Compliance

Complex regulations and security frameworks can make it challenging to select security products that address all the needs and requirements. This quick guide will help you understand how Duo can help your business with compliance requirements and regulatory framework guidelines.

THE CHALLENGE:

Selecting Solutions to Align with Requirements

Risk and Compliance teams within organizations need to work closely with Security teams to ensure that security practices being implemented follow recommended best practices, align with compliance requirements and adhere to data privacy regulations.

If these teams are not in alignment, it can result in heavy financial and reputational penalties. They need to work together to find the right solutions that can increase security and assist with compliance without impacting user productivity.

THE SOLUTION:

Usable Security Solutions That Help Meet Compliance and Reduce Risk

Duo provides organizations with best-in-class security technology and a trusted partnership that can help build and maintain a well-rounded security program. We believe that by focusing on security fundamentals and best practices, you can easily achieve compliance.

We focus on protecting your employees with strong multi-factor authentication (MFA) resistant to phishing and push fatigue. . In addition to protecting your employees, we provide the ability to ensure only trusted and managed devices have access to your data.

Built with a focus on security and usability, Duo's solutions can help organizations establish security practices that provide a great user experience while aligning with certain areas of compliance guidelines.

Duo offers different editions that provide organizations with flexible solutions to address security projects and requirements. Duo helps you meet components of compliance and regulatory requirements with a secure, easy-to-use platform that provides the foundation for a zero trust security approach for your workforce.

Duo Helps Follow Best Practices

Overarching security frameworks like ISO 27001 and NIST provide recommendations for security best practices, which inform many compliance guidelines that span across multiple industries and verticals.

Foundational Framework	How Duo Editions Help		
	Duo MFA	Duo Access	Duo Beyond
ISO 27001 International Organization for Standardization A.9.1.2, A.9.2.1, A.9.4.1, A.9.4.2, A.9.4.4, A.9.4.5, A.12.4.1, A.12.4.2, A.12.4.3, A.13.1.2, A.14.1.2, A.14.2.4, A.14.2.6, A.14.3.1, A.18.1.3, A.18.1.4	+ Syncs with existing identity access management (IAM) solutions. + Provides a layer of strong authentication. + Automates user provisioning and de-provisioning of authentication factors. + Reports on event logs recording user activities.	+ Enforces adaptive access policies for role-based access. + Controls access to systems and applications with a secure log-on procedure, where required by the access control policy. + Limits access to source code to verified users.	+ Provides secure access to internal applications without exposing them to external risk. + Allows only trusted endpoints to access specific applications. + Enables limited access for external third parties to specific applications and systems.
NIST 80053, NIST 800171 & DFARS National Institute of Standards and Technology 800171, Revision 2 (June '19) SP 800633b guidance NIST 80053 Control: IA2, IA3, IA5, IA6, MA4, SC7, SC11 NIST 800171 Control: 3.1.1, 3.1.1, 3.1.3, 3.1.7, 3.1.11, 3.1.12, 3.1.14, 3.1.15, 3.1.18, 3.1.20, 3.3.1, 3.3.2, 3.3.8, 3.4.1, 3.4.2, 3.5.2, 3.5.3, 3.5.7, 3.7.5	+ Uniquely identifies and authenticates users. + Meets NIST digital identity guidelines. + Limits system access to authorized users. + Provides inventory of all endpoints accessing protected applications. + Provides local access protections online/offline for DFARS requirements.	+ Limits applications that authorized users are permitted to access. + Grants access only to healthy and compliant devices. + Adds a layer of authentication for privileged accounts.	+ Routes remote access via managed access control points. + Controls connection of BYOD. + Identifies and verifies specific devices before establishing a connection. + Restricts access to controlled unclassified information (CUI) in a compliant manner.
CMMC 2.0 Cybersecurity Maturity Model Certification (CMMC) for third-party contractors	+ Provides defense contractors strong MFA across multiple domains including: Access Control (AC), Identification and Authentication (IA) and Audit and Accountability (AU)	+ Protects every application, is easy to deploy, and removes telephony + Achieves end-to-end FIPS capability + Allows actions to be logged and traceable to a specific user	+ Satisfies multi-factor requirements for local and network access to privileged accounts and for network access to non-privileged accounts + Protects cloud/ applications, remote VPN connections and SSH connections
FIPS 140-2 Federal Information Processing Standards, Control: 1402 lv13	+ Leverages FIPS 140-2 validated cryptographic modules to achieve compliance. + Zero-touch implementation for FIPS 140-2 compliant mobile authentication; no configuration required by administrators.		
SOC2 Systems and Organization Controls Report 2017 Trust Services Criteria (TSC) Reference Number: CC6.1, CC6.2, CC6.3, CC6.6, CC6.7, CC7.1	+ Provides automatic provisioning and deprovisioning of MFA tokens. + Integrates with a SIEM for fraudulent push authentication reported by users. + Provides visibility of endpoints accessing business applications.	+ Implements the concepts of least privilege to establish role-based access policies to applications. + Restricts access from devices that are out of date and provides users with self-remediation options.	+ Restricts access to known devices and locations. + Provides secure external access that can be tracked and limited to protect internal resources. + Establishes trust in BYOD in environments with an agentless approach.

Duo Helps Address Areas of Compliance Guidelines

Risk and Compliance teams will often work with Security teams to ensure their security strategy is in line with the compliance requirements to avoid potential financial penalties.

Compliance Guidelines	How Duo Editions Help		
Foundational Frameworks	Duo MFA	Duo Access	Duo Beyond
CJIS Criminal Justice Information Services Version 5.9 Section: 5.5.2.3, 5.5.6.1, 5.5.6.2, 5.6, 5.13.4.1, 5.15, 5.13.7.1, 5.13.7.2	+ Supports multiple methods for an additional factor of authentication + Provides automated management of authentication methods + Provides methods for users to report fraudulent access attempts	+ Ensures end users have up-to-date security patches on their devices. + Provides guidance for self-service remediation for systems that are out of date + Meets the MFA requirement for PAM, Gen users, device policy etc.	+ Restricts access to information protected under CJI from unmanaged and/or unknown devices + Blocks access from unverified BYOD sources
EPCS Electronic Prescriptions for Controlled Substances (75 FR 16236, March 31, 2010) [Docket No. DEA218, RIN 1117AA61]	+ Protects individual and institutional practitioners from misuse of their credentials by insiders as well as from external threats + Meets cryptographic requirements and is verified by a DEA accredited auditor	+ Ensures that only authorized practitioners are able to gain access and digitally sign for controlled substance distribution with granular access policies based on role	+ Permits access only to known/ trusted devices accessing systems for e-prescribing + Enforces security controls and encryption on BYOD devices
FFIEC Federal Financial Institutions Examination Council Version Sept 2016 Title: II.C.5, II.C.7, II.C.7(a), II.C.7(e), II.C.10(d), II.C.13(e), II.C.15(b), II.C.15(c), II.C.15(d), II.D, III.C	+ Provides controls to require multi-factor authentication for access to local workstations + Provides a detailed view of the security posture of the devices that are connecting to sensitive applications + Implements a robust authentication method consistent with the criticality and sensitivity of the application	+ Enforces access policies based on group membership for sensitive applications. + Provides guidance for device updates and remediation through self-service + Blocks access for unauthorized devices connecting to applications	+ Restricts remote access to authorized network areas and applications + Ensures seamless and secure remote access to sensitive applications + Ensures BYOD devices connecting to sensitive information are reported and meet the latest security criteria before granting access
GBLA Gramm-Leach-Bliley Act FIL222001 Title: V Subtitle A Section 501(3)	+ Provides MFA to strengthen secure password policy	+ Ensures devices and browsers accessing sensitive application are patched and updated	+ Verifies that protected screen lock is enabled on mobile devices + Makes sure device encryption is enabled on mobile devices
HIPAA Health Insurance Portability and Accountability Act, CFR 45 revised October 1, 2007 Standard: 164.304, 164.308(a)(1), 164.308(a)(3)(ii)(A), 164.308(a)(3)(ii)(B), 164.308.(a)(4), 164.308(a)(4)(ii)(B), 164.308(a)(5)(ii)(A), 164.308(a)(5)(ii)(C), 164.308(a)(6)(ii), 164.312(d)	+ Implements strong authentication requirements that protect electronic protected health information (ePHI) from unauthorized access + Provides visibility into endpoints accessing systems that contain PHI + Provides emergency access options in the event of a lost or stolen authentication method	+ Implements access controls to reduce risks and vulnerabilities + Enforces access policies to ensure that ePHI is not available or disclosed to unauthorized persons + Enforces access restrictions based on group membership to applications with ePHI + Prompts users for self-remediation on devices that don't meet security controls	+ Enables secure BYOD access to ePHI by establishing devices meet minimum security requirements + Establishes security protections for remote access to protected applications containing sensitive ePHI
NERC North American Electric Reliability Corporation CIP005 Table R2 Part 2.3, CIP0076 Table R5 5.1, CIP0102 Table R2 2.1	+ Enforces multi-factor authentication for user access	+ Offers user security training with phishing assessments for user security and audit reporting + Blocks access from unknown sources	+ Enforces controls for remote access to protected resources + Restricts access to managed devices
PCI DSS Payment Card Industry Data Security Standard, Version 4.0 Requiremts: 8.3, 8.4, 8.5	+ Provides strong MFA capabilities to protect access into the cardholder data environment	+ Restricts access to systems and applications containing cardholder data to verified users and healthy devices	+ Validates user identities and establishes trust in devices + Reduces the risk of accessing the cardholder data environment from outside the network

Duo Helps Provide Technical Controls for Data Privacy

With additional requirements around data privacy impacting businesses that have an online presence, there is added complexity for organizations as they strive to implement security solutions to protect operations while rolling out new technologies and keeping employees productive.

Data Privacy Controls	How Duo Editions Help		
	Duo MFA	Duo Access	Duo Beyond
PIPEDA Personal Information Protection and Electronic Documents Act Guidelines for Identification and Authentication	+ Provides strong authentication options for users accessing protected systems	+ Provides the ability to elevate or relax authentication requirements based on application sensitivity with access controls + Restricts access from unknown locations or devices	+ Restricts remote access to applications containing sensitive information + Provides technical controls to deliver external access while protecting internal systems
GDPR EU General Data Protection Regulation (EU) 2016/679 Article 5 Section 1(f) and 2, Article 24 Section 1, Article 32 Section 1(b) and 2	+ Prevents unauthorized access to sensitive information. + Delivers detailed logs of access events	+ Provides granular policy controls to manage and restrict access	+ Provides visibility into which corporate-managed and unmanaged devices are accessing company applications and data
CCPA California Consumer Protection Act Section 1798.150. (a) (1)	+ Verifies users' identities with strong two-factor authentication before granting access to applications that may contain personal information	+ Ensures only trusted and authorized users and healthy devices can access critical business applications and the data they store	+ Ensures that only healthy, trusted devices gain access to sensitive resources and can block unauthorized devices

Duo integrates with the most popular apps, including:

Learn more about supported applications.

Meet Compliance Requirements

Every security best practices guide and regulation asks for MFA and device visibility.

Meet MFA requirements outlined in PCI-DSS 3.2 Section 8.3

Helps meet NIST 800-63 and 800-171 access security requirements

Meet DEAs EPCS requirements when approving e-prescriptions

Aligned with GDPR data protection laws in Europe

Meet FFIEC requirements for financial applications

Get visibility into personal devices used to access PHI

Aligned with PIPEDA guidelines for identification and authentication

FedRAMP approved for public sector organizations and federal agencies

> "Duo has added two-factor authentication to our internal and client-facing solutions with little complication and almost no negative end-user impact."
>
> Ari Perlstein
> Chief Technology Officer, Compliance Discovery Solutions

Duo for Compliance

This resource highlights how Duo's editions address specific areas within the various frameworks, compliance requirements and data privacy guidelines. Duo should be considered as an integral component within overarching security strategies with its agnostic approach that integrates with and compliments other key security solutions in the market that empower organizations to meet compliance requirements.

Duo helps you:

+ Overcome the compliance confusion
+ Gain deep visibility into devices
+ Solve the PIV/CAC conundrum
+ Escape from legacy limbo

> "This is the brilliance of Duo - most people spend so little time interacting with it, as it's so quick and simple, that they barely know they're using it."

Ben Hughes, Network Security Manager, Etsy

Take Duo for a spin

with your **free 30-day trial** and learn why thousands of customers have made us the most loved company in security.

Start at **signup.duo.com.**

Duo Security, now part of Cisco, is the leading multi-factor authentication (MFA) and secure access provider. Duo is a trusted partner to more than 40,000 customers globally, including Yelp, Box, Generali, La-Z-Boy, Eastern Michigan University, Sonic Automotive and more.

Try it for free at duo.com.

Cisco Secure delivers a streamlined, customer-centric approach to security that ensures it's easy to deploy, manage, and use. We help 100 percent of the Fortune 100 companies secure work – wherever it happens – with the broadest, most integrated platform.

Learn more at cisco.com/go/secure.

866.760.4247 **duo.com**