Framework Mapping: Cisco Duo + NIST CSF 2.0

Overview of the NIST Cybersecurity Framework 2.0

The National Institute of Standards (NIST) Cybersecurity Framework (CSF) 2.0 is a voluntary set of guidelines developed to help organizations manage and reduce cybersecurity risks. While voluntary, its adoption can significantly improve an organization's security posture by offering a structured approach to risk management.

NIST released the CSF 2.0 in February 2024, marking the first major update since version 1.1 in April 2018. This update incorporates feedback from various industries and stakeholders, enhancing the framework's flexibility, applicability, and relevance. The NIST CSF 2.0 continues to serve as a voluntary, risk-based framework designed to help organizations of all sizes and sectors manage and reduce cybersecurity risks, foster resilience, and align with best practices.

Purpose of the Framework

The NIST Cybersecurity Framework provides a structured yet flexible approach to improving an organization's cybersecurity posture. It is used for:

Assessing Risks: Identifying, analyzing, and prioritizing cybersecurity risks.

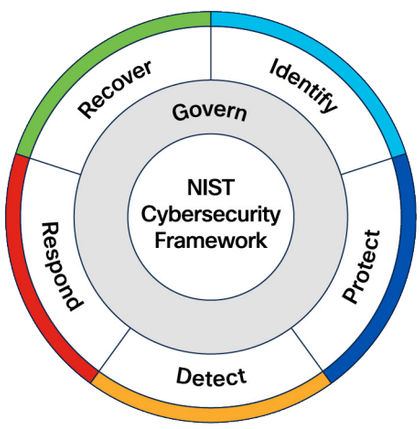
Guiding Cybersecurity Programs: Establishing or improving cybersecurity strategies in alignment with organizational goals.

Enhancing Communication: Facilitating clear communication about cybersecurity risks and strategies between technical teams, leadership, and external stakeholders.

The framework is particularly valuable for organizations that lack formalized cybersecurity programs or resources, though it is robust enough to benefit even the most mature organizations.

Key Components of the NIST Cybersecurity Framework 2.0

The NIST CSF 2.0 maintains the foundational structure of the original framework while introducing several enhancements. Its key components are:



Core Functions

The Framework Core outlines six **high-level functions** that provide a strategic view of cybersecurity risk management. These functions remain foundational in CSF 2.0 and are as follows:

GOVERN:

Establish and oversee policies, roles, processes, and accountability to align cybersecurity efforts with organizational objectives and regulatory requirements.

Examples: Risk management policies, executive accountability, cybersecurity governance framework

IDENTIFY:

Develop an understanding of cybersecurity risks to systems, assets, data, and capabilities. This involves identifying critical resources, threats, and vulnerabilities.

Examples: Asset management, governance, risk assessments

PROTECT:

Implement safeguards to ensure the delivery of critical services and mitigate risks.

Examples: Access control, data protection, training, and maintenance

DETECT:

Establish systems to identify cybersecurity events or anomalies in a timely manner.

Examples: Continuous monitoring, intrusion detection, and threat intelligence

RESPOND:

Develop and implement appropriate actions to mitigate the effects of a detected cybersecurity event.

Examples: Incident response planning, mitigation strategies, and communication

RECOVER:

Develop plans to restore operations and reduce the impact of cybersecurity incidents.

Examples: Disaster recovery, business continuity planning, and lessons learned

Implementation Tiers

The framework includes **Implementation Tiers** to help organizations evaluate their current cybersecurity practices and set goals for improvement. These tiers reflect the degree to which an organization's cybersecurity practices are informed by risk management processes, integrated with business needs, and adaptive to evolving risks:

- **Tier 1 (Partial):** Limited awareness and ad hoc implementation of cybersecurity practices.
- **Tier 2 (Risk-Informed):** Risk management practices are formally defined but not fully integrated.
- **Tier 3 (Repeatable):** Cybersecurity practices are consistently applied and documented across the organization.
- **Tier 4 (Adaptive):** Practices are continuously improved and proactively adapted to changing risks.

Profiles

The **Framework Profiles** allow organizations to align the framework to their specific goals, resources, and risk tolerance. A profile compares the current state of an organization's cybersecurity practices to its desired state, serving as a roadmap for improvement.

Why Use NIST CSF?

Organizations adopt the NIST CSF 2.0 for several reasons:

Flexibility: Its non-prescriptive nature allows organizations to tailor it to their unique needs.

Widely Recognized: The framework is globally acknowledged as a standard for cybersecurity best practices.

Risk Management: It helps organizations prioritize risks and allocate resources effectively.

Compliance Alignment: While voluntary, the framework aligns with various regulatory requirements and standards, simplifying compliance efforts.

Mapping to other Frameworks

The NIST National Online Informative References (OLIR) Program enables organizations to map cybersecurity standards and frameworks. By leveraging OLIR, Cisco can cross-reference the NIST Cybersecurity Framework (CSF) 2.0 with standards like NIST SP 800-53, simplifying compliance and security alignment. This eliminates the need for separate mappings, saving time and ensuring traceability across frameworks.

For Cisco, once solutions like Duo are mapped to NIST CSF 2.0, these mappings can be extended through OLIR to other frameworks. This is especially beneficial for public sector and regulated industries that must comply with multiple frameworks. Using NIST CSF 2.0 as a common backbone, Cisco helps customers achieve compliance and demonstrate alignment with best practices. This cross-mapping makes Cisco a key enabler of cybersecurity compliance, helping customers see how its solutions support broader compliance and risk management.

Understanding Cisco Duo

Cisco Duo is a critical component of Cisco's zero trust security architecture, designed to protect enterprise users by establishing trust for every access request regardless of location. It provides strong authentication methods, including passwordless options such as biometrics and security keys, to verify user identities securely and seamlessly.

Duo also offers device trust capabilities, enabling organizations to assess and enforce the security posture of devices before granting access to corporate applications. This approach helps minimize risk by continuously verifying both user and device trust, leveraging adaptive, context-based access controls that monitor user behavior and device health to dynamically adjust policies in real time.

Beyond authentication, Cisco Duo integrates with other Cisco security solutions like Cisco Identity Services Engine (ISE), Cisco XDR, and Cisco Secure Access to create a comprehensive zero trust environment. It provides unified visibility into user activities and device compliance, enabling organizations to detect anomalies and respond to threats proactively.

Duo supports a wide range of applications and devices, offering single sign-on (SSO), multi-factor authentication (MFA), and device trust features that simplify and protect access while reducing administrative overhead. This seamless integration and adaptive security posture make Cisco Duo a foundational element for organizations aiming to implement zero trust with minimal friction and maximum protection across hybrid and cloud environments.

Benefits of Cisco Duo

Cisco Duo offers several advantages for organizations seeking to strengthen their cybersecurity posture:

- **Enhanced Security and Compliance:** Duo provides phishing-resistant multi-factor authentication (MFA) that helps organizations meet compliance requirements, including FedRAMP, Cybersecurity Maturity Model Certification (CMMC), NIST CSF, ISO 27001, and Zero Trust Models for both Cybersecurity and Infrastructure Security Agency (CISA) and the Department of Defense (DoD). It protects against phishing attacks by requiring a second factor beyond just a password, significantly reducing the risk of unauthorized access even if credentials are compromised.
- **Advanced Proximity Verification:** In addition to traditional MFA, Duo leverages advanced technical capabilities such as proximity verification to further enhance security. With Duo, user devices need to be in close physical proximity to the computer attempting authentication. This feature uses Bluetooth Low Energy (BLE) technology to detect nearby devices, helping prevent remote attackers from successfully completing authentication requests, as only devices that are near the login device can approve access. This mitigates the risk of users being tricked into approving fraudulent authentication requests, adding an extra layer of protection against social engineering and push notification attacks.

- **User Convenience and Productivity:** Duo can remember trusted devices; this reduces the frequency of authentication prompts and improves user experience without sacrificing security. Features like Duo Passport enable seamless access across applications, browsers, thin and thick clients, and more.

- **Scalability and Flexibility:** Duo easily adapts to organizations of all sizes and diverse user bases. It supports automated user provisioning and deprovisioning, simplifying identity lifecycle management. Duo's cloud-based architecture allows for fast deployment and lowers total cost of ownership compared to traditional MFA solutions.

- **Comprehensive Device Trust:** Duo's Device Trust capability verifies the security posture of devices before granting access, assessing factors such as operating system version, encryption status, and presence of security software. This helps prevent risky or non-compliant devices from accessing sensitive resources and balancing security with user productivity.

- **Visibility and Control:** Duo offers critical IT visibility into user identities, device health, and access patterns through centralized dashboards and integrations with Cisco Identity Intelligence. This enables organizations to detect suspicious activities, enforce conditional access policies based on context (such as user role, location, and device security), and respond proactively to threats.

- **Reduced IT Burden:** Duo's self-service portal empowers users to manage their authentication devices, reducing help desk tickets. Guided remediation helps users bring devices into compliance without IT intervention, further lowering operational costs.

- **Integration and Ecosystem:** Duo integrates seamlessly with existing identity and security infrastructures, supporting single sign-on (SSO), passwordless authentication, and a broad ecosystem of over 250 partners. This maximizes the value of existing investments while enhancing security posture.

Overall, Cisco Duo delivers a robust, user-friendly, and scalable solution that strengthens security, improves compliance, and enhances productivity across hybrid and cloud environments.

Cisco Duo Deployment Options

Cisco Duo offers several deployment options to integrate MFA and zero trust security across various Cisco products and environments, including a FedRAMP Authorized federal edition tailored for public sector organizations with stringent security requirements.

Cisco ASA or Firepower VPN Integration: Duo can be deployed with Cisco ASA or Firepower VPN appliances to add two-factor authentication to AnyConnect or Cisco Secure Client logins. This setup uses the Duo Authentication Proxy to mediate authentication requests between the VPN and Duo's cloud service. It supports policies based on network location and fail mode configurations if Duo's service is unreachable. This deployment requires Cisco ASA firmware 8.3 or later or Cisco FTD version 6.3.0 or later managed by FMC 6.3.0 or later. There are two main methods:

- **RADIUS Authentication:** Cisco ASA or FTD sends authentication requests to the Duo Authentication Proxy, which performs primary authentication (e.g., Active Directory) and secondary authentication via Duo.

- **Single Sign-On (SSO) with SAML:** For Cisco Firepower Threat Defense (FTD), Duo Single Sign-On can be used with a cloud-hosted identity provider, providing an interactive MFA prompt and device insights during VPN login.

Cisco Identity Services Engine (ISE) Integration: Duo can integrate with Cisco ISE using RADIUS to add MFA for AnyConnect or Cisco Secure Client users. The Duo Authentication Proxy handles authentication requests between ISE and Duo's cloud service. This requires Cisco ISE version 2.4 or later.

Device Trust and Endpoint Security: Duo's Device Trust capabilities verify the security posture of devices before granting access, including checks for operating system version, encryption, and security software presence. Duo Desktop can enforce endpoint health policies and provide self-remediation prompts to users for compliance.

Cloud-Based and Flexible Deployment: Duo's cloud-native architecture allows for rapid deployment and scalability across organizations of all sizes. It supports integration with existing identity providers, single sign-on (SSO), passwordless authentication, and adaptive access policies.

Cisco Duo Federal Editions: Cisco offers two FedRAMP authorized, FIPS-compliant editions—Duo Federal Essentials and Duo Federal Advantage—designed to meet the strict security requirements of federal agencies and public sector organizations. These federal editions provide strong cloud-based authentication and device visibility aligned with FedRAMP, FIPS 140-2, and NIST SP 800-63-3 standards.

Key differences from commercial editions include exclusion of telephony and SMS factors, enhanced role-based and location-based access policies, biometric authentication enforcement, and compliance with federal security controls. Eligibility for these editions includes federal agencies, federal contractors, state and local governments, public sector organizations, state universities, and federally funded research centers. Transitioning from commercial to federal editions requires full redeployment and reenrollment of users due to FedRAMP security controls.

Duo Federal editions also support native VPN integration with Cisco ASA and provide unified endpoint visibility to enforce device hygiene policies, enabling or denying access based on device compliance. These capabilities align with FedRAMP/NIST 800-53 security controls and FIPS 140-2 compliance requirements for federal organizations.

These deployment options enable organizations to implement strong, context-aware authentication and device security controls across VPNs, network access, and applications, aligning with Cisco's zero trust security framework and federal compliance mandates.

For detailed deployment instructions and federal edition specifics, Cisco provides comprehensive guides and resources including the Duo Federal Guide and eligibility considerations:

- Guide to Duo's Federal Editions | Duo Security
- Duo Federal Editions: Eligibility and Considerations
- Solutions - Trusted Internet Connections (TIC) 3.0 Architecture Guide - Cisco

Technical Features

Cisco Duo offers a comprehensive set of technical features designed to enhance security through phishing-resistant authentication, device trust, and seamless user experience; all aligned with zero trust principles. Key technical features include:

- **Multi-Factor Authentication (MFA):** Duo supports a variety of strong authentication methods including push notifications via the Duo Mobile app, hardware tokens, Universal 2nd Factor (U2F) security keys, and biometric passwordless authentication. Users can authenticate even without network connectivity using offline methods or hardware tokens. Duo Mobile can be provisioned easily through QR codes during enrollment.
- **Passwordless Authentication:** Duo Directory enables organizations to eliminate passwords entirely by supporting passwordless authentication through biometrics, FIDO2 WebAuthn security keys, and integration with external cloud directories or on-premises Active Directory. Duo Desktop bridges gaps for embedded browsers that lack WebAuthn support.
- **Device Trust:** Duo provides deep visibility into device health and security posture before granting access. Features include endpoint health checks (e.g., OS version, encryption, security software), trusted endpoints tracking, and enforcement of compliance policies. Duo Desktop offers self-remediation prompts to users to update or secure their devices. Integration with Cisco Secure Endpoint allows automated blocking of compromised devices.
- **Adaptive Access Policies:** Administrators can create granular policies based on user groups, device health, network location, geo-IP, and risk factors. Duo supports IP allowlisting, trusted devices with configurable time limits, and step-up authentication requirements for higher-risk scenarios — with agentless management.
- **Single Sign-On (SSO) and Identity Federation:** Duo offers cloud-hosted SSO supporting SAML 2.0, OIDC, and OAuth 2.0 standards, enabling seamless access to multiple applications with one login. It can act as an identity provider (IdP) or integrate with existing IdPs, supporting multiple authentication sources and routing rules. Duo Passport extends SSO capabilities across browsers, operating systems, and thick clients.
- **User and Device Visibility:** Duo Device Insight inventories endpoints, providing data on OS, platform, browser versions, encryption status, and device risk indicators like jailbroken or rooted status. This visibility helps administrators identify risky devices and enforce policies accordingly.
- **Integration with Cisco Security Ecosystem:** Duo integrates with Cisco Secure Endpoint, Secure Firewall, Identity Services Engine (ISE), Cisco XDR, and Meraki to provide unified security posture, threat detection, and enforcement of zero trust policies across network and endpoint layers.
- **Administrative Controls and Support:** Duo provides an admin panel for user and policy management, supports custom attributes for identity management, and offers various support tiers including standard, enhanced, and signature support. Hardware tokens are available for one-time passcode authentication, and telephony credits can be purchased for phone-based authentication.

These technical features collectively enable organizations to implement strong, adaptive, and user-friendly security controls that verify both user identity and device trust before granting access to applications and networks, supporting a robust zero trust security framework.

Duo delivers "Security-first" IAM

Identity you can trust

Duo Directory + Easy, Phishing-resistant MFA + Device Trust + True SSO + Complete Passwordless + Minimize Identity Risks

Security-first IAM
User Directory | Single Sign-On | MFA | AI Assistant

End-to-end Phishing Resistance
Phishing-resistant MFA | Complete Passwordless | Session Theft Protection

Unified Identity Intelligence
Cross-platform Visibility | ISPM | ITDR

Mapping Cisco Duo to NIST CSF 2.0

		Cisco Duo NIST CSF 2.0 Mapping		Cisco Duo NIST 800-53 Mapping	
Function	**Category**	**Meets**	**Supports**	**Meets**	**Supports**
Govern (GV)		Non-technical controls			
Identify (ID)	Asset Management (ID.AM)		ID.AM-01, ID.AM-08		CM-08, CM-09, CM-13, MA-02, MA-06, PL-02, PM-05, PM-22, PM-23, SA-03, SA-04, SA-08, SA-22, SI-12, SI-18, SR-05, SR-12
	Risk Assessment (ID.RA)		ID.RA-01		CA-02, CA-07, CA-08, RA-03, RA-05, SA-11(02), SA-15(07), SA-15(08), SI-04, SI-05
	Improvement (ID.IM)	Non-technical controls			
Protect (PR)	Identity, Management, Authentication, and Access Control (PR.AA)	PR.AA-01, PR.AA-03, PR.AA-04, PR.AA-05	PR.AA-02	AC-01, AC-02, AC-05, AC-06, AC-07, AC-10, AC-12, AC-14, AC-16, AC-17, AC-18, AC-19, AC-24, C-03, IA-01, IA-02, IA-03, IA-04, IA-05, IA-06, IA-07, IA-08, IA-09, IA-10, IA-11, IA-13	IA-12
	Awareness and Training (PR.AT)	Non-technical controls			
	Data Security (PR.DS)		PR.DS-02		AU-16, CA-03, SC-04, SC-07, SC-08, SC-11, SC-12, SC-13, SC-16, SC-40, SC-43, SI-03, SI-04, SI-07
	Platform Security (PR.PS)		PR.PS-01, PR.PS-02, PR.PS-03, PR.PS-04		AU-02, AU-03, AU-06, AU-07, AU-11, AU-12, CM-01, CM-02, CM-03, CM-04, CM-05, CM-06, CM-07, CM-07(09), CM-08, CM-09, CM-10, CM-11, MA-03(06), SA-10(01), SA-10(03), SC-39(01), SC-49, SC-51, SI-02, SI-07
	Technology Infrastructure Resilience (PR.IR)	PR.IR-01, PR.IR-03, PR.IR-04		AC-03, AC-04, SC-04, SC-05, SC-07, CP-02, PE-09, PE-10, PE-11, PE-12, PE-13, PE-14, PE-15, PE-18, PE-23, CP, IR, SA-08, SC-06, SC-24, SC-36, SC-39, SI-13, CP-06, CP-07, CP-08, PM-03, PM-09	
Detect (DE)	Continuous Monitoring (DE.CM)	DE.CM-03, DE.CM-09		AC-02, AC-04, AC-09, AU-12, AU-13, CA-07, CM-03, CM-06, CM-10, CM-11, SC-34, SC-35, SI-04, SI-07	
	Adverse Event Analysis (DE.AE)	DE.AE-02, DE.AE-03, DE.AE-04	DE.AE-06, DE.AE-08	AU-06, CA-07, IR-04, IR-05, IR-08, PM-09, PM-11, PM-16, PM-18, PM-28, PM-30, SI-04	IR-04, IR-08, PM-15, PM-16, RA-03, RA-10
Respond (RS)	Incident Management (RS.MA)	Non-technical controls			
	Incident Analysis (RS.AN)	RS-MA-01	RS.AN-03, RS.AN-07, RS.AN-08	IR-06, IR-07, IR-08, SR-03, SR-08	IR-04, IR-08, PM-15, PM-16, RA-03, RA-10
	Incident Response Reporting and Communication (RS.CO)	Non-technical controls			
	Incident Mitigation (RS.MI)	RS.MI-01	RS.MI-02	IR-04	IR-04
Recover (RC)	Incident Recovery Plan Execution (RC.RP)				
	Incident Recovery Communication (RC.CO)	Non-technical controls			

Conclusion

The NIST Cybersecurity Framework 2.0 builds upon the foundational strengths of its predecessor by addressing the evolving and complex cybersecurity landscape with a flexible, scalable, and comprehensive risk management approach. This framework empowers organizations to enhance their cybersecurity posture, improve resilience, and ensure the continuity of critical operations. Whether an organization is initiating its cybersecurity efforts or refining an established program, CSF 2.0 serves as a vital guide for navigating today's dynamic threat environment.

Cisco Duo offers an adaptive solution designed to strengthen identity and access management through multi-factor authentication, device trust, and zero trust principles. By integrating seamless user verification, device health assessments, and granular access policies, Cisco Duo helps organizations protect critical assets and data from unauthorized access across diverse environments. Its scalability, ease of deployment, and integration with broader Cisco security ecosystems make it a key component for organizations aiming to implement effective identity security aligned with NIST CSF 2.0.

By aligning Cisco Duo with the NIST CSF 2.0 and NIST 800-53 frameworks, organizations can effectively manage identity and access risks, streamline compliance efforts, and foster clear communication between technical teams and leadership. Cisco Duo's capabilities support organizations at any stage of their cybersecurity journey, whether establishing foundational identity controls or optimizing mature zero trust programs, thereby enhancing overall security posture and operational resilience.

Resources

If you'd like to go a bit deeper on identity security, phishing resistance, or how organizations are using Cisco Duo in real-world environments, the following resources are a good place to start:

- MFA Buyer's Evaluation Guide
  A practical guide to help you understand what to look for in a modern MFA solution and how different approaches compare.
- Guide to building End-to-End Phishing Resistance
  A closer look at how phishing-resistant authentication and device trust can significantly reduce credential-based attacks.
- Understanding the Business Impact of Cisco Duo
  A look at the business value organizations are seeing with Cisco Duo, based on a Forrester Total Economic Impact™ study showing a 198% ROI and $4.4M NPV.
- Why Customers Choose Cisco Duo for User Authentication
  Insights from customer reviews and feedback highlighted in Gartner Peer Insights™.