anchor@anchor-cyber:~$ man nist-csf-2.0

ANCHOR CYBER SECURITY LLC

NIST CSF 2.0 — Field Reference

The functions, categories, tiers, and profile vocabulary you actually need mid-engagement — plus Anchor's own trust-but-verify audit loop, condensed.

$ csf --glossary

Vocabulary / 6 terms

Function	Top-level bucket of cybersecurity outcomes. There are 6: GOVERN, IDENTIFY, PROTECT, DETECT, RESPOND, RECOVER — all run concurrently, none is sequential.
Category	A named group of related outcomes within a Function. 22 total across the Core.
Subcategory	A specific, testable outcome statement. 106 total — the actual unit you rate as Implemented / Partial / Not Implemented.
Informative Ref.	A pointer from a Subcategory to an external control (SP 800-53, ISO 27001, CIS Controls) that would satisfy it.
Profile	A snapshot of which Subcategory outcomes matter and how well they're met, for one specific organization.
Tier	How systematic and risk-informed the org's cybersecurity governance process is — not a per-control maturity score.

$ csf --functions

The Six Functions / 22 categories · 106 subcategories

GV
Govern

Strategy, risk appetite, roles, policy, oversight, and supply chain risk. Informs the other five.

cat **6** sub **31**

ID
Identify

Know your assets, your risks, and where last time's fixes need following up.

cat **3** sub **21**

PR
Protect

Access control, training, data security, platform hardening, infra resilience.

cat **5** sub **22**

DE
Detect

Continuous monitoring and analysis of adverse events as they happen.

cat **2** sub **11**

RS
Respond

Manage, analyze, report on, and mitigate an incident once it's confirmed.

cat **4** sub **13**

RC
Recover

Execute and communicate the plan to restore capabilities and services.

cat **2** sub **8**

```
$ csf --categories -l
```

Category Map

CODE	CATEGORY	SUBCATS
GOVERN — GV		
GV.OC	Organizational Context	5
GV.RM	Risk Management Strategy	7
GV.RR	Roles, Responsibilities, and Authorities	4
GV.PO	Policy	2
GV.OV	Oversight	3
GV.SC	Cybersecurity Supply Chain Risk Management	10
IDENTIFY — ID		
ID.AM	Asset Management	7
ID.RA	Risk Assessment	10
ID.IM	Improvement	4
PROTECT — PR		
PR.AA	Identity Management, Authentication, and Access Control	6
PR.AT	Awareness and Training	2
PR.DS	Data Security	4
PR.PS	Platform Security	6
PR.IR	Technology Infrastructure Resilience	4
DETECT — DE		
DE.CM	Continuous Monitoring	5
DE.AE	Adverse Event Analysis	6
RESPOND — RS		
RS.MA	Incident Management	5
RS.AN	Incident Analysis	4
RS.CO	Incident Response Reporting and Communication	2
RS.MI	Incident Mitigation	2
RECOVER — RC		
RC.RP	Incident Recovery Plan Execution	6

CODE	CATEGORY	SUBCATS
RC.CO	Incident Recovery Communication	2

$ csf --tiers

Implementation Tiers / governance maturity, not a per-control score

01	Partial	Ad hoc, reactive. Little org-wide awareness of cyber risk; no formal process.
02	Risk Informed	Management approves practices, but they aren't yet organization-wide policy. Application is inconsistent.
03	Repeatable	Formally approved, written as policy, consistently applied, and updated as the threat landscape changes.
04	Adaptive	Adapts from lessons learned and predictive/real-time indicators. Risk management is cultural, not procedural.

$ csf --profile --diff

Current vs. Target Profile

CURRENT

What the organization actually does today, Subcategory by Subcategory — evidence-backed, not aspirational.

TARGET

What should be true given mission, risk appetite, and obligations. Prioritized Low/Med/High — SP 1301 calls prioritization "the defining feature of a Profile."

$ anchor-audit --run

Anchor's Trust-but-Verify Loop

/ condensed from our internal audit methodology

01 **Independent access.**
Your own read access to the real systems — never the client's script output alone.

02 **Rebuild the asset inventory.**
From the live system, not from the org's own description of itself.

03 **Verify each Subcategory rating.**
Code review AND a live-behavior test — a policy that exists isn't the same as a policy that works.

04 **Independent risk scoring.**
Score before reading theirs. Reconcile after.

05 **Collect what fieldwork can't produce from a repo.**
Signed contracts, console configs, insurance policies — get the originals.

06 **Resolve legal exposure empirically.**
Don't ask if PHI/PII touched an unauthorized system — check.

07 **Delta report, not adoption.**
Diff your findings against any self-assessment; never just co-sign it.

08 **Re-verify remediation before closing it.**
"Done" gets tested in production, by you, not taken on faith.

src: csf-2.0-core.json · NIST SP 1301/1302 · CSF 2.0 Implementation Examples (2024-02-26) exit 0