

NIST Cybersecurity Framework (CSF) v2.0

NIST Cybersecurity Framework (CSF) v2.0 is a risk-based framework that helps organizations manage and reduce cybersecurity risks.



What it is

The NIST Cybersecurity Framework (CSF) v2.0 is a risk-based cybersecurity framework that helps organizations manage and reduce cybersecurity risks across their operations. It provides a structured approach to identifying, protecting against, detecting, responding to, and recovering from cyber threats.

Developed and published by the National Institute of Standards and Technology (NIST), the CSF is widely adopted by both public and private sector organizations to strengthen cybersecurity governance and risk management practices. The framework encompasses key focus areas including cybersecurity controls, incident response, risk assessment, and operational resilience, and is designed to be adaptable across industries and organization sizes.

At a glance

PUBLISHER National Institute of Standards and Technology (NIST)	TYPE Standard	VERSION NIST Cybersecurity Framework v2.0
EFFECTIVE February 2024	DOMAIN Cybersecurity	FAMILY NIST Frameworks
REGION United States	ADOPTION MODEL Risk Management	IMPLEMENTATION COMPLEXITY Moderate

Source: <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf>

Why it matters

- **Strengthen cybersecurity governance** Establish clear roles, responsibilities, and oversight to guide security decisions and improve accountability throughout the organization.
- **Enhance regulatory alignment** Support compliance efforts by mapping controls to multiple regulatory frameworks and facilitating responses to evolving legal requirements.
- **Improve threat detection capabilities** Enable earlier identification of potential cyber threats and vulnerabilities, reducing the likelihood of undetected incidents within networks and systems.
- **Promote operational resilience** Increase organizational resilience through improved planning and response measures that minimize impacts from cyber incidents and disruptions.

How SmartSuite supports NIST CSF 2.0

CSF Profile and Roadmap Build Current and Target Profiles and track a prioritized improvement roadmap.	CSF Function Mapping Map controls and initiatives to Govern, Identify, Protect, Detect, Respond, Recover.	Control Ownership and Recurring Tasks Assign owners and set recurring tasks for key controls and reviews.
Evidence and Metrics Tracking Attach evidence and track KPIs/KRIs to show measurable progress.	Incident and Recovery Workflows Run response and recovery tasks with timelines, decisions, and lessons learned.	Executive Reporting Dashboards Report maturity, gaps, and progress by function, category, and business unit.

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 Cybersecurity Framework Implementation Tiers
Defines the implementation tiers that guide cybersecurity maturity assessment.
nist.gov/cyberframework/online-learning/components-framework

NIST Framework Core Functions
Outlines the core functions of identify, protect, detect, respond, and recover.
nist.gov/cyberframework/getting-started-csf-11

Frequently asked questions

- What is the NIST Cybersecurity Framework (CSF) v2.0 used for?**
The NIST Cybersecurity Framework (CSF) v2.0 helps organizations manage, assess, and reduce cybersecurity risks through a structured, risk-based approach. It is widely used to develop, strengthen, and mature cybersecurity governance, controls, and incident response processes, aligning security practices with organizational objectives and regulatory obligations.
- Is compliance with the NIST CSF v2.0 mandatory or certifiable?**
The NIST CSF v2.0 is voluntary and not certifiable in itself. However, many organizations voluntarily adopt the framework to demonstrate cybersecurity maturity, meet customer or regulatory expectations, and align with legal requirements where referenced by sector-specific mandates.
- Who can apply the NIST CSF v2.0, and what is its scope?**
Any organization, regardless of size, industry, or sector, can apply the NIST CSF v2.0. Its scalable and flexible structure is designed to support critical infrastructure, private enterprises, and public sector agencies in managing cybersecurity risks across all business units and technology environments.
- What are the core functions and required artifacts in the NIST CSF v2.0?**
The NIST CSF v2.0 is organized around six core functions: Govern, Identify, Protect, Detect, Respond, and Recover. Key artifacts include security control inventories, risk assessments, policies, incident response plans, and evidence documentation supporting compliance with identified controls and processes.

How do organizations implement the NIST CSF v2.0?

Implementation begins with conducting a risk assessment and establishing a target profile based on the framework's core functions and categories. Organizations integrate applicable controls, map them to business processes, assign ownership, and leverage continuous monitoring to track improvement and ensure alignment with the framework.

How does the NIST CSF v2.0 relate to other standards like ISO 27001 or NIST SP 800-53?

The NIST CSF v2.0 is designed to be compatible with other frameworks and standards, providing mappings to controls in ISO 27001, NIST SP 800-53, and others. This allows organizations to leverage their existing compliance investments and streamline cross-framework risk management and reporting.

What are the ongoing compliance requirements for the NIST CSF v2.0?

Maintaining alignment with the NIST CSF v2.0 requires regular risk assessments, periodic reviews and updates of security controls, continuous monitoring of the threat landscape, and ongoing evidence collection to support audits and executive reporting. Regular maturity assessments guide continuous improvement.

How would SmartSuite support NIST CSF v2.0?

SmartSuite enables organizations to manage the NIST CSF v2.0 by providing configurable risk registers, centralized control management, and integrated evidence collection workflows. It supports audit readiness with real-time dashboards, automated tracking of remediation activities, compliance documentation, and comprehensive reporting tools for ongoing oversight.

License included / downloadable: Yes The NIST Cybersecurity Framework is publicly available through official NIST publications.

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