SmartSuite

Framework / Cybersecurity / NIST Frameworks

NIST Cybersecurity Framework (CSF) v2.0

NIST CSF 2.0 (CSWP 29, February 26, 2024) is the voluntary cybersecurity framework with six Functions including Govern, 22 Categories, 106 Subcategories, Profiles and Tiers.



What it is

The NIST Cybersecurity Framework (CSF) 2.0, published as NIST CSWP 29 on February 26, 2024, is the current edition of NIST's voluntary framework for managing and reducing cybersecurity risk. It is written for organizations of any size, sector or maturity, including industry, government, academia and nonprofits, and it widens the scope of earlier editions beyond critical infrastructure: NIST dropped the old title, “Framework for Improving Critical Infrastructure Cybersecurity.” The previous edition is described on the NIST CSF 1.1 page .

CSF 2.0 has three components: the CSF Core, a taxonomy of outcomes arranged as 6 Functions, 22 Categories and 106 Subcategories; Organizational Profiles that describe an organization's current and target posture; and Tiers that characterize the rigor of its cybersecurity risk governance and management. Its new Function, Govern, sits at the center of the Core and covers strategy, policy, roles, oversight and supply chain risk. NIST states that the CSF may be adopted voluntarily and through governmental policies and mandates.

At a glance

PUBLISHER National Institute of Standards and Technology (NIST)	TYPE Framework	VERSION CSF 2.0 (NIST CSWP 29)
EFFECTIVE February 26, 2024	DOMAIN Cybersecurity	FAMILY NIST Frameworks
REGION United States	ADOPTION MODEL Voluntary	IMPLEMENTATION COMPLEXITY Medium

Source: nist.gov/cyberframework

Why it matters

- **Governance as a Function** GV.RM-02 asks that risk appetite and risk tolerance statements are established, communicated and maintained, and GV.RR-01 makes leadership accountable for cybersecurity risk.
- **Supplier risk in the Core** The GV.SC Category has ten Subcategories; GV.SC-05 requires supply chain cybersecurity requirements to be integrated into contracts, and GV.SC-07 requires supplier risk to be monitored over the relationship.
- **Profiles close the gap** A Current Profile and a Target Profile, compared side by side, give a prioritized action plan such as a risk register or Plan of Action and Milestones.
- **Tiers for governance** Tier 1 Partial to Tier 4 Adaptive characterize the rigor of risk governance and management and apply to Profiles, not to the Core.

 © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports NIST CSF 2.0

Core Outcome Library

Load the 22 Categories and 106 Subcategories with an owner, implementation status and linked controls and evidence.

Organizational Profiles

Record the Current Profile and Target Profile for each scope, compare them side by side and track the gap actions from section 3.1.

Govern Records

Hold the risk strategy, risk appetite and tolerance statements (GV.RM-02), roles and accountability (GV.RR) and policies (GV.PO) as linked records with approval history.

Supplier Risk Tracking

Assess and monitor suppliers against GV.SC-05 and GV.SC-07 in Third Party Risk Management, with contract requirements and review dates.

Cyber Risk Register

Log cybersecurity risks and vulnerabilities in Cyber & IT Risk with owners, treatments and the Core outcomes they affect, and share them with Enterprise Risk Management.

Tier and Transition Record

Document the Tier chosen for each Profile and keep the mapping from CSF 1.1 Subcategories to CSF 2.0 outcomes.

Common framework mappings

CIS Controls v8.1 | ISO 27001:2022 | ISO 27002:2022 | ISO 27701 | MITRE ATT&CK | NIST Privacy Framework v1.0 | NIST 800-171 Rev. 3 | NIST 800-53 Rev.5

Official resources

NIST Cybersecurity Framework v2.0

Provides the official NIST publication outlining the CSF and its core functions.

nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

NIST Cybersecurity Framework Overview

Outlines the structure and components of the NIST Cybersecurity Framework for organizations.

nist.gov/cyberframework

NIST CSF 2.0 Quick Start Guides

NIST's Quick Start Guides for CSF 2.0: small business, Organizational Profiles, Tiers, C-SCRM and enterprise risk management.

nist.gov/cyberframework/quick-start-guides

NIST CSF 2.0 informative references

NIST's informative references and mappings for CSF 2.0 through the Cybersecurity and Privacy Reference Tool.

nist.gov/cyberframework/informative-references

Frequently asked questions

What is new in NIST CSF 2.0 compared with 1.1?

CSF 2.0 adds a sixth Function, Govern, which covers organizational context, risk management strategy, roles and responsibilities, policy, oversight and cybersecurity supply chain risk management. It names organizations of all sizes and sectors as the audience, drops the critical infrastructure title, adds Implementation Examples and online Informative References, and treats Profiles and Tiers as tools for governance. The Core has 22 Categories and 106 Subcategories.

How many Functions, Categories and Subcategories does CSF 2.0 have?

Appendix A lists six Functions (Govern, Identify, Protect, Detect, Respond, Recover), 22 Categories identified in Table 1 and 106 Subcategories. Govern has 6 Categories and 31 Subcategories; Identify 3 and 21; Protect 5 and 22; Detect 2 and 11; Respond 4 and 13; Recover 2 and 8.

Updated Oct 15, 2026 · © 2026 SmartSuite Inc. All rights reserved.

What is an Organizational Profile?

An Organizational Profile describes an organization's current and/or target cybersecurity posture in terms of Core outcomes (section 3.1). A Current Profile shows what is achieved now and a Target Profile shows what has been selected and prioritized. Comparing them gives the gap analysis and action plan. A Community Profile is a published baseline for a sector, technology or threat type that an organization can use as the basis for its own Target Profile.

What do the CSF 2.0 Tiers measure?

Section 3.2 and Appendix B describe Tier 1 Partial, Tier 2 Risk Informed, Tier 3 Repeatable and Tier 4 Adaptive. They characterize the rigor of an organization's cybersecurity risk governance practices (Govern) and its risk management practices (Identify through Recover), and they are applied to Current and Target Profiles. NIST says Tiers should complement an organization's risk methodology, and that moving to a higher Tier is encouraged when risks or mandates are greater or a cost-benefit analysis supports it.

Is NIST CSF 2.0 mandatory, and can an organization be certified against it?

The CSF is a foundational resource that may be adopted voluntarily and through governmental policies and mandates (section 1). NIST describes outcomes and does not prescribe how to achieve them, so organizations express their posture with Profiles and Tiers and not with a certificate.

License included / downloadable: Yes NIST publications are works of the U.S. government. CSF 2.0 (CSWP 29), the Quick-Start Guides, the Profile template and the CSF 2.0 Reference Tool are free on the NIST CSF website and the CSRC publication page.

Full framework page and mappings: smartsuite.com/frameworks/nist-cybersecurity-framework-csf-v2-0