CS-104 · Compliance & Frameworks

NIST Cybersecurity Framework (CSF)

A voluntary, risk-based framework that organizes security work into six core functions.

Executive Summary

The NIST Cybersecurity Framework (CSF) is a voluntary, risk-based structure published by the U.S. National Institute of Standards and Technology to help organizations understand, manage, and reduce cybersecurity risk. It organizes activity into a small set of core functions and a common vocabulary that technical and non-technical leaders can share. CSF 2.0 added Govern as a function and broadened the framework beyond critical infrastructure to organizations of any size or sector.

What It Is

The NIST Cybersecurity Framework is a flexible model for describing and improving how an organization manages cybersecurity risk. It is not a checklist of mandatory rules and it is not a certification. Instead it gives leaders a shared language and a structure for deciding where to focus. The current version, CSF 2.0, is built around six core functions: Govern, Identify, Protect, Detect, Respond, and Recover. Each function breaks down into categories and subcategories that describe outcomes an organization is trying to achieve, such as knowing what assets it owns or having a plan to recover after an incident. The framework is intentionally outcome-focused, so it can be applied to a small nonprofit or a global enterprise without prescribing specific products.

Why It Matters

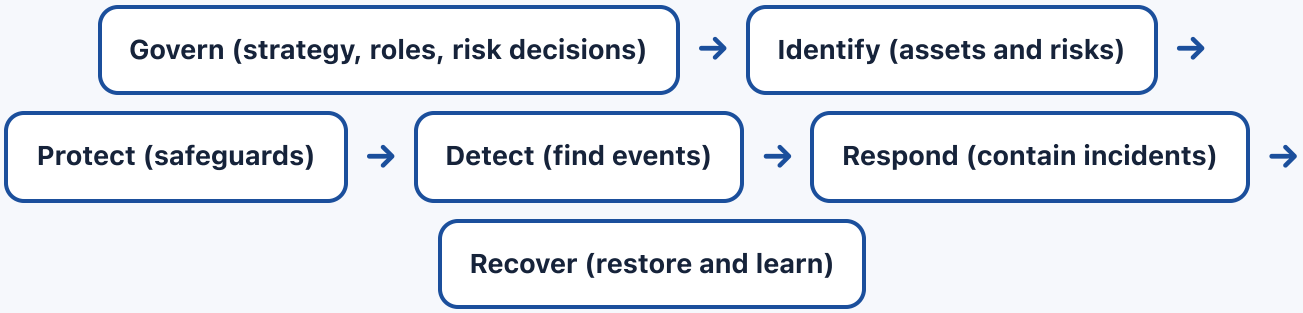
Because the CSF is widely recognized across government and private industry, it has become a common reference point when organizations describe their security posture to boards, regulators, insurers, and business partners. Adopting it helps an organization move from ad hoc

security spending to a defensible, prioritized program tied to actual risk. For professionals, fluency in the CSF is often expected in GRC, audit, and security leadership roles because it frames conversations that cut across compliance, operations, and executive strategy. Many other requirements, contracts, and internal policies map back to the CSF, so understanding it makes many other frameworks easier to navigate.

How It Works

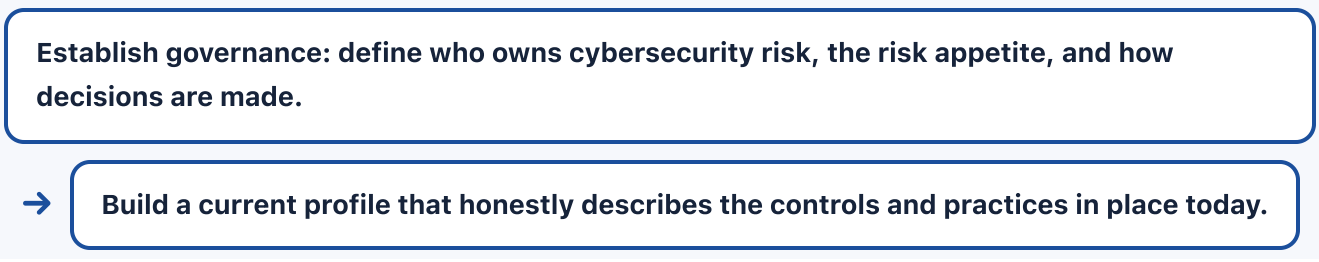
Organizations use the CSF by describing a current profile (what they do today) and a target profile (what they want to achieve), then closing the gap between them in a way that reflects their risk tolerance and resources. The six functions provide the top-level structure. Govern sets the strategy, roles, and risk decisions that steer the whole program. Identify builds understanding of assets, suppliers, and risks. Protect puts safeguards in place. Detect finds events as they happen. Respond contains and manages incidents. Recover restores operations and captures lessons. Implementation tiers describe how mature and integrated the program is, from informal and reactive to adaptive and repeatable. Because the framework references other standards and control sets, teams often pair it with a detailed control catalog for the specifics.

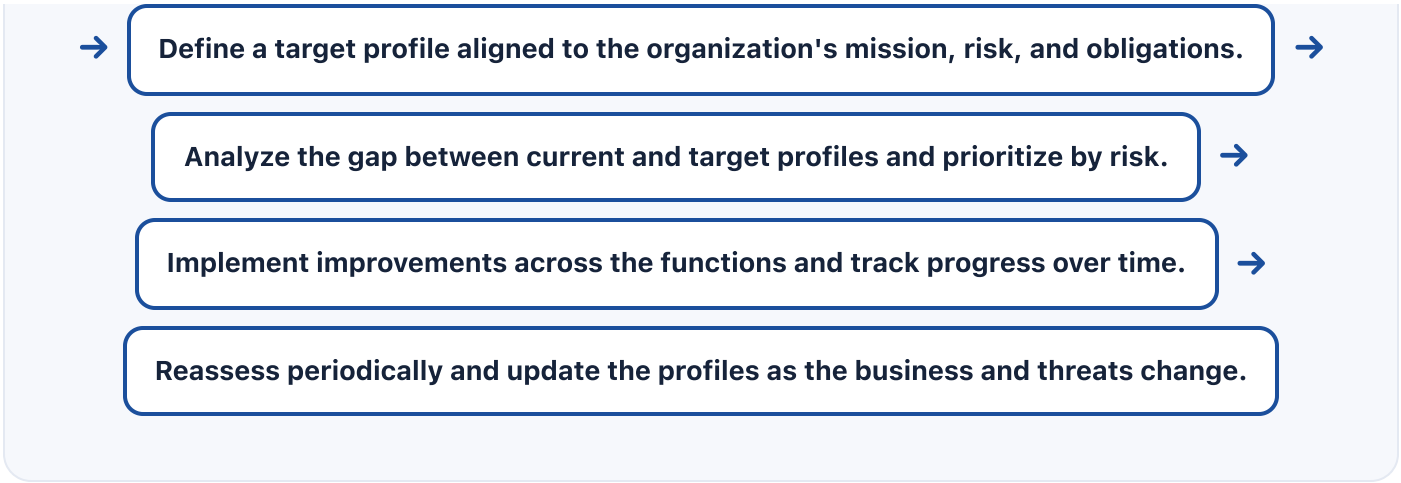
Architecture Diagram



The six CSF 2.0 functions form a continuous cycle, with Govern at the center steering the other five.

Visual Workflow





Common Attacks

- Adopting the framework on paper but never operationalizing it in daily work
- Skipping the Govern function so security decisions have no owner or risk context
- Building a target profile that ignores the organization's real resources and risk tolerance
- Treating the CSF as a one-time assessment rather than a repeated cycle
- Confusing the CSF with a certification or a rigid control checklist

Common Mistakes

- Copying another organization's target profile instead of tailoring one to your own risk
- Measuring maturity by how many tools are bought rather than outcomes achieved
- Leaving the current profile as an aspirational document rather than an honest baseline
- Failing to map existing controls to CSF categories, which hides gaps and duplication
- Assigning the framework to IT alone when Govern requires business and executive ownership

Best Practices

- Start with Govern: assign clear ownership of cybersecurity risk at the leadership level
- Create honest current and target profiles and revisit them on a regular schedule
- Prioritize gaps by business risk, not by ease or cost of the fix alone
- Map the CSF to the detailed control set you already use to avoid duplicate effort
- Use the framework's common language to report status to the board and stakeholders

- Track implementation tier over time to show maturity progress

Quick Checklist

- [x] A named owner is accountable for cybersecurity risk at the executive level
- [x] A documented current profile reflects actual practices, not intentions
- [x] A target profile is tied to mission, risk tolerance, and obligations
- [x] Gaps between profiles are prioritized and tracked to closure
- [x] CSF categories are mapped to your detailed controls or catalog
- [x] Progress and residual risk are reported to leadership on a set cadence

Recommended Tools

GRC platform
Tracks CSF profiles, mappings, gaps, and evidence in one place

Control mapping spreadsheet or catalog
Links CSF categories to detailed controls you already run

Risk register
Records prioritized risks that drive the target profile

Maturity assessment template
Scores implementation tier and tracks progress over time

Industry Standards

NIST Cybersecurity Framework (CSF) 2.0
The framework itself, organized around Govern, Identify, Protect, Detect, Respond, Recover

NIST SP 800-53
Detailed control catalog often used to implement CSF outcomes

ISO/IEC 27001
International standard that many

organizations map to the CSF

Career Relevance

The NIST CSF is a core competency for GRC analysts, compliance analysts, security auditors, and CISOs, who use it to structure programs, report to leadership, and align with other requirements. It also appears in the work of risk managers, security architects, and privacy and AI governance professionals, the audience AI-Governance-Jobs.com serves, because it provides the shared language that connects technical controls to business risk.

Interview Questions

- What are the six functions of the NIST CSF 2.0, and what does each accomplish?
- Why was Govern added as a function, and how does it change how a program is run?
- Explain the difference between a current profile and a target profile.
- How would you use implementation tiers to describe program maturity?
- How does the CSF relate to a detailed control catalog like NIST SP 800-53?

Related Certifications

ISACA CISM | ISC2 CISSP | CompTIA Security+

Further Reading

- NIST Cybersecurity Framework
- NIST CSF 2.0 Resources
- CISA: Cybersecurity Best Practices

Key Takeaways

- The NIST CSF is a voluntary, risk-based framework, not a certification or a fixed checklist.
- CSF 2.0 is built on six functions: Govern, Identify, Protect, Detect, Respond, Recover.

- Organizations close the gap between a current profile and a target profile based on risk.
- Govern anchors the program by assigning ownership and risk decisions at the leadership level.
- Fluency in the CSF is expected across GRC, audit, and security leadership roles.

FAQ

Related Careers

RELATED ROLES

Grc Analyst | Compliance Analyst | Security Auditor | Ciso

RELATED CERTIFICATIONS

ISACA CISM | ISC2 CISSP | CompTIA Security+

CURRENT OPENINGS

Live roles are on the job board.

Browse all jobs

GUIDES & SALARY

Career guides | Role roadmaps | Salary data | Career tools

SUGGESTED LEARNING PATH

1. Ground the basics with CS-001 Cybersecurity
2. Study this sheet: **NIST Cybersecurity Framework (CSF)**
3. Go deeper: CIS Controls

4. Go deeper: ISO/IEC 27001
5. Validate it: work toward **ISACA CISM**
6. Find the role: browse current openings

RELATED SHEETS

CS-105 CIS Controls | CS-106 ISO/IEC 27001 | CS-001 Cybersecurity | CS-085 Risk Ratings | CS-009 Core Security Principles