Check for updates

The NIST Cybersecurity Framework 2.0

Initial Public Draft

National Institute of Standards and Technology

This publication is available free of charge from:
https://doi.org/10.6028/NIST.CSWP.29.ipd

August 8, 2023

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

Certain commercial 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.

NIST Technical Series Policies
Copyright, Use, and Licensing Statements
NIST Technical Series Publication Identifier Syntax

How to Cite this NIST Technical Series Publication:
National Institute of Standards and Technology (2023) The NIST Cybersecurity Framework 2.0. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Cybersecurity White Paper (CSWP) NIST CSWP 29 ipd. https://doi.org/10.6028/NIST.CSWP.29.ipd

Public Comment Period
August 8, 2023 – November 4, 2023

Submit Comments
cyberframework@nist.gov

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

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

Abstract

The NIST Cybersecurity Framework 2.0 provides guidance to industry, government agencies, and other organizations to reduce cybersecurity risks. It offers a taxonomy of high-level cybersecurity outcomes that can be used by any organization — regardless of its size, sector, or maturity — to better understand, assess, prioritize, and communicate its cybersecurity efforts. The Framework does not prescribe how outcomes should be achieved. Rather, it maps to resources that provide additional guidance on practices and controls that could be used to achieve those outcomes. This document explains Cybersecurity Framework 2.0 and its components and describes some of the many ways that it can be used.

Keywords

cybersecurity; Cybersecurity Framework; cybersecurity risk governance; cybersecurity risk management; cybersecurity supply chain risk management; enterprise risk management; Privacy Framework; Profiles.

Acknowledgments

This Framework is the result of a collaborative effort across industry, academia, and government in the United States and around the world. NIST acknowledges and thanks all of those who have contributed to this revised Framework. Information on the Framework development process, including workshops and drafts, can be found on the NIST Cybersecurity Framework website.

Lessons learned on the use of the Framework can always be shared with NIST through cyberframework@nist.gov.

Table of Contents

Executive Summary **1**
1. Introduction **2**
1.1. Audience 3
1.2. Document Structure 4
2. Understanding the Framework Core **4**
2.1. Functions, Categories, and Subcategories 5
2.2. Implementation Examples and Informative References 7
3. Using the Framework **8**
3.1. Creating and Using Framework Profiles to Understand, Assess, Prioritize, and Communicate 8
3.2. Assessing and Prioritizing Cybersecurity Outcomes With the Framework 12
3.3. Using Framework Tiers to Characterize Cybersecurity Risk Management Outcomes 13
3.4. Improving Communication With Internal and External Stakeholders Using the Framework 14
3.5. Managing Cybersecurity Risk in Supply Chains With the Framework 16
4. Integrating Cybersecurity Risk Management With Other Risk Management Domains Using the Framework **18**
4.1. Integrating the Cybersecurity Framework With the Privacy Framework 19
4.2. Integrating the Cybersecurity Framework With Enterprise Risk Management 20
5. Next Steps **21**
Appendix A. Templates for Profiles and Action Plans **23**
A.1. Notional Organizational Profile Template 23
A.2. Notional Action Plan Template 24
Appendix B. Framework Tier Descriptions **26**
Appendix C. Framework Core **29**

List of Tables

Table 1. Notional organizational profile template 23
Table 2. Notional action plan template 25
Table 3. Framework Tiers 26
Table 4. CSF 2.0 Core Function and Category Names and Identifiers 29
Table 5. GOVERN (GV): Establish and monitor the organization's cybersecurity risk management strategy, expectations, and policy 30
Table 6. IDENTIFY (ID): Help determine the current cybersecurity risk to the organization 33
Table 7. PROTECT (PR): Use safeguards to prevent or reduce cybersecurity risk 36
Table 8. DETECT (DE): Find and analyze possible cybersecurity attacks and compromises 40
Table 9. RESPOND (RS): Take action regarding a detected cybersecurity incident 41

Table 10. RECOVER (RC): Restore assets and operations that were impacted by a cybersecurity incident 43

List of Figures

Fig. 1. Cybersecurity Framework Core 5
Fig. 2. Framework Functions 6
Fig. 3. Cybersecurity Framework Profiles 9
Fig. 4. Steps for creating and using Cybersecurity Framework Profiles 10
Fig. 5. Cybersecurity Framework Tiers 13
Fig. 6. Using the Cybersecurity Framework to improve communication 15
Fig. 7. Integrating cybersecurity and privacy risks 19
Fig. 8. Cybersecurity Framework and Privacy Framework alignment 20

Executive Summary

Cybersecurity risks are a fundamental type of risk for all organizations to manage. Potential impacts to organizations from cybersecurity risks include higher costs, lower revenue, reputational damage, and the impairment of innovation. Cybersecurity risks also threaten individuals' privacy and access to essential services and can result in life-or-death consequences.

The NIST Cybersecurity Framework (Framework or CSF) 2.0 provides guidance for reducing cybersecurity risks by helping organizations to understand, assess, prioritize, and communicate about those risks and the actions that will reduce them.

Those actions are intended to address cybersecurity outcomes described within the CSF Core. These high-level outcomes can be understood by a broad audience, including executives, government officials, and others who may not be cybersecurity professionals. The outcomes are sector- and technology-neutral, so they provide organizations with the flexibility needed to address their unique risk, technology, and mission considerations. These outcomes can be used to focus on and implement strategic decisions that improve cybersecurity postures (or state) while also considering organizational priorities and available resources.

The CSF Core also includes examples of how each outcome can be achieved along with references to additional guidance. Together these help an organization address its cybersecurity priorities. The CSF also describes the concepts of Profiles and Tiers, which are tools to help organizations put the CSF into practice and set priorities for where they need or want to be in terms of reducing cybersecurity risks.

The CSF is a foundational resource that is adopted voluntarily and through governmental policies and mandates. Its enduring and flexible nature transcends sectors, technologies, and national borders. The updates in CSF 2.0 address changes in technologies and cybersecurity risk.

The CSF should be used in conjunction with other resources (e.g., frameworks, standards, guidelines, and leading practices) to better manage cybersecurity risks and to inform overall management of cybersecurity and other risks at an enterprise level. Supplemental guidance to this Framework will be developed and available on the NIST Cybersecurity Framework website.

1. Introduction

The NIST Cybersecurity Framework (Framework or CSF) describes essential cybersecurity outcomes that can help an organization reduce its cybersecurity risk. The voluntary Framework is not a one-size-fits-all approach to managing cybersecurity risks. Organizations will continue to have unique risks — including different threats, vulnerabilities, and risk tolerances, as well as unique mission objectives and requirements across sectors. Thus, organizations' implementations of the Framework, and approaches to managing risk, will vary.

This collection of cybersecurity outcomes creates a taxonomy and structure that can be used to understand, assess, prioritize, and communicate about cybersecurity risks.

- **Understand and Assess**:
  - Describe an organization's current or target cybersecurity posture within and across organizations, sectors, or business units.
  - Determine where an organization may have cybersecurity gaps, including with respect to existing or emerging threats or technologies, and assess progress toward addressing those gaps.
  - Align policy, business, and technological approaches to managing cybersecurity risks across an entire organization or in a more focused area, such as a portion of the organization, a specific technology, or technology suppliers.
- **Prioritize:**
  - Prioritize opportunities to improve cybersecurity risk management.
  - Identify, organize, and prioritize actions for reducing cybersecurity risks that align with the organization's mission, legal and regulatory requirements, and risk management and governance expectations.
  - Inform decisions about cybersecurity-related workforce needs and capabilities.
- **Communicate:**
  - Provide a common language for communicating with internal and external parties about cybersecurity risks, capabilities, needs, and expectations.
  - Complement an organization's risk management process by presenting a concise way for executives and others to distill the fundamental concepts of cybersecurity risk so that they express at a high level risks to be managed and how their organization uses cybersecurity standards, guidelines, and practices.

The Framework can be used by organizations whose cybersecurity programs are at different stages of maturity. An organization with an existing cybersecurity program can leverage the Framework to identify opportunities to strengthen and communicate its management of cybersecurity risk while considering its existing practices and needed changes. An organization without an existing cybersecurity program can use the Framework as a starting point and reference to establish one.

> While many cybersecurity risk management activities focus on conditions that may *prevent* mission objectives from being achieved, it is important to also note conditions that may *enable* or *accentuate* mission achievement. Actions to reduce cybersecurity risk might benefit the organization in other ways, like increasing revenue (e.g., offering excess facility space to a commercial hosting provider for hosting their own and other organizations' data centers, then moving a major financial system from the organization's in-house data center to the hosting provider to reduce cybersecurity risk).

The Framework should be used in conjunction with other resources to better manage cybersecurity risks. The outcomes are based on and are mapped to existing global standards, guidelines, and practices. Organizations can use the Framework to efficiently scale their cybersecurity programs, address the dynamic and global nature of cybersecurity risks, and adapt to technological advances and business and legal requirements. The Framework applies to all information and communications technology (ICT), including information technology (IT), the Internet of Things (IoT), and operational technology (OT) used by an organization. It also applies to all types of technology environments, including cloud, mobile, and artificial intelligence systems. The Framework is forward-looking and is intended to apply to future changes in technologies and environments.

1.1. Audience

The Framework is designed to be used by organizations of all sizes and sectors, including industry, government, academia, and non-profit organizations. The Framework's taxonomy and referenced standards, guidelines, and practices are not country-specific, and previous versions of the Framework have been successfully leveraged by many governments and other organizations outside of the United States.

The primary audience for the Framework consists of those responsible for developing and leading a cybersecurity program. The Framework can also be used by others involved in managing risk — including executives, boards of directors, acquisition professionals, technology professionals, risk managers, lawyers, human resources specialists, and cybersecurity and risk management auditors — to guide their cybersecurity-related decisions.

Additionally, the Framework can be useful to policymakers (such as associations, professional organizations, and regulators) to set and communicate priorities for cybersecurity risk management.

Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*, issued in February 2013, directed NIST "to lead the development of a framework to reduce cyber risks to critical infrastructure." The Cybersecurity Enhancement Act of 2014 directed NIST to "on an ongoing basis, facilitate and support the development of a voluntary, consensus-based, industry-led set of standards, guidelines, best practices, methodologies, procedures, and processes to cost-effectively reduce cyber risks to critical infrastructure." NIST published Framework Version 1.0 in 2014 and updated the Framework to 1.1 in 2018.

Since then, Congress has explicitly directed NIST to consider small business concerns (in the NIST Small Business Cybersecurity Act) and the needs of institutions of higher education (in the CHIPS and Science Act) in the Framework. While Version 2.0 can be used by any organization, NIST will continue to build additional resources to help implement the Framework, including an updated NIST Special Publication (SP) 1271, *Getting Started with the NIST Cybersecurity Framework: A Quick Start Guide*. All resources will be publicly available on the NIST Cybersecurity Framework website.

1.2. Document Structure

This document contains the following sections and appendices:

- Section 2 explains the basics of the Framework Core: Functions, Categories, Subcategories, Implementation Examples, and Informative References.
- Section 3 provides an overview of common uses for the Framework, including through Current and Target Profiles, as well as guidance on using the Framework to understand, assess, prioritize, and communicate cybersecurity efforts and cybersecurity supply chain risk management efforts.
- Section 4 discusses using the Framework to help integrate cybersecurity risk management with other types of risk management.
- Section 5 briefly outlines next steps for readers who want to use the Framework.
- Appendix A offers notional templates for Framework Profiles and action plans.
- Appendix B describes the Framework Tiers.
- Appendix C provides the Framework Core.

2. Understanding the Framework Core

The Framework Core provides a set of cybersecurity *outcomes* (arranged by Function, Category, and Subcategory), examples of how those outcomes might be achieved (Implementation Examples), and references to additional guidance on how to achieve those outcomes (Informative References), as depicted in Fig. 1. The cybersecurity outcome statements in the Core reflect activities across sectors and are technology-neutral. They are not a checklist of actions to perform; the specific actions taken to achieve a cybersecurity outcome will vary by organization and use case, as will the individual responsible for those actions. Additionally, the