GOVDATAHOSTING
POWERED BY IT-CNP, INC.

FEDRAMP HIGH (CLASS D) AUTHORIZED CLOUD PLATFORM

COMPLETE NIST CYBERSECURITY FRAMEWORK (CSF 2.0) GUIDE

Your Roadmap to Managing Cybersecurity Risk with a Common Language

2026 EDITION • **NIST CSF 2.0 (FEB 2024) & 800-53 REV 5 MAPPINGS**

WHAT YOU'LL LEARN

What the CSF is and who uses it • The six Functions, 22 Categories & 106 Subcategories • Implementation Tiers & Profiles • A seven-step implementation process • Mapping CSF to FedRAMP, FISMA & CMMC • Common pitfalls to avoid • Implementation checklist

FOR

Federal Agencies • State & Local Government • Government Contractors • Education & Nonprofit

GovDataHosting

FedRAMP High (Class D) Certified • NIST 800-53 High • DoD IL2 Authorized

www.govdatahosting.com | 800-967-1004

What's Inside

Executive Summary

The NIST Cybersecurity Framework (CSF) is the most widely adopted cyber risk-management framework in the world. First published in 2014 for operators of critical infrastructure, it has become the common language organizations of every size and sector use to describe, assess, and communicate their cybersecurity posture. Unlike a control catalog or an audited certification, the CSF is voluntary and outcome-focused: it describes what good cybersecurity looks like and lets each organization decide how to get there.

In February 2024, NIST released CSF 2.0 — the first major revision in a decade. It added a new Govern function that elevates cybersecurity to an enterprise governance concern, formally broadened the framework beyond critical infrastructure to organizations of all types, and refreshed its mappings to current standards including NIST SP 800-53 Rev 5. This guide distills CSF 2.0 into a practical roadmap: the framework structure, how to measure maturity with Tiers and Profiles, a seven-step implementation process, and how CSF work compounds toward formal authorizations like FedRAMP and FISMA.

Key Takeaways

- **The CSF is voluntary but increasingly required** — referenced in state cybersecurity laws, insurer underwriting, and customer due-diligence questionnaires.
- **CSF 2.0 has six Functions** — Govern, Identify, Protect, Detect, Respond, and Recover — organized into 22 Categories and 106 Subcategories.
- **It is outcome-based, not prescriptive** — you choose the technologies and processes that achieve each Subcategory in your environment.
- **Tiers and Profiles turn security into a measurable, communicable posture** — ideal for board reporting and vendor risk conversations.
- **CSF is the most common on-ramp to stricter regimes** — its informative references map directly to 800-53, 800-171/CMMC, ISO 27001, and CIS Controls.

Understanding the NIST CSF

What is the Cybersecurity Framework?

The NIST Cybersecurity Framework is a voluntary set of guidelines, best practices, and standards for managing cybersecurity risk. It was created under Executive Order 13636 (2013) and first published as version 1.0 in 2014, updated to 1.1 in 2018, and to 2.0 in February 2024. Rather than dictating specific technologies, the CSF organizes cybersecurity outcomes into a hierarchy of Functions, Categories, and Subcategories that any organization can adopt and adapt.

The framework is built to do three things: **help an organization understand and assess** its current cybersecurity posture, **prioritize** opportunities for improvement, and **communicate** cyber risk consistently to internal and external stakeholders — from technical staff to executives, regulators, insurers, and business partners.

Who Uses the CSF?

Because the CSF is sector-agnostic and technology-neutral, adoption spans the public and private sectors:

Audience	How they use the CSF
Federal agencies	Executive Order 13800 directs agencies to manage risk using the CSF; it complements the mandatory FISMA / NIST 800-53 program as a strategic overlay.
State & local government	Many SLED agencies adopt CSF as their primary framework, mapping to StateRAMP / GovRAMP and CJIS for specific workloads.
Government contractors	Contractors use CSF to organize their security program before pursuing formal certifications such as CMMC Level 2 or FedRAMP.
Education & nonprofit	Universities and nonprofits use CSF as a flexible baseline before stepping up to NIST 800-171 for federally funded research or protected data.
Private enterprise	Adopted to satisfy cyber-insurance underwriting, board oversight, and third-party/vendor risk requirements.

KEY INSIGHT

Voluntary does not mean optional. CSF alignment is now written into state laws (e.g., NY DFS Part 500), cyber-insurance applications, federal executive orders, and countless customer security questionnaires. For most organizations the practical question is not whether to align to CSF, but how quickly they can demonstrate that alignment.

The CSF 2.0 Framework Structure

CSF 2.0 is organized as a hierarchy. Six high-level Functions represent the pillars of a cybersecurity program. Each Function contains Categories — groups of related outcomes — and each Category contains Subcategories, the specific, measurable outcomes an organization works toward. In total, CSF 2.0 defines 6 Functions, 22 Categories, and 106 Subcategories.

The Six Core Functions

Function	Purpose
Govern (GV) NEW in 2.0	Establish, communicate, and monitor the organization's cybersecurity risk-management strategy, expectations, and policy. Govern wraps around and informs all other functions.
Identify (ID)	Develop an organizational understanding of assets, the business environment, governance, risk, and supply-chain risk that cybersecurity must manage.
Protect (PR)	Implement safeguards to ensure delivery of critical services: identity management, access control, awareness training, data security, and platform hardening.
Detect (DE)	Implement activities to find and analyze possible cybersecurity attacks and compromises — continuous monitoring and adverse-event analysis.
Respond (RS)	Take action on a detected incident: response planning, communications, analysis, mitigation, and reporting.
Recover (RC)	Restore assets and operations affected by an incident and maintain plans for resilience and continuity.

What Changed in CSF 2.0

- **A new Govern function.** Governance moved from a Category inside Identify to a top-level Function, making cyber-risk strategy, roles, policy, and oversight an explicit executive responsibility.
- **Broadened scope.** The framework is no longer aimed only at critical infrastructure — CSF 2.0 explicitly applies to organizations of all sizes, sectors, and maturity levels, with dedicated small-business guidance.
- **Deeper supply-chain focus.** Cybersecurity Supply Chain Risk Management (C-SCRM) is integrated throughout, reflecting the rise of third-party and software-supply-chain attacks.
- **Refreshed references and tools.** Informative references were updated to current standards (including NIST 800-53 Rev 5), supported by online Reference Tool, Quick-Start Guides, and Implementation Examples.

Implementation Tiers & Profiles

The CSF deliberately avoids prescribing a single "right" answer. Instead it offers two tools for measuring and communicating posture. **Implementation Tiers** describe how rigorously and consistently an organization manages cyber risk, from ad-hoc to adaptive. **Profiles** capture where the organization is today (Current Profile) and where it needs to be (Target Profile) across the Subcategories that matter to its mission.

The Four Implementation Tiers

Tier	Name	Characteristics
Tier 1	Partial	Risk management is ad-hoc and reactive; limited organizational awareness; cybersecurity is not integrated with broader risk management. A common starting point.
Tier 2	Risk Informed	Risk-management practices are approved by management but not established as organization-wide policy; awareness exists but implementation is inconsistent.
Tier 3	Repeatable	Formal, organization-wide risk-management policy; practices are updated as threats and missions change and applied consistently across the organization.
Tier 4	Adaptive	Practices are continuously improved from lessons learned and predictive indicators; cybersecurity is embedded in organizational culture and information is shared in real time.

Tiers are assessed per Function, not as a single overall score, and higher is not automatically better. Each organization selects target Tiers that reflect its risk tolerance, mission, threat environment, and budget. For most organizations, Tier 3 (Repeatable) is a practical target that demonstrates a mature, defensible program.

Current & Target Profiles

Profile	What it captures	How it is used
Current Profile	The cybersecurity outcomes the organization is achieving today, Subcategory by Subcategory.	Establishes a factual baseline and a shared understanding of present posture.
Target Profile	The outcomes the organization needs to achieve, based on risk, mission, and external requirements.	Defines the destination and the basis for prioritizing investment.
The Gap	The difference between Current and Target Profiles.	Drives a prioritized, cost-aware action plan to close the most important gaps first.

Implementing CSF: A Seven-Step Process

NIST describes a repeatable seven-step process for establishing or improving a cybersecurity program with the CSF. The cycle is iterative — organizations repeat it as their mission, risks, and threat landscape evolve.

Step	Activity	What happens
1	Prioritize & Scope	Identify business/mission objectives and priorities, then determine the scope of systems and assets that support the selected line of business.
2	Orient	Identify related systems, assets, regulatory requirements, and the overall risk approach; consult sources to identify threats and vulnerabilities.
3	Create a Current Profile	Document which Category and Subcategory outcomes are currently being achieved and to what degree.
4	Conduct a Risk Assessment	Analyze the operational environment to discern the likelihood and impact of cybersecurity events on the organization.
5	Create a Target Profile	Describe the desired cybersecurity outcomes, informed by risk tolerance, mission drivers, and external requirements.
6	Determine, Analyze & Prioritize Gaps	Compare Current and Target Profiles to identify gaps; create a prioritized, cost-benefit-informed action plan.
7	Implement Action Plan	Execute the plan to close gaps, then monitor and repeat the cycle to sustain and improve the program.

CONTINUOUS BY DESIGN

CSF is not a one-time project. The new Govern function makes ongoing oversight explicit: leadership monitors the program, re-runs the profile-and-gap cycle as conditions change, and treats the Target Profile as a living statement of intent. This mirrors the continuous-monitoring discipline required by FISMA and FedRAMP.

CSF as an On-Ramp to Other Frameworks

One of the CSF's greatest strengths is that it does not exist in isolation. Every Subcategory carries "informative references" that map directly to detailed control catalogs and standards. That means the work an organization does to align with CSF compounds toward formal certifications rather than duplicating effort. CSF is the strategic layer; the frameworks below supply the detailed, auditable controls.

How the CSF Functions Map to NIST 800-53

CSF 2.0 Function	How GovDataHosting supports it	Primary 800-53 families
Govern (GV)	Shared-responsibility model and inheritance documentation for your authorization boundary.	PM, PL, PS
Identify (ID)	Asset inventory and system-boundary documentation for hosted workloads.	CM, RA, SA
Protect (PR)	Identity, encryption, network segmentation, and platform hardening at the infrastructure layer.	AC, IA, SC, MP
Detect (DE)	SIEM, IDS/IPS, vulnerability scanning, and anomaly alerting.	AU, SI, CA
Respond (RS)	24×7 SOC and infrastructure incident-response runbooks.	IR
Recover (RC)	Multi-zone backup, disaster-recovery infrastructure, and restoration testing.	CP

CSF Maps to Every Major Compliance Regime

Framework	Relationship to CSF
NIST 800-53 Rev 5	The detailed control catalog CSF references; the basis for FISMA and FedRAMP authorizations.
FedRAMP / FISMA	Federal authorizations built on 800-53. CSF organizes the program; 800-53 supplies the controls you must implement.
NIST 800-171 / CMMC	Protects Controlled Unclassified Information for defense contractors; CSF is a common precursor to a CMMC assessment.
ISO/IEC 27001	International information-security management standard; CSF Subcategories cross-reference ISO 27001 controls.
CIS Critical Security Controls	Prioritized, prescriptive safeguards that operationalize many CSF Subcategories.

Common Pitfalls & How to Avoid Them

Based on experience supporting CSF-aligned programs and federal authorizations, these are the issues that most often stall or weaken a CSF implementation:

1. Treating CSF as a checklist

The CSF is outcome-based, not a pass/fail control list. Copying another organization's Profile without doing your own risk assessment produces a program that looks complete but does not reflect your actual risk. Build your Target Profile from your mission and threat environment.

2. Skipping the Govern function

Teams often jump to technical controls under Protect and Detect and neglect Govern. Without executive-owned strategy, roles, and policy, improvements are inconsistent and unsustainable. In CSF 2.0, Govern comes first for a reason.

3. Setting Tiers too high

Higher Tiers are not automatically better. Targeting Tier 4 everywhere wastes resources on low-risk areas. Select Tiers per Function based on risk tolerance and mission — Tier 3 is a defensible target for most.

4. A Current Profile that isn't honest

A baseline built on optimistic self-assessment produces a gap analysis that hides real weaknesses. Validate the Current Profile with evidence — and ideally an independent assessor — before setting targets.

5. Ignoring supply-chain risk

CSF 2.0 elevates Cybersecurity Supply Chain Risk Management, yet many programs still scope it out. Third-party and software-supply-chain compromise is now a leading attack vector; include vendors and dependencies in scope.

6. Multi-vendor accountability gaps

Splitting infrastructure, monitoring, support, and compliance across many vendors creates finger-pointing and inheritance gaps. Bundled solutions provide single-source accountability across the Protect, Detect, Respond, and Recover functions.

CSF Implementation Checklist

Use this checklist to track progress through a CSF program cycle:

Phase 1: Govern & Scope

- ☐ Secure executive sponsorship and define cyber-risk roles and responsibilities
- ☐ Establish or update the organizational cybersecurity risk-management strategy and policy
- ☐ Identify mission/business objectives and the scope of systems and assets in play
- ☐ Select an infrastructure/hosting provider where controls can be inherited

Phase 2: Orient & Baseline

- ☐ Identify applicable laws, regulations, contractual, and insurance requirements
- ☐ Catalog related systems, assets, data flows, and third-party dependencies
- ☐ Identify threats and vulnerabilities relevant to the environment
- ☐ Document the Current Profile across all six Functions

Phase 3: Assess & Target

- ☐ Conduct a risk assessment (likelihood and impact of cyber events)
- ☐ Select target Implementation Tiers per Function
- ☐ Define the Target Profile based on risk, mission, and external requirements
- ☐ Validate the Current Profile with evidence or an independent assessor

Phase 4: Gap & Action Plan

- ☐ Compare Current and Target Profiles to identify gaps
- ☐ Prioritize gaps using cost-benefit and risk analysis
- ☐ Build a resourced, time-bound action plan
- ☐ Assign owners and milestones for each remediation item

Phase 5: Implement & Improve

- ☐ Execute the action plan and close prioritized gaps
- ☐ Inherit Protect / Detect / Respond / Recover capabilities from FedRAMP-authorized infrastructure
- ☐ Monitor outcomes and update Profiles as conditions change
- ☐ Re-run the cycle on a defined cadence and report status to leadership

How GovDataHosting Accelerates Your CSF Program

GovDataHosting provides a bundled, FedRAMP High (Class D) authorized cloud platform. Because the framework you must ultimately implement (NIST 800-53) is already operating at the infrastructure layer, most of your Protect, Detect, Respond, and Recover outcomes are pre-implemented and inheritable — letting your team focus CSF effort on the Govern and Identify work only your organization can do.

Single-Source Accountability

Instead of coordinating five or more vendors for infrastructure, security, monitoring, support, and disaster recovery, GovDataHosting bundles everything into one contract with one point of accountability — dramatically simplifying your scope, your Current Profile, and your inheritance documentation.

What's included	CSF benefit
FedRAMP High (Class D) authorized platform	400+ NIST 800-53 controls already implemented and independently assessed — inheritable across four CSF functions.
NIST 800-53 Rev 5 control implementations	Ready-made evidence and cross-reference mappings from controls to CSF Subcategories.
24×7 US-based Security Operations Center	Satisfies Detect and Respond outcomes with continuous monitoring and incident response.
Multi-zone backup & disaster recovery	Delivers Recover-function outcomes with tested restoration.
Dedicated compliance support staff	Helps document your Current and Target Profiles and close gaps faster.
US data centers, US citizen support	Supports supply-chain and personnel-security expectations under Govern and Identify.

Results Our Clients Achieve

- **40% faster authorization timelines** through control inheritance and documentation support.
- **10–40% cost savings** compared with a self-managed multi-vendor cloud approach.
- **300+ inherited controls** reducing Profile documentation burden by hundreds of hours.
- **100% client retention** demonstrating long-term partnership value.

Next Steps

Ready to build or mature a CSF-based cybersecurity program? Here is how to get started:

FREE CSF READINESS ASSESSMENT

We will help you define your scope, draft an initial Current Profile, and identify the fastest path to your Target Profile — including which outcomes you can inherit from FedRAMP High infrastructure.

Additional Resources

Explore these companion guides to support your compliance journey:

- **Complete FISMA Authorization Guide** — the seven-step RMF path to a federal Authorization to Operate.
- **NIST 800-53 Rev 5 Control Matrix** — complete control mapping with implementation guidance.
- **FedRAMP Migration Playbook** — step-by-step guide to leveraging FedRAMP authorization.