



NIST Cybersecurity Framework 2.0

NIST CSF 2.0 (26 Feb 2024) | Core (Functions, Categories, Subcategories), Tiers, Profiles, online resources

#CSF

#CybersecurityFramework

#Governance

#RiskManagement

What CSF 2.0 is

Source

NIST CSWP 29 (Cybersecurity White Paper 29), **The NIST Cybersecurity Framework (CSF) 2.0**, published 26 February 2024. Voluntary, outcome-based, technology-neutral. Replaces CSF 1.1 (April 2018). Applies to **all organizations** of any size or sector, not only US critical infrastructure. The Core describes **outcomes**, not how to achieve them.

6

Functions

GV, ID, PR, DE, RS, RC

22

Categories

two-letter ids, e.g. GV.SC

106

Subcategories

e.g. PR.AA-01

4

Tiers

Partial to Adaptive

Function — Highest level of the Core; the six Functions are an organized view of the risk management lifecycle, not a sequence.

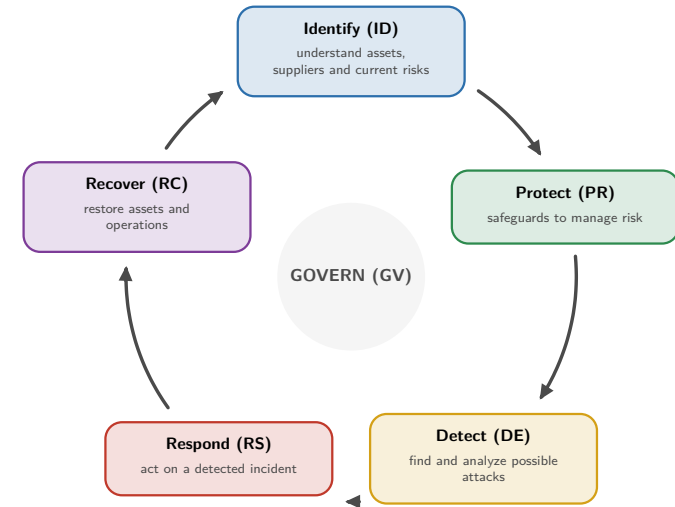
Category — Group of related outcomes inside a Function (GV.SC = Govern / Cybersecurity Supply Chain Risk Management).

Subcategory — Specific technical or management outcome (PR.AA-03 = users, services and hardware are authenticated). Identifier = Function.Category-NN.

Informative Reference — Online mapping from a Subcategory to standards and controls (SP 800-53r5, ISO/IEC 27001, CIS Controls, COBIT). Maintained in the CPRT (Cybersecurity and Privacy Reference Tool, csrc.nist.gov/projects/cprt), not in the PDF.

Implementation Example — New in 2.0: concise, action-oriented illustrations of how a Subcategory can be achieved. Not exhaustive, not a checklist.

The six Functions



Govern is the 2.0 addition and sits at the centre: it sets strategy, expectations and policy that inform how the other five Functions are prioritized. Govern also absorbed the supply chain category (ID.SC in 1.1 became GV.SC). Identify, Protect and Detect outcomes happen continuously; Respond and Recover activate when an incident occurs.

Mnemonic: **GIPDRR**

G Govern context, strategy, roles, policy, oversight, supply chain

I Identify asset management, risk assessment, improvement

P Protect identity and access, awareness, data, platform, resilience

D Detect continuous monitoring, adverse event analysis

R Respond management, analysis, communication, mitigation

R Recover recovery plan execution, recovery communication

EXAM TIP

Trap: CSF 1.1 had **5 Functions, 23 Categories, 108 Subcategories**; CSF 2.0 has **6 / 22 / 106**. Fewer categories despite a new Function because Business Environment, Governance and Supply Chain were consolidated under Govern, and Improvement (ID.IM) merged the old PR.IP, RS.IM and RC.IM.

Core: Categories by Function

■ GOVERN (GV) strategy, expectations and policy set, communicated, monitored

- GV.OC Organizational Context
 - mission, stakeholders, dependencies, legal and contractual duties understood
- GV.RM Risk Management Strategy
 - priorities, constraints, risk appetite and tolerance set and used
- GV.RR Roles, Responsibilities, Authorities
 - leadership accountable; roles, resources, HR practices
- GV.PO Policy
 - policy established, communicated, enforced, reviewed
- GV.OV Oversight
 - results of risk activities used to adjust the strategy
- GV.SC Cybersecurity Supply Chain Risk Management
 - supplier program, contracts, due diligence, exit (10 outcomes)

■ IDENTIFY (ID) current cybersecurity risks are understood

- ID.AM Asset Management
 - hardware, software, services, data and flows inventoried and prioritized
- ID.RA Risk Assessment
 - vulnerabilities, threats, likelihood, impact, responses, supplier checks
- ID.IM Improvement
 - lessons from audits, tests, exercises, operations; plans kept current

■ PROTECT (PR) safeguards to manage risk are used

- PR.AA Identity Management, Authentication, Access Control
 - identities proofed, authenticated; least privilege; physical access
- PR.AT Awareness and Training
 - all staff and specialized roles trained
- PR.DS Data Security
 - data at rest, in transit, in use protected; backups tested
- PR.PS Platform Security
 - configuration, patching, logging, allowlisting, secure development
- PR.IR Technology Infrastructure Resilience
 - segmentation, environmental protection, redundancy, capacity

■ DETECT (DE) possible attacks and compromises found and analyzed

- DE.CM Continuous Monitoring
 - networks, physical sites, people, providers, endpoints monitored
- DE.AE Adverse Event Analysis
 - events analyzed, correlated, scoped; incidents declared on criteria

■ RESPOND (RS) action taken on a detected incident

- RS.MA Incident Management
 - IR plan executed; triage, prioritize, escalate
- RS.AN Incident Analysis

- root cause, evidence integrity, magnitude

- RS.CO Incident Response Reporting and Communication
 - stakeholders notified, information shared
- RS.MI Incident Mitigation
 - incidents contained and eradicated

■ RECOVER (RC) affected assets and operations restored

- RC.RP Incident Recovery Plan Execution
 - backups verified, services restored, end of recovery declared
- RC.CO Incident Recovery Communication
 - progress and public updates communicated

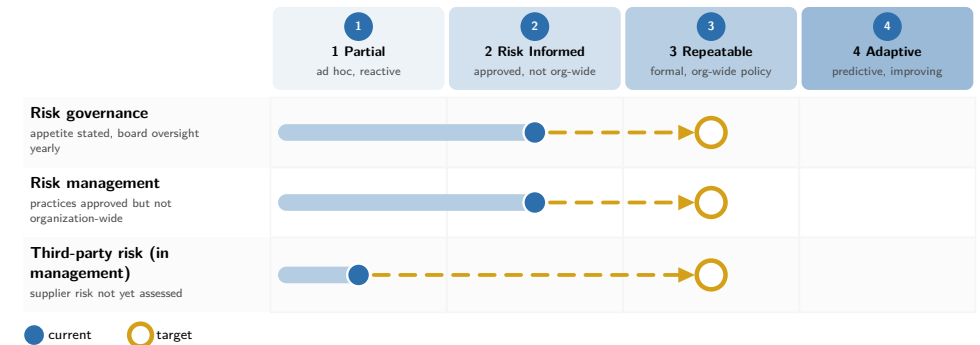
NOTE

Every one of the 106 Subcategories, with what it requires and the evidence an assessor asks for, is listed in the sheet “CSF 2.0 Core: the 106 Outcomes Explained”.

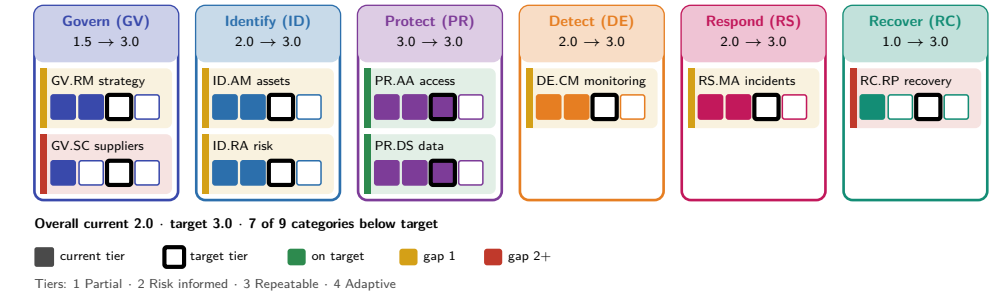
EXAMPLE

Reading an identifier: PR.DS-02 = Function PR (Protect), Category DS (Data Security), Subcategory 02 ("the confidentiality, integrity, and availability of data-in-transit are protected"). Informative Reference in the CPRT: SP 800-53r5 SC-8 Transmission Confidentiality and Integrity.

Tiers: how mature is your risk governance?



CSF Tiers (Appendix B) rate two dimensions separately: cybersecurity risk governance (how risk decisions are set and overseen) and cybersecurity risk management (how practices are run, including third-party risk). Dots = current Tier, rings = target (illustrative mid-size company)



Worked example (illustrative, 400-bed hospital): Tier reached per Category in the Current Profile (filled squares) against the Target Profile (outline). CSF 2.0 defines Tiers for the whole organization; scoring them per Category is a common practice that shows where rigor is missing (here Recover: backups exist but restores are never tested, and supplier risk is unmanaged)

❌ **Classic mistake: averaging Tiers into one score**

Reporting "we are Tier 2.2" hides the Function that fails. A Tier 1 Recover (untested backups) is what turns a ransomware intrusion into weeks of outage, even with Tier 3 Protect. Report the weakest Function and its gap action, not a mean.

⚠️ **WARNING**

Tiers are **not** maturity levels to be maximized and **not** a certification. NIST says to pick the Tier that fits the risk, budget and mission; Tier 3 is a common target, Tier 4 is justified only where the risk warrants it. A Tier is chosen for the Current Profile and the Target Profile.

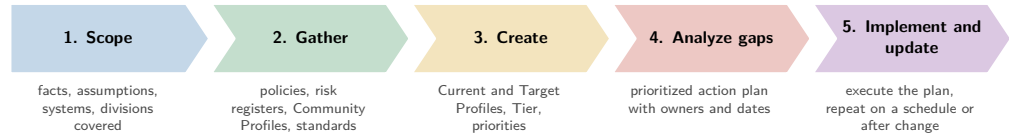
Profiles

Organizational Profile

Description of an organization's current and/or target cybersecurity posture in terms of Core outcomes. **Current Profile** = outcomes being achieved now and how. **Target Profile** = desired outcomes, prioritized from mission, risk appetite, regulations and threat intelligence.

Community Profile

Baseline of CSF outcomes created and published for a group with shared interests: a sector (water, health, elections), a technology (cloud, AI, PNT: positioning, navigation and timing), a threat (ransomware), a regulation. An organization uses it as the starting point for its own Target Profile. NIST publishes them at nist.gov/cyberframework/profiles.



Creating and using an Organizational Profile (CSF 2.0 section 3.1)

Profile column	Content
Subcategory	the 106 outcomes, plus any organization-specific ones
Current state	achieved / partially / not, with evidence
Target state and priority	desired state, rationale, High/Medium/Low
Informative References	controls that implement it (SP 800-53, ISO 27001, CIS)
Gaps and actions	owner, resources, deadline, how to measure

Subcategory	Current	Target	Priority	Action (owner, date)
ID.AM-01 hardware inventory maintained	partial	achieved	High	deploy agent-based inventory, OT passive discovery (IT ops, Q1)
PR.AA-03 users, services, hardware authenticated	partial	achieved	High	phishing-resistant MFA for admins and VPN (IAM, Q2)
DE.CM-01 networks monitored	not	partial	Medium	managed detection service for IT, OT later (SOC, Q3)
RC.RP-03 backup integrity verified before restore	not	achieved	High	quarterly restore test with malware scan (IT ops, Q1)
GV.SC-08 suppliers in incident planning	not	partial	Low	add notification clauses at contract renewal (procurement, Q4)

Worked excerpt of an Organizational Profile for a 400-person manufacturer, using the columns above (illustrative states and actions; subcategory wording shortened from the CSF 2.0 Core). High-priority gaps become the funded action plan

👤 Risk communication and integration (CSF section 5)

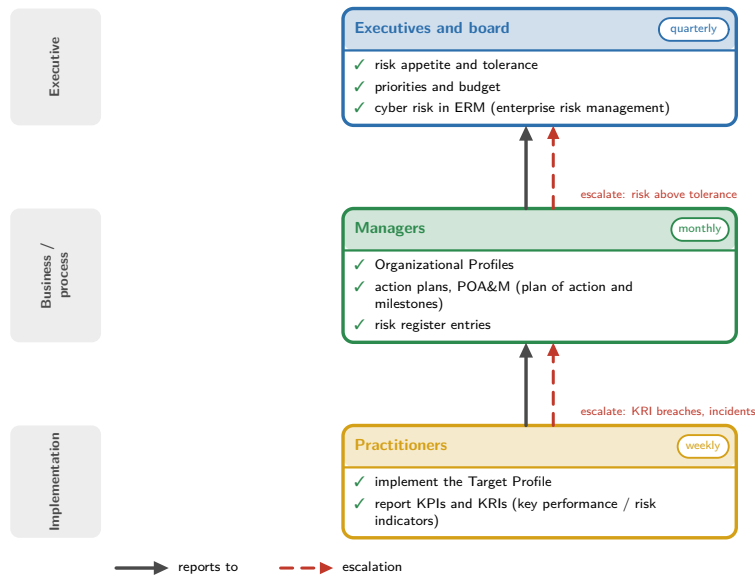


Figure 5 of CSF 2.0 as a governance chain: priorities and resources flow down, status and risk indicators flow up; a risk outside tolerance escalates to the level that owns the appetite (cadences are typical, not prescribed)

Responses to negative risk	Responses to positive risk (opportunity)
Mitigate: reduce likelihood or impact with safeguards	Realize: pursue the opportunity
Transfer: insurance, contracts	Share: with partners
Avoid: stop the risky activity	Enhance: increase its likelihood or benefit
Accept: within the stated tolerance	Accept: take it if it happens

- **NIST IR 8286 (ERM integration)** how cyber risk registers roll up into the enterprise risk register
- **IR 8286A / 8286B** identifying and estimating cyber risk; prioritizing it for ERM
- **IR 8286C / 8286D** staging risks for governance oversight; using business impact analysis (BIA) to prioritize
- **SP 800-221 / 800-221A** ICT (information and communications technology) risk in the enterprise risk portfolio; ICT risk outcomes



TIP

GV.RM-07 (strategic opportunities, i.e. positive risks, are included in risk discussions) is the Subcategory that lets a CISO argue for security as an enabler: for example, a strong SOC 2 report opens a regulated market.

🔄 1.1 to 2.0: what changed

CSF 1.1 (2018)	CSF 2.0 (2024)
Scope: US critical infrastructure	All organizations, all sectors, worldwide
5 Functions	6 Functions: Govern added, cross-cutting
23 Categories / 108 Subcategories	22 Categories / 106 Subcategories

Supply chain under ID.SC

Improvement scattered (PR.IP, RS.IM, RC.IM)
Informative References in the PDF

Profiles described informally

Few implementation aids

GV.SC with 10 subcategories; ID.RA-10 supplier assessment

Single ID.IM Improvement category

Online CPRT with references and Implementation Examples

Organizational and Community Profiles, template, 5-step process

Quick Start Guides (small business, C-SCRM, ERM, Tiers, Profiles)

🔍 CSF 2.0 Reference Tool

Browse and export the Core (JSON, Excel) with Implementation Examples and Informative References.

🔗 CPRT

Cybersecurity and Privacy Reference Tool: machine-readable mappings between CSF, SP 800-53r5, SP 800-171, Privacy Framework.

📖 Quick Start Guides

Short guides: Small Business, Creating Profiles, Tiers, C-SCRM (cybersecurity supply chain risk management), Enterprise Risk Management (ERM, NIST IR 8286).

🌐 Using CSF in practice and in regulation

NIS2 (Dir. 2022/2555) Art. 21(2) minimum measure	CSF 2.0 outcomes that implement it
(a) risk analysis and information system security policies	GV.PO, GV.RM, ID.RA
(b) incident handling	DE.AE, RS.MA to RS.MI
(c) business continuity, backup management, disaster recovery, crisis management	PR.DS-11, PR.IR-03, RC.RP
(d) supply chain security, incl. direct suppliers	GV.SC-01 to GV.SC-10, ID.RA-10
(e) security in acquisition, development and maintenance, incl. vulnerability handling and disclosure	PR.PS-02, PR.PS-06, ID.RA-01, ID.RA-08
(f) policies to assess the effectiveness of measures	GV.OV-03, ID.IM-01
(g) basic cyber hygiene and cybersecurity training	PR.AT-01, PR.AT-02, PR.PS-01
(h) cryptography and, where appropriate, encryption	PR.DS-01, PR.DS-02
(i) human resources security, access control, asset management	GV.RR-04, PR.AA-05, ID.AM-01 to 08
(j) MFA or continuous authentication, secured voice, video, text and emergency communications	PR.AA-03, PR.DS-02
Art. 20: management bodies approve measures, oversee them, follow training	GV.RR-01, GV.OV-01, PR.AT-02

Regulation or standard	Where CSF 2.0 fits
DORA (Reg. 2022/2554, Digital Operational Resilience Act, EU financial sector)	ICT risk management framework (Art. 6-16) mirrors the six Functions: identification (Art. 8) = ID, protection (Art. 9) = PR, detection (Art. 10) = DE, response and recovery (Art. 11) = RS, RC; ICT third-party risk (Art. 28-30) = GV.SC
ISO/IEC 27001:2022	Informative Reference for every Subcategory; ISMS clauses 4-10 align with Govern
SP 800-53r5 / RMF	CSF is the outcome layer, 800-53 the control catalogue, RMF (SP 800-37r2) the process
Privacy Framework 1.0	Same structure (Functions-Categories-Subcategories); Protect-P overlaps PR, DE, RS, RC
NIST IR 8286 series	Integrates CSF outcomes into Enterprise Risk Management (risk registers, risk detail records)

Requirement	SP 800-53r5	ISO 27001:2022 Annex A	CIS Controls v8.1
ID.AM-01 hardware inventory every managed device is listed and kept current	CM-8	A.5.9	1.1
ID.AM-02 software inventory installed software and services are listed	CM-8	A.5.9	2.1
ID.RA-01 vulnerabilities found assets are scanned, weaknesses recorded	RA-5	A.8.8	7.1
PR.AA-03 authentication users and services authenticated, MFA for remote and admin	IA-2	A.8.5	6.3-6.5
PR.AA-05 least privilege permissions granted, reviewed and revoked by role	AC-2, AC-6	A.5.15, A.8.2	6.8
PR.AT-01 awareness all staff trained on cyber risks	AT-2	A.6.3	14.1
PR.DS-11 backups created, protected, maintained and tested	CP-9	A.8.13	11.2-11.5
PR.PS-04 logging log records generated for continuous monitoring	AU-2, AU-12	A.8.15	8.2
DE.CM-01 network monitoring networks watched for adverse events	SI-4	A.8.16	13.3
RS.MA-01 run the IR plan plan executed with third parties once declared	IR-4, IR-8	A.5.26	17.4
GV.SC-05 supplier contracts security requirements written into contracts	SA-4, SR-3	A.5.20	15.4

Same outcome, three reference sets: one piece of evidence can answer all four frameworks (control ids as published in the CPRT and each standard; confirm the full mapping in the CSF 2.0 Reference Tool)

Minimum steps for a first CSF 2.0 assessment

✓ baseline / mandatory □ recommended – verify in your context

- ✓ Get leadership to state risk appetite and tolerance (GV.RM-02)
- ✓ Inventory hardware, software, services and data flows (ID.AM-01/02/03/07)
- ✓ Score all 106 Subcategories for the Current Profile with evidence

- **SHOULD** Start the Target Profile from a Community Profile for your sector
- **SHOULD** Map each Target gap to SP 800-53r5 or ISO 27001 controls through the CPRT
- **SHOULD** Choose a Tier for governance and for management separately
- **COULD** Re-run the Profile yearly and after major incidents or acquisitions

Q1

Which CSF 2.0 Function contains supply chain risk management?

A

Govern: category GV.SC (10 subcategories). In 1.1 it was ID.SC.

Q2

What is a Community Profile?

A

A published baseline of CSF outcomes for a sector, technology, threat or use case; used as the basis for an organization's Target Profile.

Q3

How many Functions, Categories and Subcategories in CSF 2.0?

A

6 Functions, 22 Categories, 106 Subcategories.

Q4

Name the four Tiers.

A

Tier 1 Partial, Tier 2 Risk Informed, Tier 3 Repeatable, Tier 4 Adaptive.

Q5

Where are the Informative References published?

A

Online only, in the CSF 2.0 Reference Tool and the CPRT; they are no longer in the framework document.

Q6

Which Functions run continuously and which are event-driven?

A

Govern, Identify, Protect, Detect run continuously; Respond and Recover activate on an incident.

Core in numbers and 1.1 relocations

Function	1	2	3	4	5	6
GV (31)	OC 5	RM 7	RR 4	PO 2	OV 3	SC 10
ID (21)	AM 7	RA 10	IM 4			
PR (22)	AA 6	AT 2	DS 4	PS 6	IR 4	
DE (11)	CM 5	AE 6				
RS (13)	MA 5	AN 4	CO 2	MI 2		
RC (8)	RP 6	CO 2				

Subcategories per Category (CSF 2.0 Appendix A) →

Ids are not contiguous: numbers of relocated 1.1 Subcategories are skipped (DE.AE has 02, 03, 04, 06, 07, 08). GV.SC and ID.RA are the largest categories. A legacy format similar to CSF 1.1 of the Core exists in the Reference Tool: use it to migrate a 1.1 Profile rather than remapping by hand.

CSF 1.1 category	Where it went in 2.0
ID.BE Business Environment	GV.OC Organizational Context
ID.GV Governance	GV.PO, GV.RR, GV.OV, GV.OC
ID.RM Risk Management Strategy	GV.RM
ID.SC Supply Chain Risk Management	GV.SC (10 subcategories)
PR.AC Identity Management and Access Control	PR.AA

PR.IP Information Protection Processes	ID.IM, PR.PS, PR.DS-11 (backups)
PR.PT Protective Technology, PR.MA Maintenance	PR.PS Platform Security, PR.IR Infrastructure Resilience
RS.IM, RC.IM Improvements	ID.IM Improvement
RS.RP Response Planning, DE.DP Detection Processes	folded into RS.MA, DE.AE and ID.IM