Twingate

Information Security Compliance Standards List

This document contains a list of global and regional compliance certifications, frameworks, regulations, and standards that contain information security or cybersecurity requirements. It is intended as a handy reference guide to IT teams in organizations evaluating compliance requirements.

For a guide to information security compliance for IT teams, read the Twingate Information Security & Compliance Series at: twingate.com/blog/intro-to-infosec-compliance-for-it-teams.

Explanation of Table Columns

Voluntary: "No" means that compliance is legally mandatory, where the standard is applicable to an organization. "Yes" means that compliance is generally voluntary. Note that contractual obligations that an organization voluntary agrees to may convert a voluntary standard into a mandatory one.

Certification Available: "Yes" means that an official certification is required to meet the requirements of the compliance standard, or that official certification is available on a voluntary basis. Certification in this context means that an independent third party evaluates and certifies that the organization seeking certification meets all the requirements of the relevant standard.

Contact

For questions or to submit corrections, email **privacy@twingate.com**. This guide is for general information and does not contain legal advice. Last updated on March 23, 2021.

Abbreviation	Full Name	Focus	Jurisdiction	Subject Matter	Voluntary	Certification Available
201 C.M.R. 17.00	Massachusetts Data Security Regulations	Security	Massachusetts	Regulation that requires businesses to have a comprehensive written information security program with additional requirements for electronic records.	No	No
APPs	Australian Privacy Principles	Privacy	Australia	Covers organizations with an "Australian link" who handle personal information.	No	No
CCPA	California Consumer Privacy Act	Privacy	California	Privacy legislation that covers businesses with operations over certain thresholds who handle personal information of California residents.	No	No
CIS 20	The 20 Center for Internet Critical Security Controls	Security (Controls Framework)	Global	Set of 20 security controls recommended by the CIS.	Yes[1]	No
COBIT	Control Objectives for Information and Related Technologies	Security (Controls Framework)	Global	Set of processes for IT governance.	Yes	No
COPPA	Children's Online Privacy Protection Act	Privacy (Children)	United States	Covers collection of personal information from children under 13 by commercial operators of online sites or services targeted at children.	No	No
COSO	Committee of Sponsoring Organizations of the Treadway Commission	Security (Controls Framework)	Global	A common internal control model against which organizations can evaluate their control systems. Can be used to assist with flexible standards like SOC and SOX.	Yes	No
CPPA	Canada Privacy Protection Act	Privacy	Canada	Proposed privacy legislation that will reform PIPEDA.	No	No
CPRA	California Privacy Rights Act	Privacy	California	New privacy legislation that expands and amends the CCPA and comes into effect on 1/1/2023.	No	No
CSA CAIQ	Cloud Security Alliance - Consensus Assessment Initiative Questionnaire	Security Questionnaire	Global	Standardized industry security controls questionnaire for cloud service providers that assists cloud customers to evaluate the information security and privacy posture of prospective providers.	Yes	Yes
CSA STAR	Cloud Security Alliance - Security Trust Assurance and Risk Program	Security Questionnaire	Global	Industry assurance program for cloud service providers covering security and privacy.	Yes	Yes

[1] While not technically mandatory, in February 2016, the then-Attorney General of California, Kamala Harris, released a report that stating that the CIS Critical Security Controls represent a “minimum level of information that all organizations that collect or maintain personal information should meet” and that failing to implement those controls “constitutes a lack of reasonable security” that is required by a California Privacy law passed in 2004 (AB 1950).

Abbreviation	Full Name	Focus	Jurisdiction	Subject Matter	Voluntary	Certification Available
Cyber Essentials	Cyber Essentials	Security (Controls Framework)	United Kingdom	A UK government information assurance scheme for self-assessment that includes a framework and a set of security controls to protect against internet-originated threats.	Yes	No
Cyber Essentials Plus	Cyber Essentials Plus	Security (Controls Framework)	United Kingdom	Same as cyber essentials, but with independent validations by an accredited third party, performed on an annual basis.	Yes	Yes
FedRAMP	Federal Risk and Authorization Management Program	Security (Government)	United States	Standardized approach to security assessment for cloud products and services adopted by U.S. government agencies. Compliance generally required by cloud service providers who want to supply to the U.S. government.	No	Yes
FERPA	Family Educational Rights and Privacy Act	Privacy (Education)	United States	Privacy legislation covering student education records.	No	No
FIPS	Federal Information Processing Standards	Security (Government)	United States	A set of security requirements maintained by the U.S. government for data, encryption, and other aspects of IT. Pursuant to FISMA, U.S. non-military government agencies and contractors are required to adhere to FIPS.	No	Some[2]
FISMA	Federal Information Security Management Act	Security (Government)	United States	Requires U.S. government agencies to implement security programs to ensure the security of their IT systems and information, including those provided or managed by other agencies or contractors.	No	Yes
FTC Act	Federal Trade Commission Act	Consumer Protection	United States	The FTC uses section 5 of the FTC Act as the enforcement mechanism to support lawsuits against businesses who misrepresent their security practices.	No	No
GDPR	General Data Protection Regulation	Privacy	European Union	Comprehensive privacy legislation regulating the processing of personal data. Covers organizations that are established in the EU or that process personal data of EU residents.	No	No
GLBA	Gramm-Leach-Bliley Act	Privacy (Financial Services)	United States	Covers non-public personal information collected by financial institutions. Includes the Safeguards Rule which requires a written infosec plan.	No	No
HIPAA	Health Insurance Portability and Accountability Act	Privacy (Health)	United States	Privacy legislation for the healthcare sector and their vendors (called "covered entities" and "business associates"). Covers "protected health information" (personally identifiable health-related information).	No	No

[2] For example, FIPS 140-3: *Security Requirements for Cryptographic Modules*.

Abbreviation	Full Name	Focus	Jurisdiction	Subject Matter	Voluntary	Certification Available
HITECH	Health Information Technology for Economic and Clinical Health Act	Privacy (Health)	United States	Expanded HIPAA with additional requirements concerning privacy and security of protected health information.	No	No
ISO 27001	Information Security Management System Requirements	Security (Controls Framework)	Global	International standard that describes the requirements for an Information Security Management System (ISMS).	Yes	Yes
ISO 27002	Code of Practice for Information Security Controls	Security (Controls Framework)	Global	A standard that accompanies ISO 27001. Aids the implementation of ISO 27001 by providing best practice guidance on applying the controls in Annex A of 27001. Organizations do not certify to ISO 27002.	Yes	No
ISO 27017	Code of practice for information Security Controls for Cloud Services	Security (Controls Framework)	Global	Extends on ISO 27002 but provides implementation guidance specifically relating to cloud services.	Yes	No
ISO 27018	Code of Practice for Protection of PII in Public Clouds acting as PII Processors	Security (Controls Framework)	Global	Extends on ISO 27002 but provides implementation guidance specifically relating to protection of PII in the context of public cloud services.	Yes	No
ISO 27032	Guidelines for cybersecurity	Security (Controls Framework)	Global	Provides guidance on management of cybersecurity risks.	Yes	No
ISO 27701	Extension to ISO 27001 and ISO 27002 for Privacy Information Management Requirements and Guidelines	Privacy (Controls Framework)	Global	Extends on ISO 27001 and ISO 27002 regarding Privacy Information Management Systems (PIMS), which are ISMS that are used to process PII. Applies to data controllers and data processors.	Yes	Yes
MPA CSP	Motion Picture Association Content Security Best Practices	Security (Motion Picture Industry)	United States	Security standards promulgated by the MPAA for content protection best practices.	Yes	No
NIST CSF	National Institute of Standards and Technology Cybersecurity Framework	Security (Controls Framework)	United States	Framework providing standards, guidelines and best practices to manage cybersecurity risk. Originally intended for critical U.S. infrastructure providers but flexible enough to be used globally by any type of organization.	Yes	No
Part 11	Title 21 of the Code of Federal Regulations (21 CFR Part 11)	Security (FDA-regulated industries)	United States	Imposes requirements on electronic records to uphold their reliability and trustworthiness for organizations in FDA-regulated industries that use computers for regulated activities.	No	No
PCI DSS	Payment Card Industry Data Security Standard	Security (Payment Cards)	Global	Information security standard for organizations that handle credit cardholder information.	No	Yes

Abbreviation	Full Name	Focus	Jurisdiction	Subject Matter	Voluntary	Certification Available
PIPEDA	Personal Information Protection and Electronic Documents Act	Privacy	Canada	Privacy legislation that covers private sector organizations that handle personal information in connection with commercial activity.	No	No
SHIELD Act	Stop Hacks and Improve Electronic Data Security Act (New York)	Privacy	New York State	State privacy and security legislation that covers organizations that handle personal information of New York residents.	No	No
SOC 1	System and Organization Controls 1	Security	Global	A report prepared by an auditor on Service Organization Controls related to internal controls over financial reporting.	Yes	Yes
SOC 2	System and Organization Controls 2	Security	Global	A report prepared by an auditor on Service Organization Controls related to internal controls for various Trust Services Criteria (Security, Availability, Processing Integrity, Confidentiality, Privacy). Typically intended for an organization's customers.	Yes	Yes
SOC 3	System and Organization Controls 3	Security	Global	A condensed version of a SOC 2 report that can be provided for more general use.	Yes	Yes
TPN Assessment	Trusted Partner Network Assessment	Security (Motion Picture & TV Industry)	United States	A minimum security preparedness benchmark for vendors to the motion picture and television content industry. Vendors completing a TPN assessment are added to the TPN Vendor Roster.	Yes	Yes
VSA	Vendor Security Alliance	Security Questionnaire	Global	Standardized industry security controls questionnaire that assists customers to evaluate the information security posture of prospective vendors.	Yes	No

About Twingate
Twingate was founded with the goal of helping customers easily implement Zero Trust Network Access without compromising security, usability, or performance. We believe that “Work from Anywhere” should just work. Twingate replaces legacy VPNs with a modern Identity-First Networking solution that combines enterprise-grade security with a consumer-grade user experience. It can be set up in less than 15 minutes and integrates with all major cloud providers and IdPs. Twingate helps companies move towards a SASE architecture by tying every network event to an identity—user, device, and resource—giving businesses unparalleled control and visibility over activity across their entire network. Learn more at twingate.com or email sales@twingate.com.