NIST CYBERSECURITY FRAMEWORK 2.0.

NIST published Cybersecurity Framework 2.0 on February 26, 2024, its first major update since 2014. It is a taxonomy of high-level cybersecurity outcomes for any organization, not a control set, a checklist or a certification: **CSF 2.0 says what good looks like and leaves the how to the standards it maps to.**

OUTCOMES, NOT CONTROLS | NO NIST CERTIFICATION | GOVERN JOINS THE CORE | 6 FUNCTIONS, 106 OUTCOMES

01 THE MECHANISM

A Taxonomy of Outcomes

The CSF Core is a hierarchy of Functions, Categories and Subcategories stating outcomes, not actions. NIST calls it a taxonomy any organization can use regardless of size, sector or maturity; it never prescribes the how. **Every Subcategory reads as a result, not a checklist item.** [01] [02]

Voluntary, Not Certified

NIST is not a regulator; most organizations adopt it voluntarily, though EO 13800 binds federal agencies. NIST certifies or endorses no CSF products, implementations or services and has no plans for a conformity assessment program. **A "CSF certified" badge is a third party's claim.** [07] [01]

Stable Core, Living Edges

The CSWP 29 document changes infrequently for stability; the references, examples and Quick Start Guides live online and update often. The Core covers IT, IoT and OT, plus cloud, mobile and AI. **Nothing newer than 2.0 exists in November 2026; growth is in the resources around it.** [01] [10] [06]

02 THE FLOW

How the Core Is Built STRUCTURE

1. **Six Functions:** Govern, Identify, Protect, Detect, Respond and Recover organize outcomes at the top level. Govern is new in 2.0 and sits at the center of the wheel because it informs how the other five are implemented; it also carries the cybersecurity supply chain category, GV.SC. [01] [03]
2. **22 Categories, 106 Subcategories:** each Function divides into Categories of related outcomes, and each Category into Subcategories such as PR.DS-11, "Backups of data are created, protected, maintained, and tested." Numbering gaps mark CSF 1.1 items relocated in 2.0. [01]
3. **Concurrent, not sequential:** the order and size of Functions imply no priority. Govern, Identify, Protect and Detect run continuously; Respond and Recover stay ready and act when an incident occurs. The outcomes are sector-, country- and technology-neutral by design. [01]

How an Organization Uses It PROFILE

1. **Scope and gather:** decide what the Organizational Profile covers (the whole enterprise, one system, one threat such as ransomware), then collect policies, risk priorities, BIA registers, requirements and current practices. An organization can keep as many Profiles as it needs. [01] [05]
2. **Build Current and Target Profiles:** the Current Profile records which outcomes are achieved and to what extent; the Target Profile records the outcomes selected and prioritized, often seeded from a Community Profile and shaped by the Tier that leadership chose. [01] [05] [04]
3. **Close the gap, then repeat:** compare the two Profiles, write a prioritized action plan (risk register, POA&M), follow Informative References and Implementation Examples to choose practices, implement, update the Profile and run the cycle again. [01] [05]

03 THE SIX FUNCTIONS

FUNCTION	OUTCOME IT STATES
GV Govern	Strategy, expectations and policy are established, communicated and monitored; six Categories, one on suppliers.
ID Identify	Current cybersecurity risks are understood: asset management, risk assessment and improvement across all Functions.
PR Protect	Safeguards are used: identity and access, awareness and training, data security, platform security and resilience.
DE Detect	Possible attacks and compromises are found and analyzed through continuous monitoring and adverse event analysis.
RS Respond	Actions regarding a detected incident are taken: management, analysis, reporting and communication, mitigation.
RC Recover	Assets and operations affected by an incident are restored: recovery plan execution and recovery communication.

04 THE FOUR TIERS COMPARED

TIER	RISK POLICY ORG-WIDE?	WHAT IT LOOKS LIKE
T1: Partial	No	Strategy applied ad hoc with ad hoc priorities; limited risk awareness; irregular, case-by-case management; supplier risk unknown.
T2: Risk Informed	No	Management approves practices, but not as organization-wide policy; risk assessments not repeatable; supplier risk known, not acted on.
T3: Repeatable	Yes	Practices formally approved as policy, implemented and reviewed; consistent methods track changing risk; executives confer regularly.
T4: Adaptive	Yes	Practices adapt from lessons learned and predictive indicators; executives weigh cyber risk with financial risk; live supplier data.

CONTINUED ON SHEET 2 →

NIST CSF 2.0. GOVERN · PROFILE · TIER

05 PROGRAM OPERATIONS

Pick Tiers at the right altitude. Leadership selects Tiers, usually overall or per Function or Category rather than per Subcategory, weighing threat environment, legal requirements, supply chain needs and resources. Reuse the Appendix B descriptions, customize them or use your own. [04] [01]

Seed the Target Profile from a Community Profile. NIST and partners publish baselines for sectors, technologies and threats; the Ransomware (IR 8374r1), Incident Response (SP 800-61r3), Manufacturing, Semiconductor, PNT, AI and Transit profiles are examples. Copy one, then tailor it. [01] [09] [10]

Use the Reference Tool, then export. The CSF 2.0 Reference Tool filters Core outcomes with their Implementation Examples and Informative References and exports to Excel or JSON; the NIST template spreadsheet sets Current and Target Profiles side by side for gap analysis. [06] [09] [05]

Treat mappings as pointers, not proof. NIST runs only limited conformance testing on OLIR submissions against IR 8278Ar1, does no correctness testing of non-NIST mappings, and lists them without endorsement after a 30-day comment period. Read the mapped clause before claiming coverage. [08] [06]

06 CONTROL MAPPING

SP 800-53 & THE RMF

The CSF names outcomes; SP 800-53 supplies a control catalog that NIST calls distinct but complementary. CSF 2.0 can complement the RMF's selection and prioritization of SP 800-53 controls, and an SP 800-53 Rev 5.2.0 mapping and an SP 800-171 Rev 3 mapping both sit in the OLIR catalog. [07] [01] [08]

ISO 27001 & CIS CONTROLS

Both appear as Informative References: ISO/IEC 27001:2022 and CIS Controls v8.1 were among seven new CSF 2.0 mappings NIST published in the year to February 2026. A mapped control is one way to reach an outcome, not the only way, and a single reference may cover only part of a Subcategory or span many of them. [10] [08] [01]

PCI DSS & SECTOR PROFILES

A PCI DSS 4.0.1 mapping is in the catalog, and Community Profiles carry the CSF into sectors: the CRI Profile 2.0 and the Cloud Controls Matrix 4.0 map to CSF 2.0, and NIST publishes or drafts Profiles for ransomware, incident response, manufacturing, semiconductors, positioning and timing, AI and transit. [08] [10] [09]

ERM & GOVERNANCE

Govern exists to put cybersecurity inside enterprise risk management: GV.RM-03 asks that cyber risk activities join ERM processes, GV.RR-01 makes leadership accountable, and GV.OV reviews strategy against results. The ERM Quick Start Guide and the IR 8286 series carry that link; board metrics belong to their own brief. [01] [03]

07 WHAT THIS DOES NOT SOLVE

Not a Control Set

It states outcomes and links out for the how. **No Subcategory tells you which control to deploy.** [01]

Not a Certification

NIST certifies no products, implementations or services, **and plans no conformity assessment program.** [07]

Not a Maturity Score

Tiers describe rigor; **higher Tiers are urged only when risk, mandate or cost-benefit justifies it.** [01] [04]

Not Self-Sufficient

NIST says pair it with other standards and practices; **it organizes risk, it does not implement security.** [01]

08 MYTHS VS. REALITY

MYTH	REALITY
"CSF 2.0 is only for critical infrastructure."	The 2.0 title drops "Critical Infrastructure"; **NIST aims it at all organizations of any size and sector.** [01] [07]
"We can get NIST CSF certified."	**NIST offers no certification, endorsement or conformity program.** Any badge is a third party's own. [07]
"Tier 4 Adaptive is the goal for everyone."	Tiers set tone, not targets; **progress is urged when risks or mandates grow or a cost-benefit case holds.** [01] [04]
"Implementation Examples are the required baseline."	They are notional, action-oriented illustrations; **neither exhaustive nor a baseline of required actions.** [01]
"An OLIR mapping means NIST vetted the match."	NIST checks format against IR 8278Ar1 only; **non-NIST mappings get no correctness test or endorsement.** [08] [06]

09 SPEAK THE PROGRAM — KEY TERMS

CSF CORE
The taxonomy of outcomes: **6 Functions, 22 Categories, 106 Subcategories** in Appendix A.

ORGANIZATIONAL PROFILE
Current and/or target posture **in terms of the Core's outcomes**; scoped as you choose.

COMMUNITY PROFILE
Published **outcome baseline for a sector, technology or threat**; seeds a Target Profile.

TIER
Characterizes **the rigor of governance and management practices**, Partial to Adaptive.

INFORMATIVE REFERENCE
Links a Core outcome to **an existing standard, guideline or regulation**; NIST or others.

IMPLEMENTATION EXAMPLE
A **concise, notional, action-oriented step** toward an outcome; never a required baseline.

SOURCES: NIST CSWP 29: THE NIST CSF 2.0 · NIST CSF FAQS · SP 1302: USING THE CSF TIERS · SP 1301: ORGANIZATIONAL PROFILES