tufin

NIST National Institute of Standards and Technology

NIST:

The NIST CSF 2.0 Cyber Resilience Checklist

The release of NIST CSF 2.0 marks a shift in how organizations approach cybersecurity risk. With the addition of Govern as a core function, cybersecurity is now positioned as a business driven discipline where technical controls must align directly with organizational risk, accountability, and mission. For NetOps and SecOps teams, this elevates the role of network security from execution to enforcement of strategy.

This checklist helps security and network teams assess their network security practices against NIST CSF 2.0. Use it to identify gaps, align network policy with governance and risk objectives, and strengthen resilience across governance, protection, detection, response, and recovery.

Govern & Identify

Targeting the "New" Govern Function & Asset Visibility Aligning network policy with organizational risk and mission.

[ ] **Establish Your Security Strategy:** (GV.RM) Define your organization's risk appetite and ensure network security policies reflect these business-critical priorities.
[ ] **Define Roles & Accountability:** (GV.RR) Formally document who is responsible for network policy changes and who has the authority to approve risk exceptions.
[ ] **Map the Hybrid Landscape:** (ID.AM) Maintain a dynamic inventory of all physical and cloud assets. You cannot govern what you cannot see.
[ ] **Bridge the Policy Silos:** (GV.PO) Shift from "point-in-time" snapshots to a real-time state of audit readiness by creating a unified policy that governs firewalls, SASE, and Cloud from a single source of truth.

Protect

Targeting Identity Management, Access Control, and Platform Security Implementing the technical safeguards to limit the impact of an event.

[ ] **Enforce Least-Privilege Access:** (PR.AA) Limit logical access to the network based on "need-to-know" and business justification.
[ ] **Implement Infrastructure Segmentation: (**PR.PT) Use network security controls to isolate sensitive data and prevent lateral movement during a breach.
[ ] **Clean Up Security Debt:** (PR.PO) Regularly identify and remove redundant, shadowed, or unused firewall rules that clutter your defenses and expand your attack surface.
[ ] **Harden Configurations:** (PR.PS) Ensure all network devices follow standardized, secure configuration baselines (e.g., CIS benchmarks).

Detect, Respond & Recover

Targeting Continuous Monitoring and Incident Resilience Developing the speed and agility to identify and contain threats.

[ ] **Real-Time Policy Monitoring:** (DE.CM) Shift from "point-in-time" snapshots to a real-time state of audit readiness by alerting teams the moment a manual change deviates from your approved security baseline.
[ ] **Automate Incident Response:** (RS.MA) Establish workflows to quickly contain threats by deploying corrective network controls across all platforms simultaneously.
[ ] **Simulate Before Implementation:** (RS.AN) Use topology intelligence to analyze the impact of a proposed change before it goes live, ensuring you don't inadvertently create new vulnerabilities.
[ ] **Ensure Resilience & Availability:** (RC.RP) Maintain high-availability for your policy management infrastructure to ensure access governance stays online even during recovery operations.

Simplify NIST CSF 2.0 Compliance with Tufin

NIST CSF 2.0 establishes a governance driven framework that connects cybersecurity controls to organizational risk management and accountability. Network security policy supports this framework by enforcing consistent controls, documenting risk decisions, and enabling oversight across complex hybrid environments.

Tufin helps organizations manage hybrid networks through a unified control plane that supports alignment with NIST CSF 2.0. Tufin connects firewalls, cloud, SASE, and segmentation to provide unified visibility into how security policy functions across the network. By centralizing policy management, Tufin enables security, operations, and compliance teams to coordinate governance activities and maintain cyber resilience through consistent enforcement and continuous verification.

To learn more or request a demo, visit www.tufin.com.

About Tufin

Tufin helps enterprises simplify network complexity. As the leading Network Security Posture Management platform, Tufin serves as the unified control plane for modern hybrid networks spanning on-premises, cloud, SASE, microsegmentation, and multi-vendor environments. Trusted by thousands of organizations worldwide, Tufin delivers continuous risk visibility, reduces exposure through policy-driven automation, and enables continuous compliance and audit readiness at scale.