Framework Foundations: NIST CSF 2.0

Introduction to NIST CSF 2.0

The NIST Cybersecurity Framework (CSF) 2.0, released in February 2024, is a major update to the original 2014 framework. It provides a flexible, outcome-driven approach to managing cybersecurity risks across all sectors – public, private, and nonprofit. CSF 2.0 introduces a sixth core function, Govern, emphasizing executive accountability and strategic alignment of cybersecurity with business objectives.

The framework is voluntary but widely accepted as a best-practice model for cybersecurity governance and risk management It benefits organizations without formal cybersecurity programs, yet it is robust enough for even tho most mature organizations.

Key enhancements in NIST CSF 2.0:

- Expanded scope beyond critical infrastructure to all organizations
- Updated categories and subcategories for modern threats
- Stronger emphasis on supply chain risk management
- Improved alignment with global standards like ISO/IEC 27001:2022

Objectives of NIST CSF 2.0

The NIST CSF 2.0 framework offers a structured, flexible way to strengthen cybersecurity. It is used to:

- Assess risks
- Guide cybersecurity programs
- Improve communication across teams and stakeholders

Key Requirements

NIST CSF 2.0 is structured around six core functions – Govern, Identify, Protect, Detect, Respond, and Recover. These requirements help organizations manage cybersecurity and improve resilience.

Govern (GV): Establish cybersecurity strategy, roles, policy and oversight.

- Cybersecurity governance
- Supply chain risk management
- Compliance

Identify (ID): Understand assets, risks, and business context.

- Asset management
- Risk assessment
- Improvement planning

Protect (PR): Implement safeguards to ensure service delivery.

- Identity management and access control
- Data security
- Infrastructure resilience

Detect (DE): Identify cybersecurity events and anomalies.

- Threat detection
- Continuous security management
- Event analysis

Respond (RS): Take action during and after incidents.

- Incident management
- Mitigation strategies
- Communication

Recover (RC): Restore capabilities and services post-incident.

- Recovery planning
- Post-incident review
- Resilience building

NIST CSF and Regulatory Alignment

The NIST CSF 2.0 offers significant strategic advantages for CISOs seeking compliance, streamlining audit preparation through its clear, structured approach to cybersecurity governance. This framework not only enhances an organization's overall security posture but also reduces regulatory risk and facilitates cross-framework harmonization, simplifying adherence to multiple standards and directives. Notably, NIST CSF 2.0 maps directly to many major compliance frameworks, including:

Regulation / Framework	Key Focus Areas	Aligned NIST CSF Function
SOC2	Governance, risk assessment, incident response	GV, ID, RS
HIPAA	Risk analysis, access control, breach notification	ID, PR, RS
PCI DSS	Asset classification, encryption, monitoring, technical controls, logging, and vulnerability management	ID, PR, DE
GDPR	Data protection by design, breach notification, governance	PR, RS, GV
NIST SP 800-53	Risk management, access control, continuous monitoring	GV, ID, PR, DE
NIST SP 800-171	Controlled unclassified information (CUI) protection, incident response	PR, RS
CMMC	Risk assessment, access control, maturity-based implementation	IR, PR, GV

How Cisco + Splunk Support Compliance

Cisco offers a comprehensive portfolio of security solutions that can help organizations meet the requirements of NIST CSF 2.0.

CSF Pillar	How Cisco + Splunk Supports Compliance	Relevant Products
Govern	Facilitates strategic decision-making and policy enforcement through comprehensive risk insights, performance reporting, and centralized policy management.	Cisco XDR, Cisco Secure Access, Cisco Security Cloud Control, Cisco Identity Services Engine (ISE), Splunk Enterprise Security (ES)
Identify	Enables continuous discovery and categorization of assets, systems, and associated cybersecurity risks to facilitate prioritized risk management and strategic understanding.	Cisco ISE, Cisco XDR, Meraki Systems Manager, Cisco Attack Surface Management, Cisco Secure Workload, Cisco Secure Endpoint, Splunk Asset & Risk Intelligence, Splunk ES
Protect	Proactively enforces and hardens security controls to safeguard assets, manage identity and access, and enhance resilience against cyber attacks.	Cisco Duo, Cisco Secure Access, Cisco Umbrella, Cisco Sure Email Threat Defense, Cisco Secure Web Appliance, Cisco Cloud Application Security, Cisco Secure Workload, Cisco Secure WAF, Cisco Multicloud Defense, Cisco Firewall, Cisco Secure Endpoint, Cisco Secure Client,
Detect	Enables rapid and accurate detection of cybersecurity incidents through continuous monitoring, anomaly analysis, and integrated threat intelligence.	Cisco XDR, Cisco Secure Network Analytics (SNA), Cisco Secure Malware Analytics, Cisco Telemetry Broker, Cisco Cyber Vision, Cisco Industrial Threat Defense, Cisco Secure Endpoint, Splunk ES, Splunk User Behavior Analytics (UBA), Splunk Attack Analyzer
Respond	Supports effective incident response by enabling rapid containment, thorough analysis, and coordinated communication to mitigate cybersecurity incidents.	Cisco XDR, Cisco SNA, Cisco Secure Firewall, Cisco Secure Endpoint, Cisco Security Cloud Control, Splunk ES, Splunk SOAR, Splunk Attack Analyzer, Cisco Talos Threat Intelligence
Recover	Facilitates the restoration of systems and data, ensures business continuity, and drives post-incident improvements for enhanced resilience.	Cisco Secure Endpoint, Cisco XDR, Cisco Security Cloud Control, Splunk ES, Splunk SOAR, Talos Threat Intelligence

NIST CSF 2.0 Compliance with Cisco Security + Splunk

Cisco and Splunk together provide a strong foundation for aligning with NIST CSF 2.0. Cisco's integrated architecture offers visibility, control, and threat response across hybrid environments, while Splunk enhances detection, investigation, and response through scalable analytics and automation.

This approach supports all CSF functions by enabling continuous monitoring, efficient incident handling, and effective risk management. Cisco's telemetry tools and Splunk's SIEM, SOAR, and UBA capabilities help security teams reduce dwell time and enhance response accuracy.

By leveraging both platforms, organizations can simplify cybersecurity operations, strengthen resilience, and align more effectively with regulatory and framework requirements.

Resources

For more information and guidance on NIST CSF 2.0 compliance, please refer to the following resources:

- Framework Mapping: Cisco Security Portfolio and Splunk + NIST CSF 2.0
- Splunk and the Cybersecurity Framework
- The NIST Cybersecurity Framework (CSF) 2.0