Apptega

GUIDE

NIST

Cybersecurity Framework (CSF) v2.0

Compliance Guide

For organizations that need a practical, implementable path to adopt NIST CSF v2.0 and improve cybersecurity risk management

Current as of August 29, 2025

1. Introduction

This practical guide helps organizations become compliant with NIST CSF v2.0 by translating the six core functions—GOVERN, IDENTIFY, PROTECT, DETECT, RESPOND, RECOVER—into concrete actions, owners, parameters, measurable acceptance criteria, and auditable evidence. It focuses on execution rather than theory.

1A. Beginner Quick-Start (First 30—90 Days)

Days 1—15 — Stand-up

- Appoint: Executive Cyber Risk Owner, CISO/ISO, System/Asset Owners, Identity Owner, Network/Platform Owners, IR Lead, TPRM Lead.
- Define the authorization boundary and draft data/asset/workflow diagrams (on-prem, cloud, SaaS, OT/IoT).
- Publish Cyber Risk Appetite (loss events, tolerances) and a one-page Security Policy.
- Start an Evidence Register and Risk Register.
- Launch a Security Awareness baseline for all users.

Days 16—45: Implement & tailor

- Establish IAM with MFA for remote/admin; enable central logging/SIEM; deploy EDR/anti-malware; harden baselines; start vulnerability management; protect backups.
- Produce draft GOVERN/IDENTIFY/PROTECT narratives; document supply-chain roles and provider responsibilities.
- Approve incident response runbooks and contact trees; schedule a tabletop.

Days 46—90: Validate & evidence

- Populate the Evidence Register; run an IR tabletop and a restore test; complete initial self-assessment against this guide.
- Record gaps with owners/dates in the w; brief leadership; lock a 90-day rolling improvement plan.

2. Scope & Alignment

Scope. People, processes, information, technology (on-prem, cloud, SaaS, endpoints, OT/IoT), and third parties that create, receive, maintain, transmit, or can materially affect the confidentiality, integrity, or availability of scoped information/services.

Key definitions

- **Authorization boundary:** Components and trust zones managed to CSF v2.0.
- **Organization-defined parameters (ODPs):** Tailorable values (timeouts, thresholds, retention, SLAs) you set and enforce across controls.
- **Third-party scope:** Providers that handle or influence in-scope services or data (MSPs, MSSPs, cloud, SaaS, telecom, data processors).

OT/IoT considerations (if applicable). Define zones, owners, and allowable interfaces between IT and OT; document safety dependencies, vendor maintenance access, and compensating controls for legacy devices.

2A. Profiles & Implementation Tiers (Current vs. Target, Gap Closure)

Purpose. Use Profiles to describe current and target cybersecurity outcomes for the scope; use Implementation Tiers to describe risk management rigor.

Steps

1. **Current Profile:** List outcomes currently met (per Function/Category) with evidence links.
2. **Target Profile:** Select outcomes required by risk appetite, regulators, contracts.
3. **Gap analysis:** For each gap, assign owner, due date, milestones, and acceptance criteria; log in the Remediation Log.
4. **Tier selection (Partial → Risk-Informed → Repeatable → Adaptive):** Target a Tier per business unit/system; record Tier drivers (governance, ERM linkage, continuous improvement).
5. **Measure progress:** Re-evaluate Profiles/Tiers after incidents, major changes, and at least semiannually.

Acceptance Criteria. Profiles exist and are reviewed by leadership; each gap has an owner/date; a Tier is declared with rationale; progress reviews occur at least twice per year.

2B. Metrics (Optional, Organization-Defined)

Purpose. Provide simple, leadership-friendly metrics that quantify progress against your CSF Profile and Implementation Tier without claiming an official NIST score.

Minimal metrics

- **Outcome Coverage (%)** = met_applicable_outcomes ÷ applicable_outcomes × 100
- **Evidence Completeness (%)** = outcomes_with_current_evidence ÷ met_applicable_outcomes × 100
- **Tier Attainment (0–3)** = map Current Implementation Tier per in-scope unit (Partial=0, Risk-Informed=1, Repeatable=2, Adaptive=3)
- **Tier Delta** = Target Tier – Current Tier (per Function or unit)
- **Remediation Velocity** = POA&M items closed ÷ POA&M items opened (rolling 90 days)

Optional composite (for exec dashboards; keep transparent)

- **Function Scores:** For each Function (GOVERN, IDENTIFY, PROTECT, DETECT, RESPOND, RECOVER), use **Coverage × Evidence**
- **Risk-Weighted Score (0–100):** Σ(weight_function × function_score); document weights (e.g., GOVERN 15%, IDENTIFY 15%, PROTECT 30%, DETECT 15%, RESPOND 15%, RECOVER 10%)

Reporting cadence

- **Monthly:** Coverage, Evidence, Tier deltas, Remediation Velocity
- **Quarterly:** Re-validate weights; sample evidence; recalibrate outliers

Acceptance Criteria

- Metrics and formulas are documented and repeatable
- Function-level Coverage/Evidence meet targets; Tier deltas shrink quarter-over-quarter
- Any composite score is traceable to underlying outcomes and evidence

3. Standards & Practices (Mapped to NIST CSF v2.0 Functions)

For each family: Intent • Minimums • Implement (Procedural/Technical/Contractual) • Evidence • Acceptance Criteria • Common Failures • Internal QA Plan • Documentation tie-in.

GOVERN

Intent: Set strategy, policy, roles, and **oversight**, including **supply-chain risk management** (C-SCRM).

Minimums: Written policy; risk appetite; roles & segregation; governance cadence; exception & risk acceptance rules; supplier/contract controls.

Implement—Procedural: Security policy; charter; risk appetite; governance calendar; exception handling with expiry; leadership reviews; **pre-launch security gate** for high-impact changes; KPI/KRI set (e.g., % assets with owner, MFA coverage, patch SLA, MTTR).

Implement—Technical: Asset & risk dashboards; qualitative/quantitative risk method; provider inventory and responsibility matrices.

Implement—Contractual: Security & privacy addenda; right-to-audit; incident notice timelines; data handling; **software supply-chain** requirements (SBOM/VEX where feasible).

- **Evidence:** Policy set; role matrix; risk appetite; governance minutes; exception register; provider matrices; KPI/KRI reports.
- **Acceptance Criteria:** Governance meets cadence; risk decisions documented; provider duties clear; exceptions time-bound with compensating controls; KPIs/KRIs trend toward targets.
- **Common Failures:** Vague risk appetite; ad-hoc exceptions; unclear provider responsibilities; no KPI/KRI program.
- **Internal QA Plan:** Quarterly review of risk decisions, KPI/KRI trends, and three provider matrices.
- **Documentation tie-in:** Policy set; Risk Management Plan; Supplier Responsibility Matrix; Metrics Standard.

IDENTIFY

Intent: Understand business mission, critical services, assets, and risk.

Minimums: Asset inventory (hardware, software, data, services); business context & criticality; threat/vulnerability exposure; risk register.

Implement—Procedural: Business impact analysis; critical service mapping; risk methodology; periodic risk reviews; **data classification** scheme (labels, handling rules).

Implement—Technical: Automated discovery (CMDB/ASM); software inventory (SBOM where available); classification & ownership; vulnerability intel; exposure management (internet-facing assets).

Implement—Contractual: Provider asset disclosures; SBOM availability; notification of material changes.

- **Evidence:** Asset lists; CMDB/ASM outputs; data classifications; risk register; BIA results; exposure scan summaries.
- **Acceptance Criteria:** 100% critical assets identified with owners; crown-jewel data labeled; risk register current; high risks owned with due dates; external exposure tracked.
- **Common Failures:** Shadow IT; stale inventories; orphaned assets; unlabeled sensitive data.
- **Internal QA Plan:** Monthly reconciliation (CMDB vs reality); external attack surface review; quarterly risk review.
- **Documentation tie-in:** Asset & Data Management Standards; Risk Register; BIA.

PROTECT

Intent: Implement safeguards to ensure delivery of critical services.

Minimums: Identity & Access (MFA remote/admin, least privilege); **Data Security** (encryption, DLP where needed); **Platform/Endpoint** (hardening, patching, EDR); **Awareness & Training; Protective Technology** (segmentation, secure config, backups).

Implement—Procedural: Access approvals & recerts; secure configuration & change control; backup/restore SOP; training plan; exception handling with expiry.

Implement—Technical: SSO/IdP; PAM for admin; network segmentation; TLS 1.2+; EDR on 100% endpoints/servers; vulnerability & patch SLAs; tested immutable/offline backups; secrets management; email & web protections; least privilege for service accounts.

Implement—Contractual: Provider IAM boundaries; encryption/key management expectations; backup/BC/DR responsibilities; minimum endpoint/tenant controls for MSPs.

- **Evidence:** Access requests; role matrices; MFA/PAM coverage; hardening baselines; patch dashboards; backup/restore results; training rosters; exception logs.
- **Acceptance Criteria:** 100% MFA for remote/admin; patch SLAs met; restore test passes within RTO/RPO; training completion ≥98%; exceptions tracked with expiry/compensating controls.
- **Common Failures:** Shared admin accounts; untested restores; missed patches; default configs; unmanaged secrets.
- **Internal QA Plan:** Quarterly sample—25 users/10 admins; 20 hosts for patch SLAs; one restore test/quarter; secret rotation review.
- **Documentation tie-in:** Access Control Policy; Hardening Standards; Backup & Recovery SOP; Training Plan; Secrets Standard.
- **OT/IoT addendum (if applicable).** Use jump hosts; vendor maintenance windows; signed firmware; compensating network controls; physical port protections; restricted egress.

DETECT

Intent: Develop and implement activities to **identify anomalies and events** and understand their potential impact.

Minimums: Central logging; time sync; monitoring coverage; detection use-cases; alert triage SLAs; periodic testing.

Implement—Procedural: Detection engineering backlog; alert handling playbooks; tuning & suppression governance; purple-team exercises; runbook hygiene reviews.

Implement—Technical: SIEM + telemetry from endpoints, identity, network, cloud, and critical SaaS; UEBA where available; honeypots/canaries for high-value assets; DNS and egress monitoring.

Implement—Contractual: Provider log and telemetry access; retention and export rights; clock/time sync requirements.

- **Top detection use-cases (at minimum):** Admin & privilege escalation; MFA bypass; impossible travel; disabled logging; new external exposure; mass file encryption; suspicious egress; service account misuse; mailbox rules for BEC; anomalous OAuth consent; public S3/Blob creation; IPS/EDR tamper.
- **Evidence:** SIEM configs; event samples; use-case catalog; alert metrics; test results.
- **Acceptance Criteria:** Required event types ingested from 100% in-scope systems; false positives within target; MTTA/MTTR within SLA; quarterly simulation success.
- **Common Failures:** Logging without review; cloud/identity telemetry gaps; noisy untuned rules.
- **Internal QA Plan:** Monthly detection efficacy review; quarterly attack simulation; SIEM ingestion health dashboard.
- **Documentation tie-in:** Logging & Monitoring Standard; Detection Runbooks; Use-Case Catalog.

RESPOND

Intent: Take action regarding detected cybersecurity incidents.

Minimums: IR plan; roles & on-call; communications/escalation; regulatory/contractual notice timelines; lessons-learned loop.

Implement—Procedural: Incident severity matrix; playbooks (ransomware, BEC, data loss, insider, cloud credential theft, third-party breach); evidence handling; liaison with Legal/Privacy and Communications; tabletop frequency.

Implement—Technical: Forensic imaging; containment automation; golden images; secure evidence storage; out-of-band comms.

Implement—Contractual: Incident notice SLAs; breach/notification clauses; joint investigations with providers.

- **Severity & notification matrix (example):**
  - **High:** Data exfiltration, service outage > RTO, privileged compromise → Exec/legal notified ≤1h; external notice per contract/regulation.
  - **Medium:** Contained malware; suspected credential theft → Exec/SecOps notified; 24h internal report.
  - **Low:** False positive or minor policy violation → Document and trend.
- **Evidence:** IR plan; playbooks; tabletop reports; incident tickets & AARs.
- **Acceptance Criteria:** Escalations within SLA; comms through approved channels; post-incident actions tracked and completed in defined windows.
- **Common Failures:** No call tree; late notices; missing evidence; unclear legal coordination.
- **Internal QA Plan:** Semiannual tabletop; post-mortem audit; notification time drills.
- **Documentation tie-in:** Incident Response Plan; Communications Guide; Severity Matrix.

RECOVER

Intent: Maintain plans for resilience and restore capabilities or services impaired due to incidents.

Minimums: Business continuity & disaster recovery plans; tested backups; recovery communications; improvement loop.

Implement—Procedural: BC/DR governance; dependency mapping; crisis comms; supplier failover expectations; annual plan refresh; quarterly restore tests.

Implement—Technical: Regular restores; alternate processing; prioritized run-books; immutable/offline backups; data integrity checks.

Implement—Contractual: RTO/RPO with providers; failover testing rights; data export options.

- **Evidence:** BC/DR plans; restore/DR test results; crisis comms templates; supplier attestations.
- **Acceptance Criteria:** Critical services meet RTO/RPO in test; recovery comms executed; lessons learned fed to governance within 30 days.
- **Common Failures:** Unpracticed failover; brittle dependencies; incomplete backups or missing keys.
- **Internal QA Plan:** Quarterly restore; annual DR exercise with suppliers; integrity spot-checks.
- **Documentation tie-in:** BC/DR Plans; Restore/Failover Runbooks; Crisis Comms.

4. Authorization Boundary & Data/Workflow Mapping

Define components, interfaces, trust zones, external providers, and where data flows, rests, and exits. Identify high-value assets, safety-critical dependencies, monitoring points, and change authorities. Keep diagrams current via change control and link them in the Evidence Register.

5. Documentation Set — Canonical Narratives

Maintain cohesive narratives that prove how your program satisfies CSF v2.0 across the boundary: mission & business context; governance & risk appetite; asset & data inventories; IAM & hardening; monitoring & detection; IR & recovery; third-party responsibilities; training; change management; continuous monitoring.

6. Applicability & Acceptance Criteria Mapping (to CSF v2.0)

Maintain a definitive record for each Function/Category you rely on: applicability, implementation summary, ODPs, measurable acceptance criteria, inheritance (if any), and evidence link.

Excerpt:

Function	Category	Applicable	Implementation Summary	ODPs	Acceptance Criteria	Inheritance	Evidence
GOVERN	Supply-Chain Risk	Y	Provider matrices; security addenda; notices	Notice ≤72h	Matrices current; notices on time	Some	TPRM/
IDENTIFY	Asset Management	Y	CMDB + ASM; owners; labels	Tag rules	100% critical assets owned	None	CMDB/
PROTECT	Identity & Access	Y	SSO; MFA remote/admin; PAM	Idle 15m	100% MFA remote/admin	None	IAM/
DETECT	Continuous Monitoring	Y	SIEM with endpoint/IdP/cloud logs	Ret 12–24m	MTTA/MTTR within SLA	Some	SIEM/
RESPOND	Communications	Y	Contact trees; notice paths	SLA matrix	Notices within SLA	Some	IR/
RECOVER	Recovery Planning	Y	BC/DR tested; backups	RTO/RPO	Tests meet RTO/RPO	Some	DR/

7. Program Parameters (Organization-Specific Settings)

- **Authentication:** MFA for remote network access and all admin actions; session idle 15 min; password min length 12; privileged sessions via PAM.
- **Cryptography & Network:** TLS 1.2+; cert rotation ≤13 months; segmentation with deny-by-default; egress allow-listing; DNS security controls.
- **Logging:** Required events (auth, admin, access, config, data actions); retention ≥12 months; MTTA ≤1h High; MTTR ≤24h High.
- **Patching/Vulnerability:** Critical ≤15 biz days; High ≤30; Medium ≤60; Low ≤90; exceptions time-bound with compensating controls.
- **Backups/Recovery:** 3-2-1 backups; quarterly restores; RTO/RPO targets per critical service; key escrow/rotation rules.
- **Training:** Before access; annual refresher; role-based tracks (end users, admins, developers, IR).
- **Third-Party:** Incident notice ≤72h; right-to-audit; SBOM or equivalent visibility where feasible; change notices for material updates.
- **Risk:** Quarterly review board; risk acceptance expires ≤180 days unless renewed with justification.
- **OT/IoT (if applicable):** Maintenance access approvals; network isolation; allow-listed protocols; firmware signing and inventory.

8. Evidence Register

Artifact	Function(s)	Location/Path	Owner	Format	Retention
Policy Set & Risk Appetite	GOV	GRC/Policy/	CISO	PDF	3y
Governance Minutes & Exceptions	GOV	GRC/Minutes/	CISO	PDF	3y
KPI/KRI Reports	GOV	GRC/Metrics/	CISO	PDF/CSV	2y
Asset & Data Inventories (CMDB/ASM)	ID	IT/CMDB/	CMDB Owner	CSV/PDF	1–2y
Exposure Management Reports	ID	SecOps/ASM/	SecOps	PDF/CSV	1–2y
BIA & Critical Service Maps	ID/RC	GRC/BIA/	Continuity Lead	PDF	3y
IAM Requests/Recerts; MFA/PAM Coverage	PR	IAM/	IAM Lead	CSV	1–2y
Hardening Baselines & Change Tickets	PR	Build/	Platform	PDF/CSV	1–2y
Patch Dashboards & Exceptions	PR	SecOps/Patch/	SecOps	CSV/PDF	1–2y
SIEM Configs, Use-Cases, Alert Reviews	DE	SecOps/SIEM/	SecOps	JSON/PDF	1–2y
IR Plan, Playbooks, Tabletop AARs	RS	IR/	IR Lead	PDF	3y
BC/DR Plans & Restore/DR Test Results	RC	DR/	Continuity Lead	PDF/CSV	3y
Provider Responsibility Matrices & Addenda	GOV/All	TPRM/	Procurement	PDF/XLSX	Active+1y
Training Rosters & Content	PR	L&D/Sec/	L&D	CSV/PDF	3y
Risk Register & Reviews	GOV/ID	GRC/Risk/	CISO	CSV/PDF	3y

9. Continuous Monitoring

- **Daily:** SIEM ingestion health; high/critical alerts triage; EDR coverage; failed backups; certificate expiry <30 days.
- **Weekly:** Vulnerability scan deltas; IAM anomalies; egress rule changes; third-party notices review.
- **Monthly:** Access recerts (rolling); baseline drift; patch SLA dashboard; restore test; KPI/KRI review.
- **Quarterly:** Detection rule review; red/purple-team exercise; BC/DR exercise (at least tabletop); supplier control attestations.
- **Automation:** Open tickets for ingestion failures, MFA gaps, crypto drift, expired exceptions, failed restores, or unreviewed alerts; track to closure with owner/SLA.

10. Remediation & Risk Acceptance Workflow

Identify → Log (severity, owner, due date, milestones) → Treat (process, tech, training, provider) → Verify with evidence → Report to governance.

Risk acceptance only by designated officials, with explicit expiry and compensating controls; track in the risk register and review at governance cadence.

11. Third-Party & Supply-Chain (External Providers)

Inventory all in-scope providers; document shared responsibilities, incident/notice SLAs, logging & export rights, data handling, continuity expectations, and SBOM/patch posture where feasible. Require flow-downs to subcontractors. Validate annually or on material change, including access recertifications and termination paths.

12. Training & Awareness (Role-Based)

Tracks for workforce, privileged admins, developers, SOC/IR, leadership, procurement/TPRM. Onboarding *before* access; annual refresher; targeted refreshers after incidents. KPI: completion ≥98% and decreasing repeat findings.

13. Change Management for Security Impact

Assess CSF impact for product/process/network changes, new providers, cloud moves, or mobile/OT rollouts. Update diagrams, inventories, logging scope, MFA coverage, and recovery dependencies; ensure pre-launch security gate for high-impact changes, with rollback plans validated.

14. Evidence Sampling Plans (Internal QA)

- **Identity & Access:** Sample 25 users/10 admins; verify least privilege, MFA, timely deprovisioning.
- **Patching/Hardening:** Sample 20 hosts; confirm baselines and SLA compliance; verify exception expiries.
- **Logging/Detection:** Validate 5 systems end-to-end (required events, alerts, response).
- **IR/Recovery:** Review last tabletop and last restore/DR exercise; verify actions closed and RTO/RPO met.
- **Third-Party:** Review two provider matrices; confirm incident notice terms; spot-check one change notice and offboarding.

15. Common Pitfalls

Governance without **clear risk appetite** or expiry on exceptions; CMDB/asset lists that miss SaaS, cloud, or OT/IoT; MFA gaps for remote/admin; logging enabled but not reviewed; cloud/identity telemetry gaps; restore plans untested; RTO/RPO unrealistic; provider responsibilities unclear; no incident notice SLA or rights to logs.

16. Quick Reference Summary

Area	Core Artifacts	Examples
GOVERN	Policy; risk appetite; minutes	Exception register; supplier matrices; KPI/KRI
IDENTIFY	CMDB/ASM; data classification	BIA; critical service map; exposure report
PROTECT	IAM/MFA; baselines; EDR	Patch dashboards; backup tests; secrets mgmt
DETECT	SIEM configs; use-cases	Alert metrics; simulation results
RESPOND	IR plan; playbooks; AARs	Contact trees; severity/notice matrix
RECOVER	BC/DR plans; restores	RTO/RPO evidence; comms templates
TPRM	Responsibility matrices	Addenda; change/notice logs

17. Self-Assessment & Leadership Attestation

Use status: **Compliant (C) / Partially Compliant (PC) / Not Compliant (NC) / Not Applicable (N/A)**.

Tracker (illustrative):

Function/Category	Status	Rationale (for N/A or gaps)	Evidence Link	Owner	Action ID
PROTECT – Identity & Access	PC	Legacy VPN lacks MFA	IAM/MFA_Coverage_Q3.csv	IAM Lead	ACT-2025-044
DETECT – Continuous Monitoring	C	Required events ingested	SIEM/UseCase_Review_2025Q3.pdf	SecOps	—
GOVERN – Supply-Chain Risk	C	Matrices current; notices tested	TPRM/Matrix_v2025.xlsx	Procurement	—

Leadership attests scope is complete, evidence exists for each “C,” and PC/NC items have owners and due dates.

18. References & Resources

NIST Cybersecurity Framework (CSF) 2.0 — Core & Resources
https://www.nist.gov/cyberframework

NIST CSF 2.0 Reference Tool
https://csf.tools

NIST SP 800-161 Rev. 1 (Cybersecurity Supply Chain Risk Management)
https://csrc.nist.gov/publications/detail/sp/800-161/rev-1/final

NIST IR 8286 series (Integrating Cybersecurity & ERM)
https://csrc.nist.gov/publications/detail/nistir/8286/final

NIST SP 800-53 Rev. 5 (Security & Privacy Controls)
https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

Apptega Product Features

16+ Security Frameworks

One-Click Reporting

Automated Alerts & Notifications

API & Application Connectors

Automated Framework Crosswalking

Real-Time Compliance Scoring

Restricted Auditor View

Single Sign-On Connectivity

Policy & Plan Templates

Automated Risk Assessments

Document Repository for Artifacts

Multi-Tenant Environment

Apptega

About Apptega

A perennial G2 leader across various cybersecurity categories, Apptega is the cybersecurity and compliance platform purpose-built for security providers who are growing lucrative security practices, creating stickier customer relationships, and winning more business from competitors.

With Apptega's end-to-end platform, IT providers can:

1. Build continuous compliance offerings that set them apart, retain customers, and grow their ARR.
2. Build and manage world-class cybersecurity and compliance programs for their clients.
3. Increase the capacity and efficiency of their existing team so they can service 2–3× more customers.
4. Assess, measure, and manage their own security programs against a standard set of industry-leading frameworks.

To learn more, visit apptega.com

Visit apptega.com