PRESCIENT SECURITY

NIST CSF 2.0:
Understanding the 6 Functions & Organizational Profiles

CSF 2.0 (NIST CSWP 29) updates the industry-standard cybersecurity framework to address modern risk landscapes. The updated framework expands beyond critical infrastructure to apply universally to all organizations, it doesn't matter what size, sector, or maturity level.

CSF 2.0 introduces "Govern" as an overarching sixth function, and elevates supply chain risk management, as well as formalizes organizational profiles to help security leaders align cybersecurity investments with strategic business objectives.

Here is what has changed:

- **From 5 Functions to 6:** The addition of "Govern" (GV) places governance, enterprise risk strategy, and supply chain at the center of cyber decision-making.
- **Universal scope:** Framework guidance is expanded beyond critical infrastructure to cover tech startups, cloud SaaS, enterprises, and small-to-midsize businesses.
- **Organizational Profiles replace pass/fail:** Security posture is uplifted through tailored current state and target state profiles (NIST SP 1301). Implementation tiers are an optional mechanism to characterize the rigor of an organization's cybersecurity risk management practices.
- **Actionable Implementation Examples:** NIST provides curated, outcome-specific guidance to streamline mapping against ISO 27001, SOC 2, and NIST SP 800-53.

The 6 functions at a glance

Function	Subcategory scope	Core focus	Best fit	Primary deliverable
GOVERN (GV)	6 Categories 31 Subcategories	Strategy, risk tolerance, cybersecurity policies & supply chain oversight	Executive leadership, CISOs, board reporting, and legal teams	Cybersecurity Governance Charter & Supply Chain Risk Strategy
IDENTIFY (ID)	3 Categories 21 Subcategories	Asset discovery, threat environment, risk assessment & improvement planning	Enterprise architecture, asset management, and risk teams	Integrated Asset Inventory & Risk Assessment Register
PROTECT (PR)	5 Categories 22 Subcategories	dentity management, data protection, access control & workforce awareness	SecOps, IAM teams, infrastructure engineering, and IT	Zero Trust IAM Policies & Data Protection Baselines
DETECT (DE)	2 Categories 11 Subcategories	Continuous monitoring, anomaly detection, threat hunting & telemetry analysis	SOC analysts, MDR providers, and threat intelligence teams	Continuous Monitoring Architecture & Alert Playbooks
RESPOND (RS)	4 Categories 13 Subcategories	Incident management, analysis, containment, reporting & external coordination	Incident response teams, SecOps, and communications leads	Tested Incident Response Plan & Tabletop Exercises
RECOVER (RC)	2 Categories 8 Subcategories	Incident recovery, restoration planning, business continuity & lessons learned	Disaster recovery leads, business continuity, and sysadmins	Business Continuity / Disaster Recovery (BC/DR) Plan

How to think about each implementation tier

Tier 1: Partial

Cybersecurity risk management is informal, reactive, and localized.

- Risk is addressed on an ad-hoc basis with limited organizational awareness.
- No formal enterprise-wide risk management strategy or supply chain review.
- Best fit: Early-stage discovery baseline to identify immediate security deficiencies.

Tier 2: Risk-Informed

Management approves cybersecurity practices, but processes are not enterprise-wide.

- Awareness of risk exists, but policies are inconsistently implemented across departments.
- Tooling and controls exist but lack automated telemetry or continuous validation.
- Best fit: Growing organizations transitioning from informal to structured security.

Tier 3: Repeatable

Processes are formally approved, documented, and consistently executed organization-wide.

- Policies and procedures are regularly updated based on risk reviews and threat intelligence.
- Personnel are fully trained; cross-functional teams execute coordinated responses.
- Best fit: Mature commercial SaaS and enterprise vendors seeking third-party attestation.

Tier 4: Adaptive

Cybersecurity practices are continuously adapted based on predictive indicators and lessons learned.

- Risk-informed continuous monitoring and automated defensive response mechanisms.
- Deep supply chain integration and real-time collaboration with external security ecosystems.
- Best fit: High-assurance environments, federal suppliers, and critical infrastructure leaders.

What makes the implementation tiers different

Evaluation Dimension	Tier 1 (Partial)	Tier 2 (Risk-Informed)	Tier 3 (Repeatable)	Tier 4 (Adaptive)
Risk Management Process	Ad-hoc / Reactive	Approved, but siloed	Organization-wide policy	Continuously improving / Predictive
Integrated Risk Program	None / Isolated	Informal coordination	Enterprise-wide integration	Culture of proactive risk adaptation
Supply Chain Risk (C-SCRM)	Unassessed	Vendor awareness	Formal vendor evaluations	Real-time supply chain monitoring
Evidence & Validation	Narrative / Unstructured	Periodic manual checks	Documented + automated evidence	Machine-readable, continuous metrics
Third-Party Attestation	Baseline Gap Report	Maturity Roadmap	Target Attestation Letter	Advanced Maturity Attestation

Why customers choose Prescient Security

- We deliver structured gap analyses, target state profiles, and independent Attestation Letters accepted by enterprise buyers.
- We try to leverage your existing audit evidence to populate CSF 2.0 subcategories without extra data collection.
- We validate control effectiveness through using automated and clear maturity scoring and engineering-level remediation roadmaps.

Technical Guidance Callout: NIST does not issue "NIST CSF 2.0 Certifications." CSF 2.0 compliance is formally proven through third-party maturity assessments, documented organizational profiles, and independent Attestation Letters.