息，参见[SP800-92r1]。**N3:**参见 PR 的注释。
PR.PS-05	安装和执行 未经授权的软件是 已阻止	中	**N1:**参见 PR 的注释。
PR.PS-06	安全软件开发 实践被整合，并且 其性能受到监控 贯穿整个软件 开发生命周期	中	**N1:**有关安全的更多信息 软件开发实践，包括响应涉及已发布软件的脆弱性或事件，参见[SP800-218]. **N2:**参见 PR 的注释。

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 要素	CSF 要素说明	优先级	建议、考虑事项、说明
PR.IR(技术基础设施韧性）	安全架构是按照组织的风险策略进行管理，以保护资产保密性、完整性和可用性以及组织韧性	中	**N1:**参见 PR 的注释。
PR.IR-01	网络和环境是保护免受未经授权的逻辑访问和使用	中	**N1:**参见 PR 的注释。
PR.IR-02	组织的技术资产受到保护，免受环境威胁	中	**N1:**参见 PR 的注释。
PR.IR-03	机制被实施在正常和不利情况下实现韧性要求	中	**N1:**参见 PR 的注释。
PR.IR-04	充足的资源容量以确保可用性得以维持	中	**N1:**参见 PR 的注释。

3.2. 事件响应

表 3 包含社区概况的第二部分：事件响应。

注意：概况此部分中的所有 CSF 要素均**特定于响应事件**，因此它们相对于事件响应的优先级高于第一部分中的要素。相应地，此部分中的所有 CSF 要素均附有建议或考虑事项。

表 3. CSF 2.0 社区概况第 2 部分：事件响应

CSF 要素	CSF 要素说明	优先级	建议、考虑事项、说明
检测	可能的网络安全攻击和入侵被发现并分析	高	**N1:**检测功能涵盖所有为发现和刻画潜在不利事件、进而发现网络安全事件而执行的监控与分析活动。
DE.CM（持续监控）	资产受到监控以发现异常、指标入侵及其他潜在不利事件	高	**R1:**持续监控未经授权的活动、偏离预期活动，以及安全方面的变化态势应始终涵盖以下类型的资产：网络与网络服务；计算硬件与软件、运行时环境及其数据；物理环境；人员活动与技术使用；以及外部服务提供商的活动。 **C1:**考虑将网络威胁信息与持续监控结合使用，以帮助识别原本可能被视为良性活动的潜在恶意活动。

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 要素	CSF 要素说明	优先级	建议、考虑事项、说明
			R2:调整持续监控技术，将误报和漏报降至可接受水平。
DE.CM-01	网络和网络服务 受到监控以发现潜在的 不利事件	高	R1：监控应涵盖有线和 无线网络、网络 通信与流量、网络服务(例如 DNS 和 BGP)，以及设施内未经授权或 rogue 网络的存在。
DE.CM-02	物理环境受到 监控以发现潜在的 不利事件	高	**R1:**监控物理环境 应包括进入所有受控区域的所有成功和失败的访问尝试、人员与设备进出设施安全区域的活动，以及物理访问被篡改的迹象 控制措施。
DE.CM-03	人员活动和 技术使用受到监控 以发现潜在不利 事件	高	R1：监控人员活动及 技术使用应包括异常用户活动或异常活动模式、身份验证与逻辑访问尝试，以及欺骗技术的使用。
DE.CM-06	外部服务提供商 活动和服务是 监控以发现潜在的 不利事件	高	**R1:**监控外部服务提供商 活动与服务应包括提供商对组织系统执行的远程和现场管理与维护活动，以及基于云的服务、互联网服务提供商和其他服务提供商偏离预期行为的情况。
DE.CM-09	对计算硬件与软件、运行时环境及其数据进行监控，以发现潜在不利事件	高	**R1:**监控电子邮件、Web、文件共享、协作服务及其他常见攻击途径，以检测恶意软件、网络钓鱼、数据泄露、数据外泄及其他不利事件。 **R2:**监控身份验证尝试，以识别针对凭据的攻击和未经授权的凭据使用。 **R3:**监控软件和硬件配置，以发现偏离安全基线的情况。 **R4:**监控硬件和软件(包括网络安全防护机制)，以发现篡改、故障或失陷的迹象。 **R5:**监控端点以发现网络健康问题(例如缺少补丁、恶意软件感染或未经授权的软件)，并在授权访问之前将存在问题的端点重定向到修复环境。

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 要素	CSF 要素说明	优先级	建议、考虑事项、说明
DE.AE(不利 事件分析）	异常、指标 入侵及其他 潜在不利事件被 分析以描述 事件并检测网络安全 事件	高	**N1:**不良事件分析涉及 研究潜在不利 持续监控收集的事件，以发现可能的攻击和入侵，并在事件发生时予以宣告，从而启动事件响应 活动。 **R1:**需要分析的可能不利事件的数量通常相当大，因此组织应依赖技术解决方案，将大型事件数据集过滤为适合人工查看和分析的子集。 **N2:**事件的保真度因多种因素而异。异常可能有良性或恶意的基础。有些事件在噪声中相对容易发现，而另一些则需要深入、专业的技术知识和经验。**N3:** CTI在及早检测恶意活动、减少其影响和缩短恢复时间方面可能具有不可估量的价值。事件的迹象在攻击生命周期后期可能更为明显，但事件的影响和范围可能大得多。 **R2:**组织应努力在攻击生命周期的更早阶段发现事件，并对事件检测和响应采取主动方法。
DE.AE-02	潜在不利事件被 分析以更好地理解 相关活动	高	**R1:**使用工具(例如，安全信息 以及事件管理[SIEM]；安全编排、自动化和响应[SOAR])，以持续监控日志事件中的已知恶意和可疑活动，并生成其发现结果的报告。 **R2:**在日志分析工具中利用最新的CTI，以提高检测准确性，并刻画威胁行为者、其方法和入侵指标。 **R3:**对于无法通过自动化充分监控的技术，定期对日志事件进行人工审查。
DE.AE-03	信息从 多个来源进行关联	高	**R1:**持续传输日志数据 由其他来源生成并发送到相对较少数量的日志服务器。 **R2:**使用事件关联技术(例如SIEM、SOAR)来收集多个来源捕获的相关数据片段。**R3:**利用CTI帮助关联日志来源之间的事件。

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 要素	CSF 要素说明	优先级	建议、考虑事项、说明
DE.AE-04	不利事件的估计影响和范围 被 已理解	高	**R1:**评估影响和范围 通过自动化(例如SIEM、SOAR)和/或人工方式分析不利事件，并审查和完善估计结果。
DE.AE-06	不利事件的信息被 提供给授权人员和 工具	高	**R1:**生成警报并将其提供给 网络安全和事件响应工具与人员(例如SOC和事件响应人员)。 **R2:**使日志分析发现结果随时可供事件响应人员和其他授权人员访问。 **R3:**考虑在发生某些类型的警报时，在组织的工单系统中自动创建和分配工单。
DE.AE-07	网络威胁情报和 其他上下文信息是 整合到分析中	高	**R1:**整合最新的CTI及其他 将上下文信息(例如资产清单)纳入不利事件分析，以提高检测准确性，并刻画威胁行为者、其方法和入侵指标。**R2:**从供应商、销售商和第三方安全机构快速获取并分析组织所用技术的脆弱性披露信息 公告。 **N1:**关于CTI的消费、使用和存储以及建立CTI关系的指南，参见[SP800-150]。
DE.AE-08	当不利事件满足定义的 事件标准时，宣布 事件	高	**R1:**将事件标准应用于已知和 所分析活动的假定特征，并考虑已知的误报，以确定是否应宣告事件。
RS(响应)	关于检测到的事件响应活动的 网络安全事件被采取	高	**N1:**响应功能是核心所在 行动。
RS.MA(事件管理)	对检测到的 网络安全事件的响应被 管理	高	**N1:**事件管理涉及 监督对所有事件的响应并 根据需要调整优先级和资源。评估事件的整体风险并应用适当的优先级排序，或许是事件响应过程中最关键的决策点。**R1:**由于资源限制，事件不应按先到先得的方式处理。 **R2:**事件分级研判、优先级排序、升级和提升，以及关于何时启动恢复流程的决策，都应基于一组风险评估因素。这组因素可以涵盖

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 要素	CSF 要素说明	优先级	建议、考虑事项、说明
			从简单到极其复杂，取决于需求和成熟度 组织。 **N2:**可能的风险评估因素示例包括资产关键性、事件的功能影响、事件的数据影响、观察到的活动阶段、威胁行为者特征以及可恢复性。**R3:**应跟踪每个事件的事件响应状态以及相关信息，例如事件摘要、与事件相关的入侵指标、每个分配操作的状态和预期时间范围以及要采取的后续步骤。
RS.MA-01	事件响应计划被 与以下协调执行 相关第三方一旦 事件已宣布	高	**R1:**检测技术应 自动报告其发生的事件 已确认。 **C1:**考虑为每个事件指定一名事件负责人。 **R2:**如适当，联系组织的事件响应服务提供商请求协助。**R3:**根据需要启动其他网络安全计划的执行(例如业务连续性和灾难恢复计划)，以支持事件响应。
RS.MA-02	事件报告经过分级研判并 验证	高	**R1:**对新进行初步审查 事件报告以核实 网络安全事件已经发生，然后估计事件的严重性和响应所需的紧急程度 它。 **R2:**建立机制，使第三方能够报告涉及组织的可能事件。报告应被仔细监控并认真对待。例如，组织可能会被声称其系统正受到组织内某系统攻击的一方联系。外部用户可能会报告其他指标，例如服务不可用。其他事件响应团队也可能向 组织。
RS.MA-03	事件被分类并 确定优先级	高	**R1:**对以下内容进行更详细的审查 事件，以帮助按事件类型(例如数据泄露、勒索软件、账户接管、拒绝服务)对其进行分类。

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 要素	CSF 要素说明	优先级	建议、考虑事项、说明
			R2:根据每个事件的范围、可能影响、时间紧迫性和资源可用性，确定事件响应执行速度的优先级。**R3:**通过平衡快速从事件中恢复的需要与观察攻击者或进行更彻底调查的需要，为活动中的事件选择事件响应策略。 **N1:**每个响应策略决策都有权衡。例如，支持观察攻击者行为或进行更彻底调查的策略，可能与快速恢复正常运行的需要相冲突。
RS.MA-04	事件根据需要进行升级或提升	高	**N1:**升级通常指增加资源或时间框架，而提升通常表示让更高层级的管理层参与响应工作。 **R1:**跟踪并验证所有进行中事件的状态，以便能够识别需要更多响应资源或需要改变响应策略的事件，并迅速启动必要的变更。
RS.MA-05	启动事件的标准恢复被应用	高	**R1:**将事件恢复标准应用于事件的已知和假定特征，以确定何时应启动事件的恢复流程。**R2:**将事件恢复活动可能造成的运行中断纳入考虑，以确定何时应启动恢复。
RS.AN(事件分析)	进行调查以确保有效响应并支持取证和恢复活动	高	**N1:**事件分析类别侧重于关于调查、确定和记录事件期间发生了什么，以及如何发生和为何发生发生了。
RS.AN-03	进行分析以确定发生了什么在事件期间以及根本事件的原因	高	**R1:**确定事件发生的顺序，该顺序在事件期间发生了什么，以及涉及了哪些资产和资源在每一个那些事件中。 **R2:**尝试确定哪些脆弱性、威胁和威胁行为者直接或间接参与了事件。 **R3:**分析事件以找出潜在的或系统性的根本原因。**R4:**检查任何已部署的网络欺骗技术，以获取有关攻击者行为的更多信息。

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 要素	CSF 要素说明	优先级	建议、考虑事项、说明
			N1:此信息也可能有助于识别网络安全风险管理中应加以解决的弱点，以防止将来发生类似事件。
RS.AN-06	在调查期间执行的操作 被记录，并且 记录的完整性和 来源被保留	高	N1：发现的事实和采取的行动 在事件响应任务期间，可以通过多种方式记录，包括纸质日志本、音频/视频记录或自动会话监控和记录，具体以组织的事件响应计划和策略允许为准。 **R1:**保护事件响应记录的保密性和完整性，并确保只有授权人员 访问。 **N2:**事件响应记录可能包含敏感信息，例如关于被利用的脆弱性、近期数据泄露以及可能执行了不当操作的用户的数据。事件负责人通常负责确保事件响应记录得到妥善保护。
RS.AN-07	事件数据和元数据被 收集，并且其完整性和 来源被保留	高	**N1:**许多事件响应涉及 收集事件数据和元数据。可能不会对发生的每一起事件都使用监管链程序进行正式的证据收集和处理(例如，大多数恶意软件事件不会导致起诉)。然而，收集到的事件数据仍被视为证据，其定义为"相信或不相信的依据；用于证明或确立真伪的数 据"[SP800-160v1]。 **R1:**按照组织的事件证据保全程序和数据保留政策，收集并保留事件中的证据，并考虑诸如起诉的可能性，以及保留数据及未来访问这些数据所需的硬件和软件的成本等因素。
RS.AN-08	事件的严重程度被 估计并验证	高	**N1:**确定事件的规模 往往是事件响应中最具挑战性的方面之一。 **R1:**在已知被针对的资产和其他潜在目标上，查找入侵指标、持久化证据以及其他事件迹象。

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 要素	CSF 要素说明	优先级	建议、考虑事项、说明
			跳过此活动或以肤浅的方式执行它，可能导致低估事件的严重程度，从而使事件在组织不知情或未监控的情况下在其他目标上无限期地持续下去。
RS.CO(事件响应报告与沟通)	响应活动被与内部和外部利益相关方协调，视法律、法规或政策	高	**N1:**事件响应报告与沟通活动往往归入四个类别。事件协调涉及沟通当前和针对特定事件在具有事件响应角色和职责的内部和外部各方之间计划的事件响应活动。事件通知涉及正式告知受影响的客户、员工、合作伙伴、监管机构或其他方有关数据泄露或其他事件。公共通信涉及向公众传达特定事件的状态，例如回应媒体询问。事件信息共享涉及基于在组织技术资产内观察到的活动与他人共享网络安全威胁信息，通常是自愿的。 **R1:**组织应事先建立机制，以便在发生事件时与受影响方进行协调 需要。
RS.CO-02	内部和外部利益相关方被告知事件	高	**R1:**当对事件进行分析并按优先级排序后，事件响应团队应与组织内外的适当人员协调，以便所有需要参与的人员都能发挥其作用。**R2:**遵循既定的有关事件协调的程序，包括必须向谁报告什么内容以及在什么时间报告(例如，初始通知、定期状态更新)。 **R3:**按照与组织所属行业、地理位置、客户所在地以及适用于组织的任何其他特征相关的现行事件通知相关法律法规执行通知。事件通知是一个不断发展的主题，新的法律法规正在制定中 频繁地。

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 要素	CSF 要素说明	优先级	建议、考虑事项、说明
			R4:按照监管、法律和合同要求，将数据泄露和其他网络安全事件通知受影响的第三方。 **R5:**根据事件响应计划中的标准和管理层批准，将事件通知执法机构和监管机构。指定人员应以符合法律要求以及组织政策和程序的方式联系这些机构。
RS.CO-03	信息与 指定的内部和外部 利益相关方	高	N1：自愿事件信息共享 通常互惠互利，因为相同的威胁和攻击会同时影响多个组织。一个例子是与特定行业的信息共享和分析中心(ISAC)共享有关观察到的TTP的信息。 **N2:**组织之间共享防御策略可以增强整体态势感知并提高所有组织的韧性。威胁行为者开发或购买漏洞利用程序并部署它们是有成本的。有效识别和传播检测技术会降低攻击者的投资回报率并增加其成本。 **N3:**事件处置人员可能会与合作伙伴组织的同事协调工作，共享有关缓解跨越这些组织的攻击的战术和技术信息。参与此类关系的组织通常是彼此之间没有管辖权的同级组织。除了选择共享信息外，它们还可以汇集资源以解决共同的 问题共享。 **R1:**按照组织的响应计划和信息共享协议(包括与供应商的合同)，与利益相关方安全地共享信息。 **R2:**定期向高级领导层更新重大事件的状态。**R3:**在发生恶意内部人员活动时通知人力资源部门。**R4:**建立并遵循符合以下要求的事件响应媒体沟通程序

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 要素	CSF 要素说明	优先级	建议、考虑事项、说明
			组织关于媒体互动和信息披露的政策。
RS.MI(事件缓解)	执行活动以防止事件扩展并减轻其影响	高	**N1:**手动选择遏制和根除行动可能更容易且如果组织有标准和程序，则会更快。标准可以考虑事件类型(例如，基于云的服务泄露或用户端点勒索软件感染)，并使用RS.MA中的一些风险评估因素。另一个需要考虑的因素是遏制措施的持续时间(例如，必须在数小时内移除的紧急变通方法、要在两周内移除的临时变通方法或永久解决方案)。根除措施的持续时间可以类似地评估。 **R1:**在某些情况下，组织会将攻击者重定向到沙箱，以便监控攻击者的活动，通常是为了收集更多证据。这会延迟遏制和根除活动。事件响应团队在执行此策略之前应首先与法律部门讨论其可行性。故意延迟可能很危险，因为攻击者可能升级未经授权的访问或破坏其他系统。
RS.MI-01	事件被遏制	高	**N1:**遏制指的是防止事件的扩大。遏制可以防止额外损害并避免使组织的资源不堪重负。大多数事件需要某种形式的 遏制。 **C1:**考虑配置网络安全技术(例如，防病毒软件)和其他技术的网络安全功能(例如，操作系统、网络基础设施设备)以自动执行一些遏制操作，例如隔离恶意软件、将受损端点转移到隔离的修复网络或停止受感染容器的执行。 **C2:**考虑授权第三方(例如，组织的互联网服务提供商和云服务提供商)自动采取行动以遏制某些类型

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 要素	CSF 要素说明	优先级	建议、考虑事项、说明
			代表组织处理事件(例如，大规模 DDoS 攻击)。 **R1:**允许事件处置人员手动选择和执行遏制行动，以替代或补充自动化遏制措施。
RS.MI-02	事件被根除	高	**N1:**根除指的是缓解一种事件的影响。遏制之后，可能需要进行根除以消除持久化机制和入口点，例如删除恶意软件、禁用被入侵的用户账户，以及识别和缓解所有被利用的脆弱性。**R1:**识别组织内所有受影响的宿主和服务，以便所有缺陷和弱点都能得到修复。 **C1:**考虑配置网络安全技术和其他技术的网络安全功能(例如，操作系统、网络基础设施设备)以自动执行某些根除行动。 **C2:**考虑授权第三方(例如，组织的互联网服务提供商和云服务提供商)代表组织自动采取行动以根除某些类型的事件。**R2:**允许事件处置人员手动选择和执行根除行动，以替代或补充自动化根除措施。
RC(恢复)	受影响的资产和运营 受网络安全事件影响的 被恢复	高	**N1:**在事件恢复期间，人员将系统恢复到正常运行状态，确认系统正常运行，并在适用的情况下修复漏洞以防止类似事件。**N2:**恢复操作包括从干净的备份恢复系统、重建系统、用干净版本替换受损文件、安装补丁、更改密码以及收紧安全控制。在威胁行为者高度复杂且其战术全貌尚未完全揭示的入侵中，可能有必要采取更彻底的措施，例如更换所有受损系统的硬件(如裸机)。 **N3:**有关事件恢复的更多信息，请参见[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 要素	CSF 要素说明	优先级	建议、考虑事项、说明
RC.RP(事件恢复计划执行)	恢复活动被执行以确保运营系统和受影响的网络安全事件	高	**N1:**执行事件恢复计划涉及选择、确定优先级和在安全的环境中执行恢复操作方式；验证恢复资产的完整性；宣布事件恢复结束；并完成事件文档。 **N2:**有关事件恢复计划和计划执行的更多信息，请参见[SP800-184]。
RC.RP-01	事件响应计划中的恢复部分在从事件响应流程启动后执行事件响应流程	高	**R1:**在.....期间或在事件响应过程之后。**R2:**将所有负有恢复职责的人员告知恢复计划以及实施计划各方面所需的授权。
RC.RP-02	恢复操作的选择、范围确定、优先级排序和执行	高	**R1:**恢复措施应及时性、精确性和可靠性(例如，仅恢复受影响的文件还是恢复所有文件)。 **R2:**根据事件响应计划中定义的标准和可用资源选择恢复行动。 **R3:**根据对组织需求和资源的重新评估，更改计划的恢复行动。
RC.RP-03	备份和其他恢复资产的完整性在在使用它们进行之前已验证恢复	高	**R1:**检查恢复资产是否存在指标泄露、文件损坏及其他使用前检查完整性问题。
RC.RP-04	关键任务功能和网络安全风险管理被视为确立事件后运营规范	高	**R1:**验证基本服务是否按适当顺序恢复。 **R2:**与系统所有者合作，确认系统成功恢复并恢复正常运行。 **R3:**监控已恢复系统的性能，以验证其充分性恢复。
RC.RP-05	已恢复资产的完整性得到验证，系统和服务得到恢复，正常运行状态已确认	高	R1：检查已恢复资产是否存在以下迹象：受损情况，并在生产前根除事件的根本原因使用。 **R2:**在将恢复的系统上线之前，验证所采取的恢复行动的正确性和充分性。
RC.RP-06	事件恢复的结束是根据标准宣布的，并且事件相关文档已完成	高	**R1:**准备一份事后报告，该报告记录事件本身、所采取的响应和恢复行动以及经验教训已吸取。

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.

CSF 要素	CSF 要素说明	优先级	建议、考虑事项、说明
RC.CO(事件恢复沟通）	恢复活动被与内部和外部各方	高	**N1:**事件恢复沟通是沟通的延续RS.CO 中的活动。
RC.CO-03	恢复活动与进展在恢复运营能力方面进行沟通向指定的内部和外部利益相关方	高	**R1:**安全共享恢复信息，包括恢复进度，与响应计划和信息保持一致共享协议。 **R2:**定期向高级领导层更新重大事件的恢复状态和恢复进展。 **R3:**遵循合同中定义的规则和协议，在组织与其之间共享事件信息供应商。 **R4:**协调组织与其关键之间的危机沟通供应商。
RC.CO-04	关于事件的公开更新恢复情况通过以下方式共享经批准的方法和消息传递	高	**R1:**遵循组织的数据泄露从.....恢复的通知程序一起数据泄露事件。 **R2:**说明正在采取的从事件中恢复和防止发生再次发生。

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

参考文献

[CISA-PB] 网络安全和基础设施安全局(2021) 网络安全事件与脆弱性响应行动手册：在FCEB信息系统中规划和开展网络安全事件与脆弱性响应活动的操作程序。(网络安全和基础设施安全局，弗吉尼亚州阿灵顿)。可查阅https://www.cisa.gov/sites/default/files/publications/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf

[CNSSI-4009] 国家安全系统委员会(2022)国家安全委员会安全系统(CNSS)术语表。(国家安全局，马里兰州米德堡)。国家安全系统委员会指令(CNSSI) 4009。可查阅https://www.cnss.gov/CNSS/issuances/instructions.cfm

[CSF2.0] NIST(2024) NIST网络安全框架(CSF) 2.0。(NIST，马里兰州盖瑟斯堡),NIST网络安全白皮书(CSWP) NIST CSWP 29。https://doi.org/10.6028/NIST.CSWP.29

[CSWP32] Pascoe C, Snyder JN, Scarfone K(2024) NIST网络安全框架2.0：创建社区概况指南。(NIST，马里兰州盖瑟斯堡),NIST网络安全白皮书(CSWP) NIST CSWP 32。https://doi.org/10.6028/NIST.CSWP.32.ipd

[FISMA2014] 2014年联邦信息安全现代化法案，Pub.L.113-283, 128 Stat.3073。可在https://www.govinfo.gov/app/details/PLAW- 113publ283获取

[IR8286] Stine KM, Quinn SD, Witte GA, Gardner RK(2020) 整合网络安全与企业风险管理(ERM)。(NIST，马里兰州盖瑟斯堡),NIST机构间或内部报告(IR) NIST IR 8286。https://doi.org/10.6028/NIST.IR.8286

[SP800-30r1] 联合任务组转型倡议(2012) 开展风险评估指南。(NIST，马里兰州盖瑟斯堡),NIST特别出版物(SP) NIST SP 800-30r1。https://doi.org/10.6028/NIST.SP.800-30r1

[SP800-37r2] 联合任务组(2018) 信息系统与组织的风险管理框架：用于安全与隐私的系统生命周期方法。(NIST，马里兰州盖瑟斯堡),NIST特别出版物(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

[SP800-61r2] Cichonski PR, Millar T, Grance T, Scarfone KA(2012) 计算机安全事件处置指南。(NIST，马里兰州盖瑟斯堡),NIST特别出版物(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) 测试指南，培训和演练计划指南。(NIST，马里兰州盖瑟斯堡),NIST特别出版物(SP) NIST SP 800-84。https://doi.org/10.6028/NIST.SP.800-84

[SP800-92r1] Scarfone K, Souppaya M(2023) 网络安全日志管理规划指南。(NIST，马里兰州盖瑟斯堡),NIST特别出版物(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) 指南网络威胁信息共享。(美国国家标准与技术研究院物(SP)NIST SP 800-150。https://doi.org/10.6028/NIST.SP.800-150

[SP800-160v1] Ross RS, McEvilley M, Winstead M(2022) 工程可信安全系统。(NIST，马里兰州盖瑟斯堡),NIST 特别出版物(SP)NIST SP 800-160v1r1。https://doi.org/10.6028/NIST.SP.800-160v1r1

[SP800-184] 巴托克·M·J、斯卡福内·K·A、史密斯·M·C、维特·G·A、奇琼斯基·J·A、苏帕亚·M·P (2016) 网络安全事件恢复指南。(美国国家标准与技术研究院，马里兰州盖瑟斯堡),NIST 特别出版物(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) 联邦建议漏洞披露指南。(美国国家标准与技术物(SP)NIST SP 800-216。https://doi.org/10.6028/NIST.SP.800-216

[SP800-218] Souppaya MP, Scarfone KA, Dodson DF(2022) 安全软件开发框架框架(SSDF)1.1 版：缓解软件漏洞风险的建议。(美国国家标准与技术研究院，马里兰州盖瑟斯堡),NIST 特别出版物(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

附录 A.符号、缩写和首字母缩略语列表 CISA

网络安全和基础设施安全局

CPRT
网络安全与隐私参考工具

CSF
网络安全框架

CSP
云服务提供商

CTI
网络威胁情报

ISAC
信息共享与分析中心

ISP
互联网服务提供商

MOU
谅解备忘录

MSSP
托管安全服务提供商

NDA
保密协议

SIEM
安全信息与事件管理

SOAR
安全编排、自动化与响应

SOC
安全运营中心

SOP
标准操作程序

TTPs
战术、技术与程序

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]

附录 B.术语表

不利网络安全事件
任何可能对网络安全产生负面影响的事件。

计算机安全事件见网络安全
事件。

网络威胁情报
经过聚合、转换、分析、解释或充实，为决策过程提供必要上下文的网络威胁信息。[SP800-150，改编]

网络安全事件
在无合法授权的情况下，实际或即将危及信息或信息系统的完整性、保密性或可用性的发生情况；或构成对法律、安全策略、安全程序或可接受使用策略的违反或即将违反的威胁。[FISMA2014]

事件
涉及计算资产的任何可观察到的发生情况，包括物理和虚拟平台、网络、服务和云环境。

事件
见网络安全事件。

事件响应
对违反安全策略和推荐做法的补救或缓解。[FISMA2014]

入侵指标
表明攻击即将发生或正在进行，或表明可能已经发生入侵的技术痕迹或可观察迹象。[SP800-150，改编]

战术、技术和程序
行为者的行为。战术是对该行为的最高层级描述，技术在战术的语境下提供更详细的行为描述，而程序在技术的语境下提供更低层级、高度详细的行为描述。[SP800-150]

威胁
通过信息系统，经由未经授权的访问、信息的破坏、泄露或修改，和/或拒绝服务，可能对组织运营(包括任务、功能、形象或声誉)、组织资产、个人、其他组织或国家造成不利影响的任何情况或事件。[SP800-30r1]

脆弱性
系统、系统安全程序、内部控制或实现中的弱点，行为者或事件可能有意利用或意外触发该弱点，以访问、修改或扰乱系统的正常运行，从而导致安全事件或违反系统安全策略。[CNSSI-4009，改编]

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

附录 C.变更日志

本出版物对上一版本 NIST SP 800-61 第 2 版(2012 年)进行了如下修订：

- 对先前内容进行了全面重写，以提高清晰度和可用性，并删除过时材料以及在其他 NIST 出版物和其他联邦机构内容中已有更深入论述的材料
- 将文档重点从检测、分析、优先级排序和处理事件的指南，转变为在整个组织的网络安全风险管理活动中纳入网络安全事件响应考虑因素的建议和考量
- 重组了内容，以构成一个 CSF 2.0 社区概况
- 将大多数超链接移至新的 SP 800-61 项目网站，以便于维护
- 已重新格式化所有内容，以遵循最新的 NIST 技术报告模板

How this file was made

This is a complete Chinese translation of NIST SP 800-61r3, Incident Response Recommendations and Considerations. Tables, captions, headers, footers and numbering all keep their original positions. Nothing has been cut.

If you have documents of your own

- Contracts, tenders, standards, patents, reports: original layout kept, CNY 0.15/page
- PDF to Word: free up to 100 pages, CNY 0.10/page beyond that
- Scanned or image-only PDFs: OCR to Word, free
- No sign-up, no login: upload and download

Open the address below and try it with your own file:

https://www.ivyivy.com.cn/nist-800-61r3-zh

On-premise deployment available (subject to model and compliance review)

Machine translation, provided for reading reference only. For professional judgement and compliance citation, please refer to the original English source.

This page is a translator's note; it is not part of the original document.

这份文件是怎么做出来的

本译本是《事件响应建议（SP 800-61r3）》的中文全译本，共 48 页。表格、图注、页眉页脚、编号层级都按原文位置一一还原，未做任何删节。

你手上如果也有英文文件要处理

- 合同、标书、标准、专利、报告：翻译后保留原版式，0.15 元/页
- PDF 转 Word：100 页内免费，超出 0.1 元/页
- 扫描件、图片版 PDF：先 OCR 再转 Word，免费
- 不用注册、不用登录，传上去直接下载

打开下面这个地址，把你自己的文件传上去试试：

https://www.ivyivy.com.cn/nist-800-61r3-zh

支持私有化部署（需按贵方模型与合规要求评估）

本译本由机器翻译生成，仅供阅读参考；专业技术判断与合规引用，请以英文原文为准。

本页为译制说明，不属于原文件内容。