NIST CSF 2.0: What has changed?

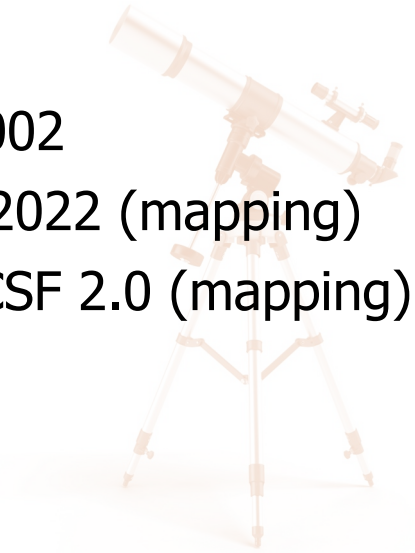
by Andrey Prozorov, CISM, CIPP/E, CDPSE, LA 27001

www.patreon.com/AndreyProzorov

2.0, 02.03.2024

Agenda

1. Journey To CSF 2.0
2. New Title
3. New Scope
4. What is the Framework?
5. Desired outcomes
6. Components of the Framework
7. Purpose
8. The new function (Govern) and changes in Categories and Subcategories
9. Framework Profiles
10. CSF Tiers: New criteria
11. Steps for Creating and Using Profiles
12. Other publications
13. NIST CSF 2.0 Mindmap
14. Significant Updates
15. NIST CSF 2.0 vs ISO 27001:2002
16. NIST CSF 2.0 and ISO 27001:2022 (mapping)
17. EU NIS 2 Directive and NIST CSF 2.0 (mapping)



BIG NEWS | The NIST CSF 2.0 has been released, along with other supplementary resources!

CSF 2.0

For industry, government, and organizations to reduce cybersecurity risks

Read the Document

Quick Start Guides

For users with specific common goals

View the Quick Start Guides

CSF 2.0 Profiles

Templates and useful resources for creating and using both CSF profiles

See the Profiles

Informative References (Mappings)

See how NIST's resources overlap and share themes

See the Mappings

www.nist.gov/cyberframework

Why is NIST deciding to update the Framework now toward CSF 2.0?

The NIST Cybersecurity Framework was intended to be a living document that is refined, improved, and evolves over time.

These updates help the Framework keep pace with technology and threat trends, integrate lessons learned, and move best practice to common practice.

NIST initially produced the Framework in 2014 and updated it in April 2018 with CSF 1.1. Based on stakeholder feedback, in order to reflect the ever-evolving cybersecurity landscape and to help organizations more easily and effectively manage cybersecurity risk, NIST is working on a new, more significant update to the Framework: CSF 2.0.

www.nist.gov/cyberframework/updating-nist-cybersecurity-framework-journey-csf-20


August 2022
Workshop #1
February 2023
Workshop #2
February 2023
Working Sessions
September 19-20, 2023
Workshop #3
2022
COMMUNITY ENGAGEMENT
2024
February 2022
NIST Cybersecurity RFI
June 2022
RFI Analysis
September 2022
Workshop Analysis
January 2023
Concept Paper
April 2023
Core Draft
August 2023
Draft 2.0
February 2024
CSF 2.0
April 2022
Comments Received
March 2023
Comments Received
November 2023
Comments Received
November 2023
Comments Received

The NIST Cybersecurity Framework (CSF) 2.0

National Institute of Standards and Technology
This publication is available free of charge from: https://doi.org/10.6028/NIST.CSWP.29
February 26, 2024

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

Table of Contents

List of Figures

https://csrc.nist.gov/pubs/cswp/29/the-nist-cybersecurity-framework-csf-20/final

New Title

CSF 1.1	CSF 2.0
Framework for Improving Critical Infrastructure Cybersecurity	The NIST Cybersecurity Framework 2.0

New Scope (wider)

NIST CSF 2.0 is designed to be used by **organizations of all sizes and sectors**, including industry, government, academia, and nonprofit organizations, **regardless of the maturity level of their cybersecurity programs**.

The CSF is a foundational resource that may be adopted **voluntarily** and **through governmental policies and mandates**.

The CSF's taxonomy and referenced standards, guidelines, and practices are **not country-specific**, and previous versions of the CSF have been leveraged successfully by many governments and other organizations both inside and outside of the United States.

What is the Framework?

The Cybersecurity Framework (CSF) 2.0 is designed to help organizations of all sizes and sectors — including industry, government, academia, and nonprofit — **to manage and reduce their cybersecurity risks**.

It is useful regardless of the maturity level and technical sophistication of an organization's cybersecurity programs. Nevertheless, the CSF does not embrace a one-size-fits-all approach. Each organization has both common and unique risks, as well as varying risk appetites and tolerances, specific missions, and objectives to achieve those missions. By necessity, the way organizations implement the CSF will vary.

Current revision: 2.0, February 26, 2024

Desired outcomes

Ideally, the CSF will be used to address cybersecurity risks alongside other risks of the enterprise, including those that are financial, privacy, supply chain, reputational, technological, or physical in nature.

The CSF describes desired outcomes that are intended to be understood by a broad audience, including executives, managers, and practitioners, regardless of their cybersecurity expertise. Because these outcomes are sector-, country-, and technology-neutral, they provide an organization with the flexibility needed to address their unique risks, technologies, and mission considerations. **Outcomes are mapped directly to a list of potential security controls for immediate consideration to mitigate cybersecurity risks**.

Components of the Framework (CSF 2.0)

NIST CSF 2.0 includes the following components:

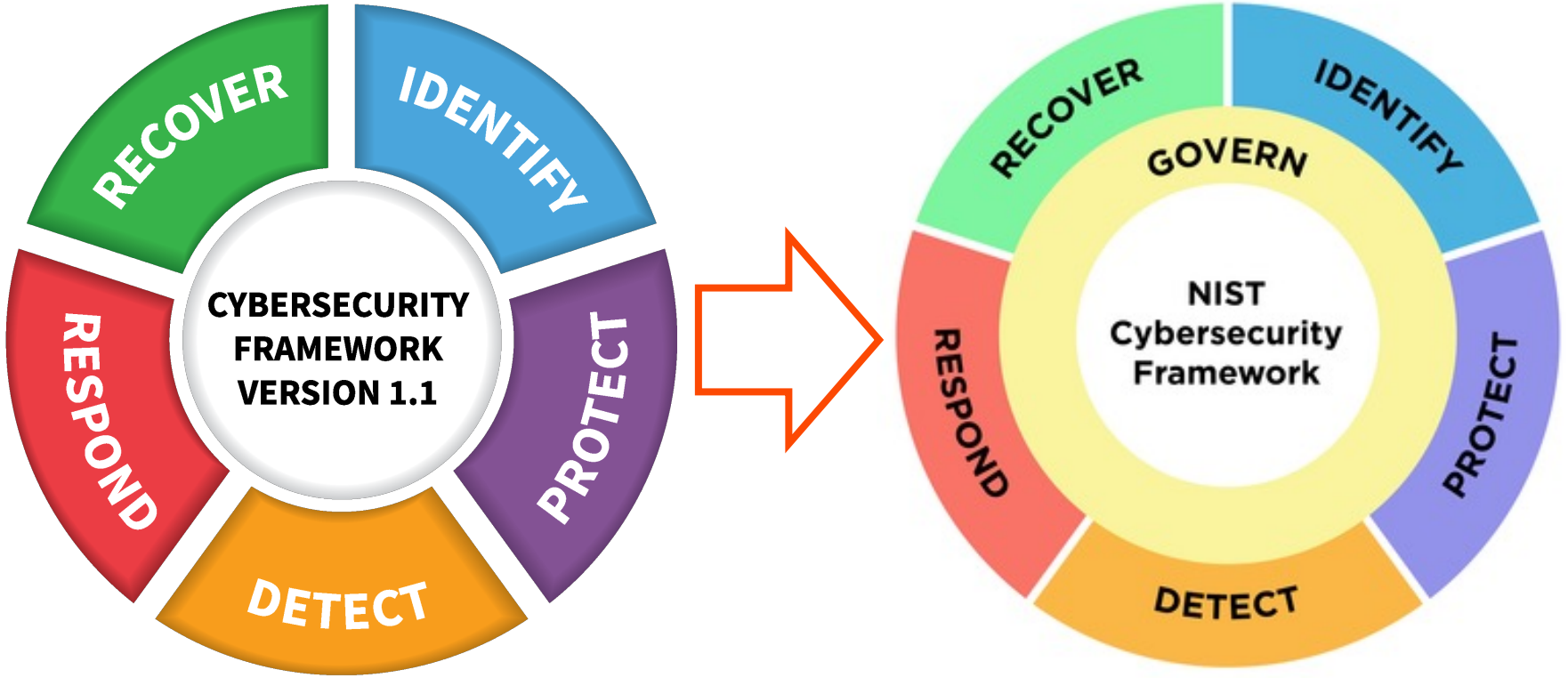
- **CSF Core**, the nucleus of the CSF, which is a taxonomy of high-level cybersecurity outcomes that can help any organization manage its cybersecurity risks. The CSF Core components are a hierarchy of Functions, Categories, and Subcategories that detail each outcome.
- **CSF Organizational Profiles**, which are a mechanism for describing an organization's current and/or target cybersecurity posture in terms of the CSF Core's outcomes.
- **CSF Tiers**, which can be applied to CSF Organizational Profiles to characterize the rigor of an organization's cybersecurity risk governance and management practices. Tiers can also provide context for how an organization views cybersecurity risks and the processes in place to manage those risks.

Purpose (CSF 2.0)

An organization can use the CSF Core, Profiles, and Tiers with the supplementary resources to understand, assess, prioritize, and communicate cybersecurity risks.

Understand and Assess	Prioritize	Communicate
Describe the current or target cybersecurity posture of part or all of an organization, determine gaps, and assess progress toward addressing those gaps.	Identify, organize, and prioritize actions for managing cybersecurity risks that align with the organization's mission, legal and regulatory requirements, and risk management and governance expectations.	Provide a common language for communicating inside and outside the organization about cybersecurity risks, capabilities, needs, and expectations.

The new function (Govern) and changes in Categories and Subcategories



CSF 1.1	CSF 2.0
-	**Govern (GV)**: The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored.
Identify (ID): Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.	**Identify (ID)**: The organization's current cybersecurity risks are understood.
Protect (PT): Develop and implement appropriate safeguards to ensure delivery of critical services.	**Protect (PT)**: Safeguards to manage the organization's cybersecurity risks are used.
Detect (DE): Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.	**Detect (DE)**: Possible cybersecurity attacks and compromises are found and analyzed.
Respond (RS): Develop and implement appropriate activities to take action regarding a detected cybersecurity incident.	**Respond (RS)**: Actions regarding a detected cybersecurity incident are taken.
Recover (RC): Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.	**Recover (RC)**: Assets and operations affected by a cybersecurity incident are restored.

CSF 1.1

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Identity Management and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

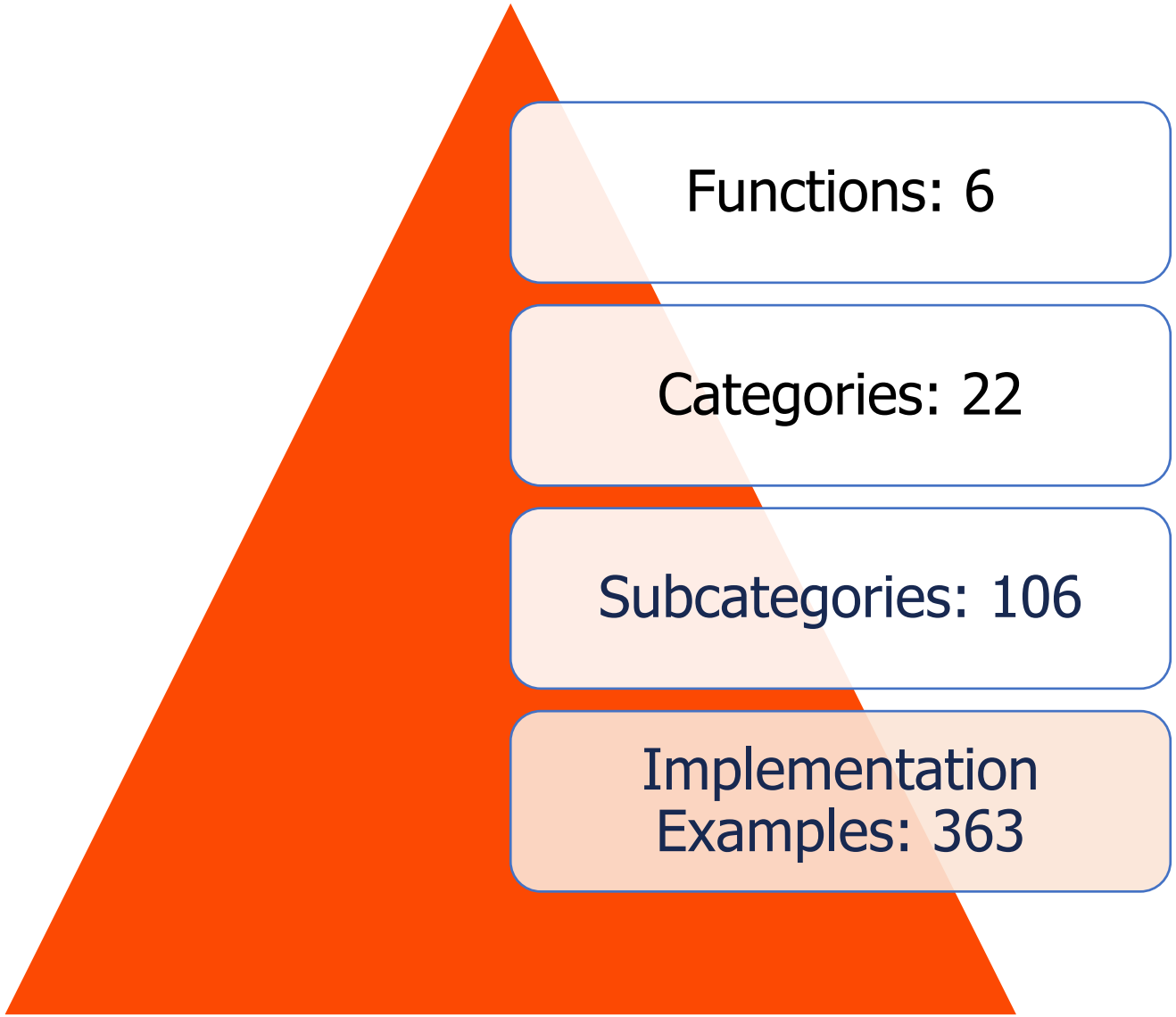
CSF 2.0

Function	Category	Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Roles, Responsibilities, and Authorities	GV.RR
	Policy	GV.PO
	Oversight	GV.OV
	Cybersecurity Supply Chain Risk Management	GV.SC
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication, and Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

CSF 1.1	CSF 2.0
5 Functions	6 Functions
23 Categories	22 Categories
108 Subcategories	106 Subcategories
-	363 Implementation Examples

Function	Category	Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Roles, Responsibilities, and Authorities	GV.RR
	Policy	GV.PO
	Oversight	GV.OV
	Cybersecurity Supply Chain Risk Management	GV.SC
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication, and Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

CSF 2.0 Pyramid



CSF Core: A taxonomy of high-level cybersecurity outcomes that can help any organization manage its cybersecurity risks. Its components are a hierarchy of Functions, Categories, and Subcategories that detail each outcome

- **CSF Function**: The highest level of organization for cybersecurity outcomes. There are six CSF Functions: Govern, Identify, Protect, Detect, Respond, and Recover
- **CSF Category**: A group of related cybersecurity outcomes that collectively comprise a CSF Function
- **CSF Subcategory**: A group of more specific outcomes of technical and management cybersecurity activities that comprise a CSF Category
- **CSF Implementation Example**: A concise, action-oriented, notional illustration of a way to help achieve a CSF Core outcome

Framework Profiles

A CSF Organizational Profile describes an organization's current and/or target cybersecurity posture in terms of the Core's outcomes.

Every Organizational Profile includes one or both of the following:

- A **Current Profile** specifies the Core outcomes that an organization is currently achieving (or attempting to achieve) and characterizes how or to what extent each outcome is being achieved.
- A **Target Profile** specifies the desired outcomes that an organization has selected and prioritized for achieving its cybersecurity risk management objectives. A Target Profile considers anticipated changes to the organization's cybersecurity posture, such as new requirements, new technology adoption, and threat intelligence trends.

CSF Outcomes		Current Profile			Target Profile	
Identifier	**Description**	**Practices**	**Status**	**Rating**	**Priority**	**Goals**
The identifiers and descriptions from the CSF Core – Functions, Categories, Subcategories. You can also add your own outcomes to address your organization's unique risks and requirements.		Policies, processes, procedures and other activities related to an outcome. May include artifacts that contain evidence of achieving an outcome.	The current state or condition of an outcome, such as whether it is being achieved and to what degree.	An assessment or evaluation of current practices using scales such as: • high/medium/low • 1-5 • 0-100%, • red/yellow/green	The relative importance of an outcome using scales such as: • Low/Medium/High • 1/2/3/4/5 • rankings (1, 2, 3…)	Such as: • Policies, Processes, and Procedures • Roles and Responsibilities Selected from: • Informative References - standards, guidance, and best practices

Steps for Creating and Using Profiles

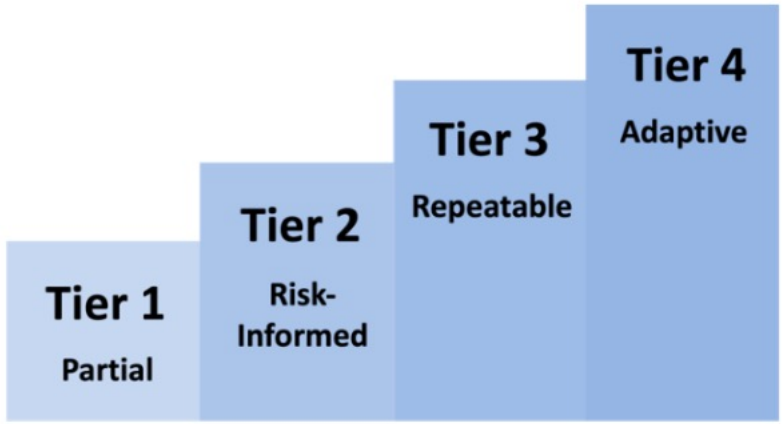
Replaced 3.2 Establishing or Improving a Cybersecurity Program (CSF 1.1):
Step 1: Prioritize and Scope, Step 2: Orient, Step 3: Create a Current Profile,
Step 4: Conduct a Risk Assessment, Step 5: Create a Target Profile,
Step 6: Determine, Analyze, and Prioritize Gaps, Step 7: Implement Action Plan

CSF Tiers: New criteria

CSF Tier: A characterization of the rigor of an organization's cybersecurity risk governance and management practices.

An organization can choose to use the Tiers to inform its Current and Target Profiles.

New criteria for Tiers were presented in NIST CSF 2.0.

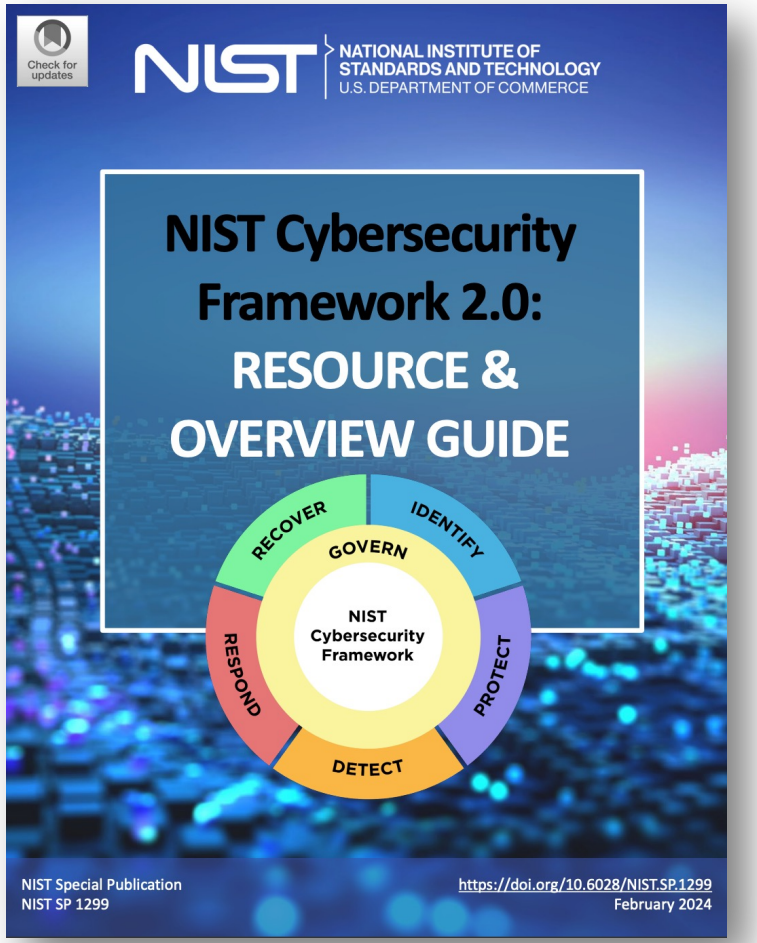


CSF 1.1	CSF 2.0
• Risk Management Process • Integrated Risk Management Program • External Participation	• Cybersecurity Risk Governance • Cybersecurity Risk Management • ~~Third-Party Cybersecurity Risks~~

Tier	Cybersecurity Risk Governance	Cybersecurity Risk Management
Tier 1: Partial	Application of the organizational cybersecurity risk strategy is managed in an ad hoc manner. Prioritization is ad hoc and not formally based on objectives or threat environment.	There is limited awareness of cybersecurity risks at the organizational level. The organization implements cybersecurity risk management on an irregular, case-by-case basis. The organization may not have processes that enable cybersecurity information to be shared within the organization. The organization is generally unaware of the cybersecurity risks associated with its suppliers and the products and services it acquires and uses.
Tier 2: Risk Informed	Risk management practices are approved by management but may not be established as organization-wide policy. The prioritization of cybersecurity activities and protection needs is directly informed by organizational risk objectives, the threat environment, or business/mission requirements.	There is an awareness of cybersecurity risks at the organizational level, but an organization-wide approach to managing cybersecurity risks has not been established. Consideration of cybersecurity in organizational objectives and programs may occur at some but not all levels of the organization. Cyber risk assessment of organizational and external assets occurs but is not typically repeatable or reoccurring. Cybersecurity information is shared within the organization on an informal basis. The organization is aware of the cybersecurity risks associated with its suppliers and the products and services it acquires and uses, but it does not act consistently or formally in response to those risks.
Tier 3: Repeatable	The organization's risk management practices are formally approved and expressed as policy. Risk-informed policies, processes, and procedures are defined, implemented as intended, and reviewed. Organizational cybersecurity practices are regularly updated based on the application of risk management processes to changes in business/mission requirements, threats, and technological landscape.	There is an organization-wide approach to managing cybersecurity risks. Cybersecurity information is routinely shared throughout the organization. Consistent methods are in place to respond effectively to changes in risk. Personnel possess the knowledge and skills to perform their appointed roles and responsibilities. The organization consistently and accurately monitors the cybersecurity risks of assets. Senior cybersecurity and non-cybersecurity executives communicate regularly regarding cybersecurity risks. Executives ensure that cybersecurity is considered through all lines of operation in the organization.

Tier	Cybersecurity Risk Governance	Cybersecurity Risk Management
		The organization risk strategy is informed by the cybersecurity risks associated with its suppliers and the products and services it acquires and uses. Personnel formally act upon those risks through mechanisms such as written agreements to communicate baseline requirements, governance structures (e.g., risk councils), and policy implementation and monitoring. These actions are implemented consistently and as intended and are continuously monitored and reviewed.
Tier 4: Adaptive	There is an organization-wide approach to managing cybersecurity risks that uses risk-informed policies, processes, and procedures to address potential cybersecurity events. The relationship between cybersecurity risks and organizational objectives is clearly understood and considered when making decisions. Executives monitor cybersecurity risks in the same context as financial and other organizational risks. The organizational budget is based on an understanding of the current and predicted risk environment and risk tolerance. Business units implement executive vision and analyze system-level risks in the context of the organizational risk tolerances. Cybersecurity risk management is part of the organizational culture. It evolves from an awareness of previous activities and continuous awareness of activities on organizational systems and networks. The organization can quickly and efficiently account for changes to business/mission objectives in how risk is approached and communicated.	The organization adapts its cybersecurity practices based on previous and current cybersecurity activities, including lessons learned and predictive indicators. Through a process of continuous improvement that incorporates advanced cybersecurity technologies and practices, the organization actively adapts to a changing technological landscape and responds in a timely and effective manner to evolving, sophisticated threats. The organization uses real-time or near real-time information to understand and consistently act upon the cybersecurity risks associated with its suppliers and the products and services it acquires and uses. Cybersecurity information is constantly shared throughout the organization and with authorized third parties.

Other publications: Quick Start Guides



CSF 2.0 Organizational Profiles, Tiers, CSF 2.0 Community Profiles, C-SCRM Small Business, Enterprise Risk Management…

CSF Quick Start Guide: A supplementary resource that gives brief, actionable guidance on specific CSF-related topics.

Other publications: CSF 2.0 Informative References

CSF 2.0 Informative References

Informative References help inform how an organization may achieve the Core's outcomes. Given the diversity of use cases this page allows the user to choose how to best consume Informative References.

Download CSF 2.0 Informative Reference in the Core

Directly download all the Informative References for CSF 2.0

For users that want all informative references.

Download (xlsx)

Select Informative References to be included with the Core

For users that want to select specific informative references.

Browse

CSF 2.0 Implementation Examples

Implementation Examples offer potential ways to achieve each outcome

Download (xlsx)

Download (pdf)

Informative Reference Catalog

Browse and download specific informative references

Catalog

Compare Informative References

Generate, view and download Comparison Reports between CSF 2.0 Informative References

Comparison Reports

Other publications: Implementation Examples

(used as potential IS controls)

NIST CSF 2.0 Implementation Examples

February 26, 2024

Category	Subcategory	Implementation Examples
Organizational Context (GV.OC): The circumstances — mission, stakeholder expectations, dependencies, and legal, regulatory, and contractual requirements — surrounding the organization's cybersecurity risk management decisions are understood		
	GV.OC-01: The organizational mission is understood and informs cybersecurity risk management	**Ex1:** Share the organization's mission (e.g., through vision and mission statements, marketing, and service strategies) to provide a basis for identifying risks that may impede that mission
	GV.OC-02: Internal and external stakeholders are understood, and their needs and expectations regarding cybersecurity risk management are understood and considered	**Ex1:** Identify relevant internal stakeholders and their cybersecurity-related expectations (e.g., performance and risk expectations of officers, directors, and advisors; cultural expectations of employees) **Ex2:** Identify relevant external stakeholders and their cybersecurity-related expectations (e.g., privacy expectations of customers, business expectations of partnerships, compliance expectations of regulators, ethics expectations of society)
	GV.OC-03: Legal, regulatory, and contractual requirements regarding cybersecurity — including privacy and civil liberties obligations — are understood and managed	**Ex1:** Determine a process to track and manage legal and regulatory requirements regarding protection of individuals' information (e.g., Health Insurance Portability and Accountability Act, California Consumer Privacy Act, General Data Protection Regulation) **Ex2:** Determine a process to track and manage contractual requirements for cybersecurity management of supplier, customer, and partner information **Ex3:** Align the organization's cybersecurity strategy with legal, regulatory, and contractual requirements
	GV.OC-04: Critical objectives, capabilities, and services that	**Ex1:** Establish criteria for determining the criticality of the organization's capabilities and services as viewed by internal and external stakeholders

CSF Implementation Example: A concise, action-oriented, notional illustration of a way to help achieve a CSF Core outcome.

The NIST Cybersecurity Framework (CSF) 2.0

26.02.2024 www.patreon.com/AndreyProzorov

Intro

- ***The NIST Cybersecurity Framework (CSF) 2.0*** — 32 pages
- NIST CSF 2.0 is designed to help organizations of all sizes and sectors to manage and reduce their cybersecurity risks — regardless of the maturity level of their cybersecurity programs
- NIST CSF Website — www.nist.gov/cyberframework
- Revisions
  - Current — 2.0, February 2024
  - Previous — 1.1, April 2018
- **CSF 2.0 Framework**
  - **1. CSF Core** — A taxonomy of high-level cybersecurity outcomes that can help any organization manage its cybersecurity risks; Its components are a hierarchy of Functions, Categories, and Subcategories that detail each outcome
  - **2. CSF Organizational Profiles** — A mechanism for describing an organization's current and/or target cybersecurity posture in terms of the CSF Core's outcomes
  - **3. CSF Tiers** — A characterization of the rigor of an organization's cybersecurity risk governance and management practices
- Additional resources
  - FAQ
  - Informative References — References to additional guidance on how to achieve those outcomes
  - Cybersecurity and Privacy Reference Tool (CPRT)
  - Implementation Examples — Examples of how those outcomes might be achieved
  - Community Profiles and Organizational Profile Templates
  - Quick-Start Guides
    - Resources and Overview Guide
    - Quick-Start Guide for Cybersecurity Supply Chain Risk Management (C-SCRM)
    - Small Business Quick-Start Guide
    - Quick-Start Guide for Creating and Using Organizational Profiles
    - A Guide to Creating Community Profiles
    - Quick-Start Guide for Using the CSF Tiers
    - Enterprise Risk Management Quick-Start Guide

Purpose

- **Understand and Assess** — Describe the current or target cybersecurity posture of part or all of an organization, determine gaps, and assess progress toward addressing those gaps
- **Prioritize** — Identify, organize, and prioritize actions for managing cybersecurity risks that align with the organization's mission, legal and regulatory requirements, and risk management and governance expectations
- **Communicate** — Provide a common language for communicating inside and outside the organization about cybersecurity risks, capabilities, needs, and expectations

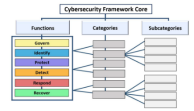
Significant Updates (1.1->2.0)

- New Title and Wider scope
- New Function, Govern
- Changes in the Categories and Subcategories
- Increased guidance on CSF implementation
  - Profiles
  - Examples
  - Quick-Start Guides
- Emphasized cybersecurity supply chain risk management (C-SCRM)
- Clarified understanding of cybersecurity measurement and assessment
- Alignment (and integration) with other Frameworks and standards

Glossary

- ***CSF Function*** — The highest level of organization for cybersecurity outcomes
- ***CSF Category*** — A group of related cybersecurity outcomes that collectively comprise a CSF Function
- ***CSF Subcategory*** — A group of more specific outcomes of technical and management cybersecurity activities that comprise a CSF Category
- ***CSF Implementation Example*** — A concise, action-oriented, notional illustration of a way to help achieve a CSF Core outcome
- ***CSF Informative Reference*** — A mapping that indicates a relationship between a CSF Core outcome and an existing standard, guideline, regulation, or other content

1. CSF Core



GOVERN (GV)

The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored

- GV.OC Organizational Context
- GV.RM Risk Management Strategy
- GV.RR Roles, Responsibilities, and Authorities
- GV.PO Policy
- GV.OV Oversight
- GV.SC Cybersecurity Supply Chain Risk Management

IDENTIFY (ID)

The organization's current cybersecurity risks are understood

- ID.AM Asset Management
- ID.RA Risk Assessment
- ID.IM Improvement

PROTECT (PR)

Safeguards to manage the organization's cybersecurity risks are used

- PR.AA Identity Management, Authentication, and Access Control
- PR.AT Awareness and Training
- PR.DS Data Security
- PR.PS Platform Security
- PR.IR Technology Infrastructure Resilience

DETECT (DE)

Possible cybersecurity attacks and compromises are found and analyzed

- DE.CM Continuous Monitoring
- DE.AE Adverse Event Analysis

RESPOND (RS)

Actions regarding a detected cybersecurity incident are taken

- RS.MA Incident Management
- RS.AN Incident Analysis
- RS.CO Incident Response Reporting and Communication
- RS.MI Incident Mitigation

RECOVER (RC)

Assets and operations affected by a cybersecurity incident are restored

- RC.RP Incident Recovery Plan Execution
- RC.CO Incident Recovery Communication

2. CSF Profiles

- Two types
  - ***Current Profile*** — Specifies the Core outcomes that an organization is currently achieving (or attempting to achieve) and characterizes how or to what extent each outcome is being achieved
  - ***Target Profile*** — Specifies the desired outcomes that an organization has selected and prioritized for achieving its cybersecurity risk management objectives
- Steps for creating and using profiles
  1. Scope the Organizational Profile
  2. Gather needed information
  3. Create the Organizational Profile
  4. Analyze gaps and create an action plan
  5. Implement action plan and update Profile
  - Repeat...

3. CSF Tiers

- An organization can choose to use the Tiers to inform its Current and Target Profiles
- Tiers
  - ***Tier 1: Partial***
  - ***Tier 2: Risk Informed***
  - ***Tier 3: Repeatable***
  - ***Tier 4: Adaptive***
- Criteria
  - Cybersecurity Risk Governance
  - Cybersecurity Risk Management

Significant Updates

1. Recognition of the broad use of the Framework (New Title and wider Scope)
2. New Function, Govern, and changes in the Categories and Subcategories
3. Increased guidance on CSF implementation (Profiles and Examples)
4. Emphasized cybersecurity supply chain risk management (C-SCRM) (see also NIST SP 800-161r1)
5. Clarified understanding of cybersecurity measurement and assessment (see also NIST SP 800-55)
6. Alignment (and integration) with other Frameworks and standards. (see also Cybersecurity and Privacy Reference Tool (CPRT) - https://csrc.nist.gov/Projects/cprt)

NIST CSF 2.0 vs ISO 27001:2002

TLP:CLEAR

ISO 27001:2022 vs NIST CSF 2.0

1.0, 28.0.2024

	ISO/IEC 27001:2022	NIST CSF 2.0
Type	International standard	Guide
Name	Information security, cybersecurity and privacy protection. Information security management systems. Requirements	NIST Cybersecurity Framework (CSF)
Website	www.iso.org/standard/27001	www.nist.gov/cyberframework
Description	ISO/IEC 27001 is the world's best-known standard for **information security management systems (ISMS)**. It defines requirements an ISMS must meet. The ISO/IEC 27001 standard provides companies of any size and from all sectors of activity with guidance for establishing, implementing, maintaining and continually improving an information security management system. Conformity with ISO/IEC 27001 means that an organization or business has put in place a system to manage risks related to the security of data owned or handled by the company, and that this system respects all the best practices and principles enshrined in this International Standard.	The NIST Cybersecurity Framework (CSF) 2.0 provides guidance to industry, government agencies, and other organizations **to manage 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 CSF does not prescribe how outcomes should be achieved. Rather, it links to online resources that provide additional guidance on practices and controls that could be used to achieve those outcomes. This document describes CSF 2.0, its components, and some of the many ways that it can be used.
Current version	October 2022 + Amd 1:2024	2.0, February 2024
The first versions	BS 7799-1 (->27002): 1995 BS 7799-2 (->27001): 1999	1.0: February 2014 1.1: April 2018
Pages	19 (26)	27 (32)
Price	CHF 129 (150$)	Free
Framework	**Requirements** (clauses): 4. Context of the organization 5. Leadership 6. Planning 7. Support 8. Operation 9. Performance evaluation 10. Improvement **Annex A. IS Controls:** • 5. Organizational controls • 6. People controls • 7. Physical controls • 8. Technological	**CSF Core**: A taxonomy of high-level cybersecurity outcomes that can help any organization manage its cybersecurity risks. Its components are a hierarchy of Functions, Categories, and Subcategories that detail each outcome. There are six CSF Functions: Govern, Identify, Protect, Detect, Respond, and Recover. **CSF Organizational Profiles**: A mechanism for describing an organization's current and/or target cybersecurity posture in terms of the CSF Core's outcomes. **CSF Tiers**: A characterization of the rigor of an organization's cybersecurity risk governance and management practices.

TLP:CLEAR

ISO 27001:2022 vs NIST CSF 2.0

1.0, 28.0.2024

	ISO/IEC 27001:2022	NIST CSF 2.0
ISMS	Information security management systems	Cybersecurity program
IS Controls	4 Categories, 93 controls Detailed description and additional attributes are in ISO 27002	22 Categories, 106 Subcategories and 363 Implementation Examples (separate publication)
Profiles	Not used, but the Statement of Applicability (SoA) with specified statuses of controls can be used for this purpose	Yes • CSF 2.0 Organizational Profiles • CSF 2.0 Community Profiles
TIERs	Not mentioned, but the Maturity levels can be used (separate methodology)	There are four Tiers: • Partial (Tier 1) • Risk Informed (Tier 2) • Repeatable (Tier 3) • Adaptive (Tier 4)
Certification	Yes, formal audit and certification	No NIST does not offer certifications or endorsements of CSF-related products, implementations, or services, and there are no plans to develop a conformity assessment program.
Related standards and other publications	ISO 27k family, especially: • ISO 27000 (ISMS Overview and vocabulary) • ISO 27002 (IS Controls) • ISO 27003 (ISMS Guidance) Privacy: • ISO 27701 (PIMS): Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management. Requirements and guidelines Risk Management: • ISO 27005: Guidance on managing information security risks Supply chain security, ISO 27036 (set): • Part 1: Overview and concepts • Part 2: Requirements • Part 3: Guidelines for hardware, software, and services supply chain security • Part 4: Guidelines for security of cloud services	CSF Publications: • NIST's CSF 2.0 Quick Start Guides • NIST CSF 2.0 Informative References • FAQ Other NIST publications, especially: • NIST SP 800-53, Security and Privacy Controls for Information Systems and Organizations Privacy: • NIST Privacy Framework • NIST Privacy Risk Assessment Methodology (PRAM) Risk Management: • NIST SP 800-37 Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy • NIST SP 800-30 Guide for Conducting Risk Assessments • NIST Risk Management Framework Supply chain security: • NIST SP 800-161 Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations

TLP:CLEAR

Andrey Prozorov, CISM, CIPP/E, CDPSE, LA 27001
www.patreon.com/AndreyProzorov || www.linkedin.com/in/AndreyProzorov

TLP:GREEN

NIST CSF 2.0 and ISO 27001:2022 (mapping)

1.0, 01.03.2024

NIST CSF 2.0 NIST Cybersecurity Framework 2.0
https://www.nist.gov/cyberframework

ISO 27001 ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements
https://www.iso.org/standard/27001

CSF Functions and Categories

1. Govern (GV): The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored	• Organizational Context (GV.OC) • Risk Management Strategy (GV.RM) • Roles, Responsibilities, and Authorities (GV.RR) • Policy (GV.PO) • Oversight (GV.OV) • Cybersecurity Supply Chain Risk Management (GV.SC)
2. Identify (ID): The organization's current cybersecurity risks are understood	• Asset Management (ID.AM) • Risk Assessment (ID.RA) • Improvement (ID.IM)
3. Protect (PR): Safeguards to manage the organization's cybersecurity risks are used	• Identity Management, Authentication, and Access Control (PR.AA) • Awareness and Training (PR.AT) • Data Security (PR.DS) • Platform Security (PR.PS) • Technology Infrastructure Resilience (PR.IR)
4. Detect (DE): Possible cybersecurity attacks and compromises are found and analyzed	• Continuous Monitoring (DE.CM) • Adverse Event Analysis (DE.AE)
5. Respond (RS): Actions regarding a detected cybersecurity incident are taken	• Incident Management (RS.MA) • Incident Analysis (RS.AN) • Incident Response Reporting and Communication (RS.CO) • Incident Mitigation (RS.MI)
6. Recover (RC): Assets and operations affected by a cybersecurity incident are restored	• Incident Recovery Plan Execution (RC.RP) • Incident Recovery Communication (RC.CO)

CSF Core: A taxonomy of high-level cybersecurity outcomes that can help any organization manage its cybersecurity risks. Its components are a hierarchy of Functions, Categories, and Subcategories that detail each outcome.

CSF Function: The highest level of organization for cybersecurity outcomes. There are six CSF Functions: Govern, Identify, Protect, Detect, Respond, and Recover.

CSF Category: A group of related cybersecurity outcomes that collectively comprise a CSF Function.

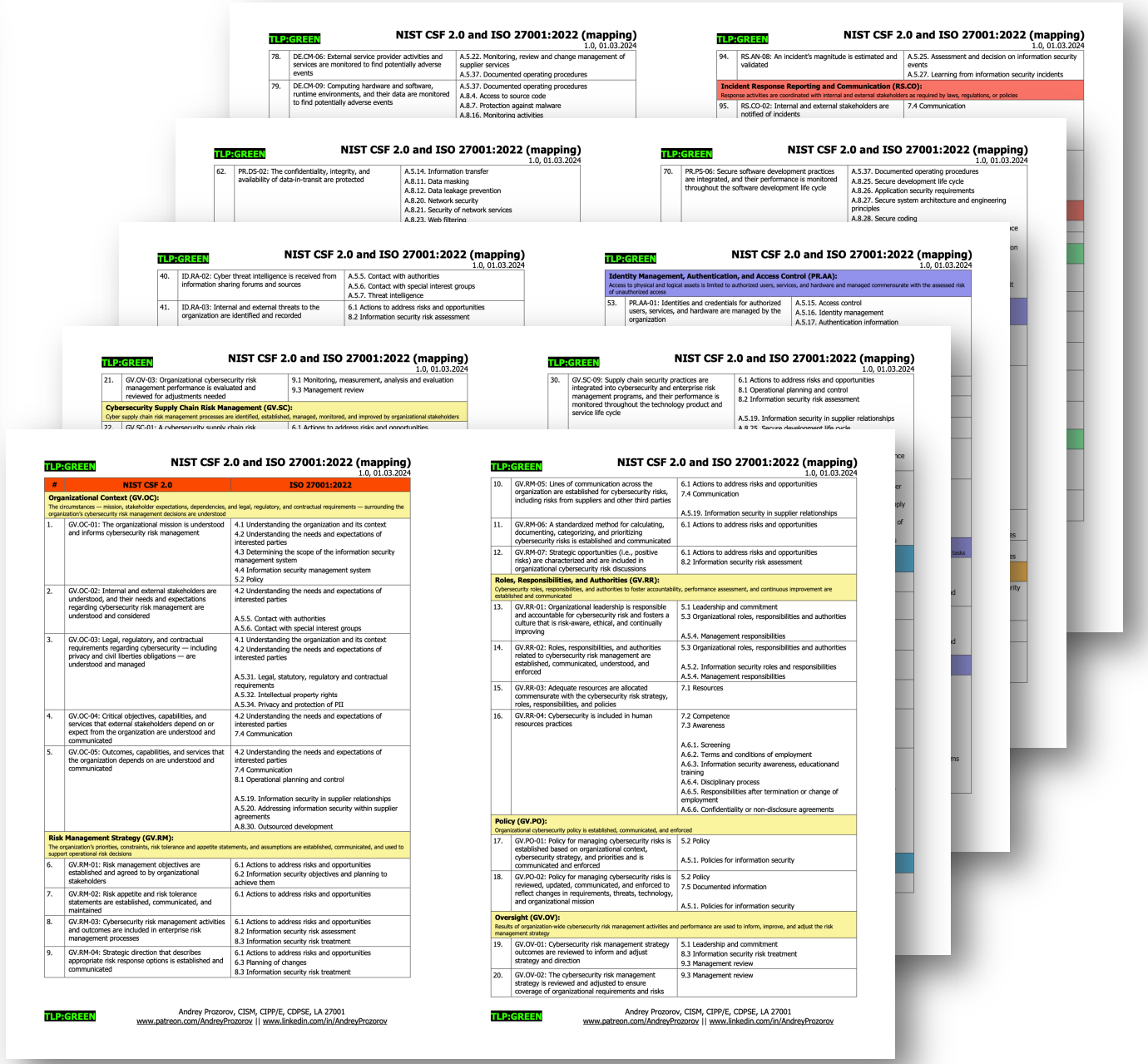
CSF Subcategory: A group of more specific outcomes of technical and management cybersecurity activities that comprise a CSF Category.

See also:

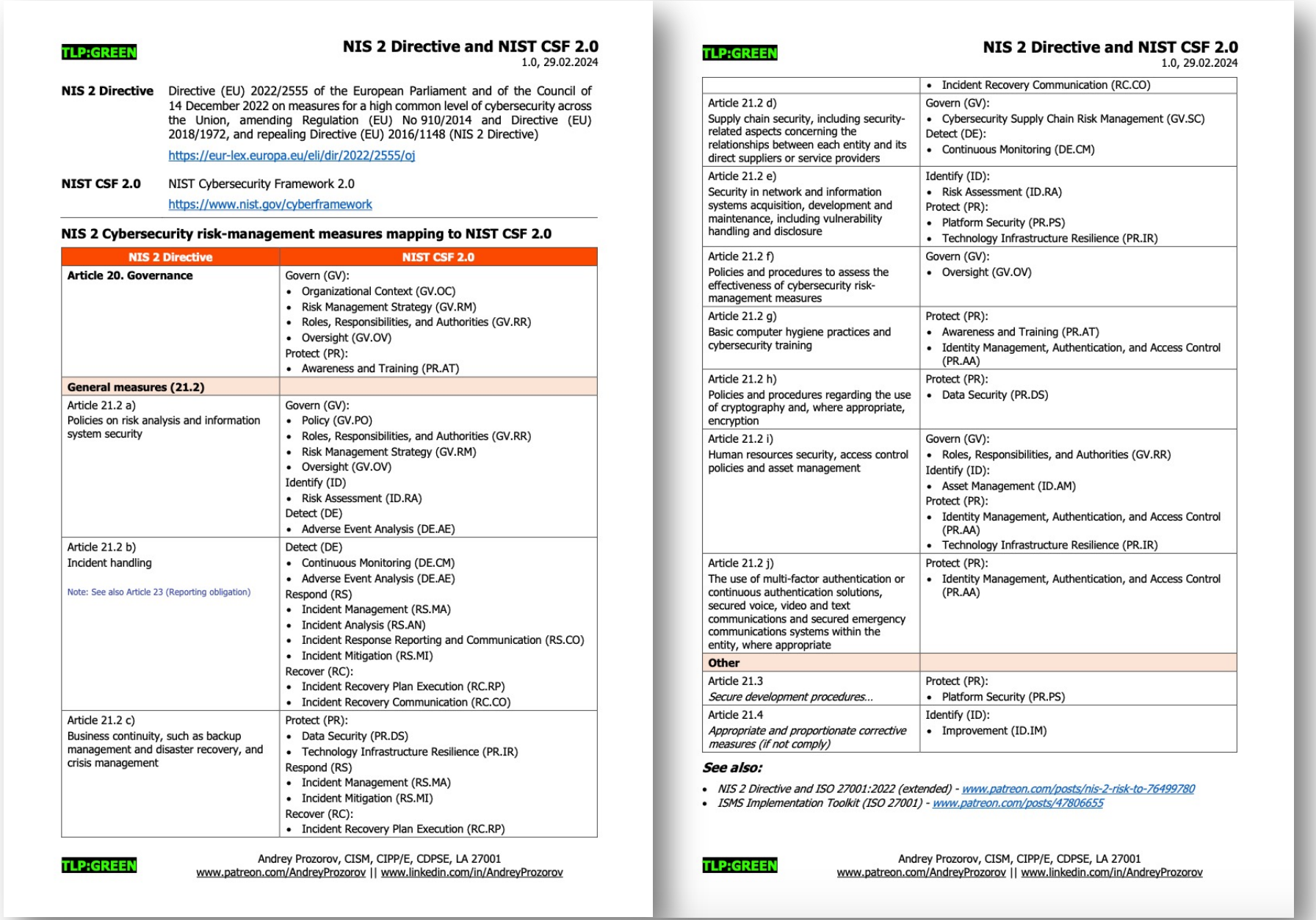
CSF 2.0 Informative References and Implementation Examples - https://www.nist.gov/informative-references

TLP:GREEN

Andrey Prozorov, CISM, CIPP/E, CDPSE, LA 27001
www.patreon.com/AndreyProzorov || www.linkedin.com/in/AndreyProzorov



EU NIS 2 Directive and NIST CSF 2.0 (mapping)



TLP:GREEN

NIS 2 Directive and NIST CSF 2.0
1.0, 29.02.2024

NIS 2 Directive Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)
https://eur-lex.europa.eu/eli/dir/2022/2555/oj

NIST CSF 2.0 NIST Cybersecurity Framework 2.0
https://www.nist.gov/cyberframework

NIS 2 Cybersecurity risk-management measures mapping to NIST CSF 2.0

NIS 2 Directive	NIST CSF 2.0
Article 20. Governance	Govern (GV): • Organizational Context (GV.OC) • Risk Management Strategy (GV.RM) • Roles, Responsibilities, and Authorities (GV.RR) • Oversight (GV.OV) Protect (PR): • Awareness and Training (PR.AT)
General measures (21.2)	
Article 21.2 a) Policies on risk analysis and information system security	Govern (GV): • Policy (GV.PO) • Roles, Responsibilities, and Authorities (GV.RR) • Risk Management Strategy (GV.RM) • Oversight (GV.OV) Identify (ID) • Risk Assessment (ID.RA) Detect (DE) • Adverse Event Analysis (DE.AE)
Article 21.2 b) Incident handling Note: See also Article 23 (Reporting obligation)	Detect (DE) • Continuous Monitoring (DE.CM) • Adverse Event Analysis (DE.AE) Respond (RS) • Incident Management (RS.MA) • Incident Analysis (RS.AN) • Incident Response Reporting and Communication (RS.CO) • Incident Mitigation (RS.MI) Recover (RC): • Incident Recovery Plan Execution (RC.RP) • Incident Recovery Communication (RC.CO)
Article 21.2 c) Business continuity, such as backup management and disaster recovery, and crisis management	Protect (PR): • Data Security (PR.DS) • Technology Infrastructure Resilience (PR.IR) Respond (RS) • Incident Management (RS.MA) • Incident Mitigation (RS.MI) Recover (RC): • Incident Recovery Plan Execution (RC.RP)

TLP:GREEN

Andrey Prozorov, CISM, CIPP/E, CDPSE, LA 27001
www.patreon.com/AndreyProzorov || www.linkedin.com/in/AndreyProzorov

TLP:GREEN

NIS 2 Directive and NIST CSF 2.0
1.0, 29.02.2024

	• Incident Recovery Communication (RC.CO)
Article 21.2 d) Supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers	Govern (GV): • Cybersecurity Supply Chain Risk Management (GV.SC) Detect (DE): • Continuous Monitoring (DE.CM)
Article 21.2 e) Security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure	Identify (ID): • Risk Assessment (ID.RA) Protect (PR): • Platform Security (PR.PS) • Technology Infrastructure Resilience (PR.IR)
Article 21.2 f) Policies and procedures to assess the effectiveness of cybersecurity risk-management measures	Govern (GV): • Oversight (GV.OV)
Article 21.2 g) Basic computer hygiene practices and cybersecurity training	Protect (PR): • Awareness and Training (PR.AT) • Identity Management, Authentication, and Access Control (PR.AA)
Article 21.2 h) Policies and procedures regarding the use of cryptography and, where appropriate, encryption	Protect (PR): • Data Security (PR.DS)
Article 21.2 i) Human resources security, access control policies and asset management	Govern (GV): • Roles, Responsibilities, and Authorities (GV.RR) Identify (ID): • Asset Management (ID.AM) Protect (PR): • Identity Management, Authentication, and Access Control (PR.AA) • Technology Infrastructure Resilience (PR.IR)
Article 21.2 j) The use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communications systems within the entity, where appropriate	Protect (PR): • Identity Management, Authentication, and Access Control (PR.AA)
Other	
Article 21.3 *Secure development procedures…*	Protect (PR): • Platform Security (PR.PS)
Article 21.4 *Appropriate and proportionate corrective measures (if not comply)*	Identify (ID): • Improvement (ID.IM)

See also:

- *NIS 2 Directive and ISO 27001:2022 (extended) - www.patreon.com/posts/nis-2-risk-to-76499780*
- *ISMS Implementation Toolkit (ISO 27001) - www.patreon.com/posts/47806655*

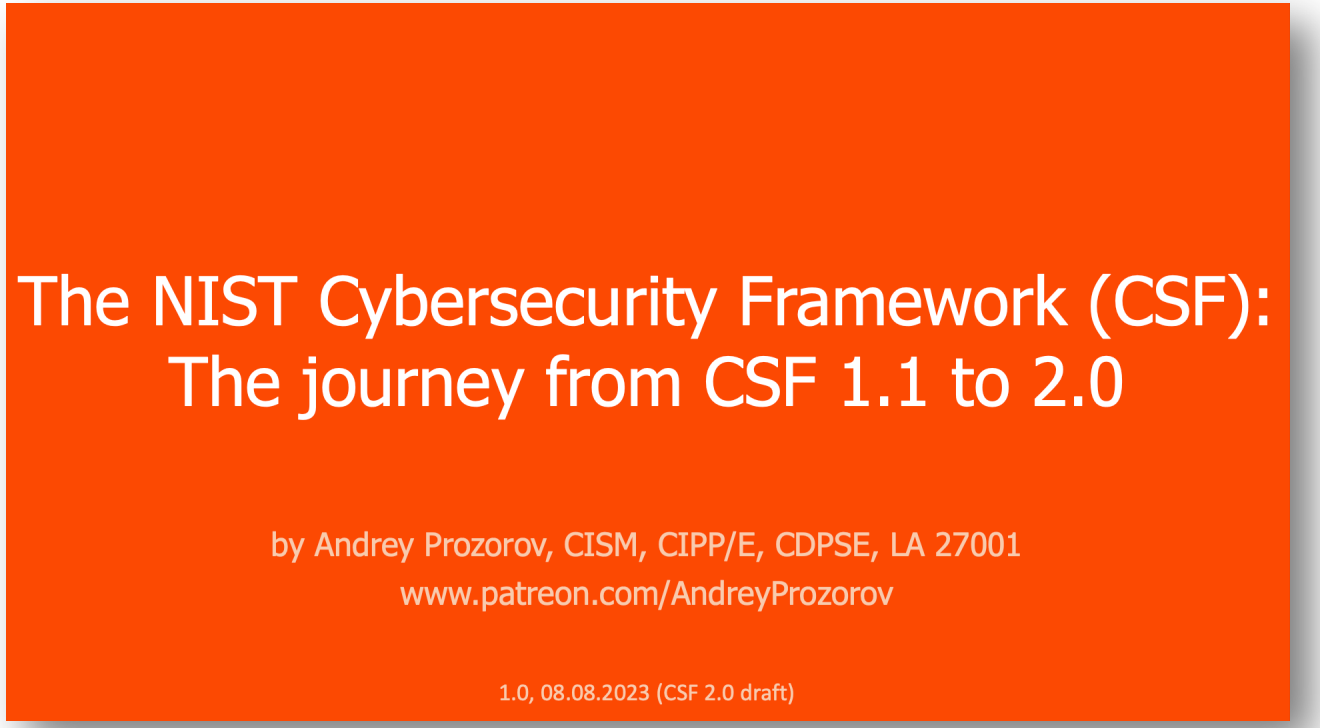
TLP:GREEN

Andrey Prozorov, CISM, CIPP/E, CDPSE, LA 27001
www.patreon.com/AndreyProzorov || www.linkedin.com/in/AndreyProzorov

Thanks, and good luck!

www.linkedin.com/in/andreyprozorov

www.patreon.com/AndreyProzorov



New slide

Changes

No changes

If you have viewed my previous presentation, these markers will help you identify the differences between the draft and final versions of NIST CSF 2.0