

NIST Cybersecurity Framework (CSF) v1.1

NIST Cybersecurity Framework helps organizations identify, protect, detect, respond, and recover from cybersecurity risks to critical infrastructure.



What it is

The NIST Cybersecurity Framework (CSF) v1.1 is a voluntary cybersecurity framework that helps organizations manage and reduce cybersecurity risk to critical infrastructure and key business operations. It provides a structured approach for identifying, assessing, and addressing cybersecurity threats, supporting organizations in protecting information assets and maintaining operational resilience.

Developed and published by the National Institute of Standards and Technology (NIST), the CSF is widely used by both public and private sector entities in the United States and internationally. The framework outlines five core functions—Identify, Protect, Detect, Respond, and Recover—encompassing cybersecurity controls, risk management practices, and incident response activities that support robust security governance.

At a glance

PUBLISHER National Institute of Standards and Technology (NIST)	TYPE Framework	VERSION v1.1
EFFECTIVE April 2018	DOMAIN Cybersecurity	FAMILY NIST Special Publications
REGION United States	ADOPTION MODEL Risk Management	IMPLEMENTATION COMPLEXITY Moderate

Source: <https://www.nist.gov/cyberframework/framework>

Why it matters

- **Strengthen cybersecurity governance** Support consistent risk management practices and leadership oversight across business units and technology environments.
- **Enable regulatory alignment** Facilitate compliance with multiple regulatory requirements and simplify documentation for audit and reporting obligations.
- **Improve threat detection capabilities** Enhance the ability to identify, analyze, and respond effectively to evolving cyber threats in real time.
- **Promote operational resilience** Reduce the impact of security incidents by improving response planning, recovery, and business continuity measures.

How SmartSuite supports NIST CSF v1.1

CSF Control and Function Mapping

Organize controls and activities across the five NIST CSF functions and framework categories.

Risk Register and Asset Context

Link assets, business processes, and threats to CSF categories to prioritize risk management.

Security Program Workflows

Track implementation tasks across protection, monitoring, incident response, and recovery activities.

Continuous Monitoring and Detection

Capture monitoring outputs, alerts, and investigation records supporting the Detect function.

Incident Response and Recovery Coordination

Manage response playbooks, communications, and recovery actions across security teams.

Executive Cybersecurity Reporting

Provide dashboards showing CSF maturity, risk exposure, and improvement initiatives.

Common framework mappings

CIS Controls v8.1

COBIT 2019

FedRAMP Rev. 5

GDPR

HIPAA (NIST SP 800-66 Rev. 2)

ISO 27001:2022

NIST 800-53 Rev.5

PCI DSS 4.0.1

SOC 2

Official resources

NIST Cybersecurity Framework Version 1.1 Document

Defines comprehensive guidelines to improve critical infrastructure cybersecurity.

nist.gov/cyberframework

NIST Cybersecurity Framework Online Learning

Provides online learning resources to understand and implement the framework.

nist.gov/cyberframework/online-learning

NIST CSF FAQs

Outlines frequently asked questions about the implementation and scope of the framework.

nist.gov/cyberframework/faqs

Framework for Improving Critical Infrastructure Cybersecurity

Details the structure, concepts, and management approach of the NIST CSF.

nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

Frequently asked questions

What is the NIST Cybersecurity Framework (CSF) v1.1 used for?

The NIST Cybersecurity Framework (CSF) v1.1 is designed to help organizations identify, assess, and manage cybersecurity risks to critical infrastructure. It provides a flexible set of standards, guidelines, and best practices to improve cybersecurity posture across sectors. The framework supports organizations in prioritizing investments and actions to protect their systems, data, and assets.

Is the NIST Cybersecurity Framework (CSF) v1.1 mandatory or certifiable?

The NIST Cybersecurity Framework is voluntary and not intended for certification. It is not a mandate, but it is widely adopted as a best practice in both public and private sectors. Some regulatory bodies may reference CSF alignment, but formal certification is not available.

Who should use the NIST Cybersecurity Framework?

The CSF is applicable to organizations of all sizes and industries, especially those classified as critical infrastructure. It is suitable for security leaders, risk managers, compliance teams, and auditors seeking a structured approach to cybersecurity risk management. The framework is scalable and adaptable to various organizational structures and risk profiles.

What are the key components of the NIST Cybersecurity Framework?

The CSF is built around five core functions: Identify, Protect, Detect, Respond, and Recover. Within these functions are categories, subcategories, and informative references that guide the implementation of controls and processes. Key artifacts include a cybersecurity profile and risk assessment documentation.

How should organizations implement the NIST Cybersecurity Framework?

Implementation typically begins with a current-state assessment and asset inventory, aligned to the framework's Core functions. Organizations determine their target profile, conduct a gap analysis, and prioritize actions to close gaps. Ongoing measurement and improvement are encouraged through periodic reviews and updates.

How does the NIST Cybersecurity Framework relate to other standards and regulations?

The CSF is designed to be compatible with other standards, such as ISO 27001, COBIT, and sector-specific regulations. It incorporates references to existing standards and guidelines to facilitate mapping and integration. This allows organizations to leverage existing controls and processes while achieving broader cybersecurity objectives.

What are the ongoing compliance requirements for the NIST CSF?

There are no strict compliance requirements, but organizations are encouraged to maintain documentation of their cybersecurity program, perform regular risk assessments, and continuously monitor and update their controls. Ongoing governance and periodic self-assessments support alignment with the CSF's principles and objectives.

How would SmartSuite support NIST Cybersecurity Framework (CSF) v1.1?

SmartSuite can help organizations manage the NIST CSF by enabling structured risk tracking, control management, and evidence collection. It supports the creation and maintenance of framework-aligned documentation and streamlines audit readiness through centralized dashboards and reporting. SmartSuite's workflow tools also facilitate ongoing monitoring and continuous improvement of cybersecurity practices.

License included / downloadable: Yes NIST CSF v1.1 is publicly available for free from NIST's website. License included with platform

Full framework page and mappings: smartsuite.com/frameworks/nist-cybersecurity-framework-csf-v1-1