Framework Name	Primary industry intended for	Framework focus	Source	Independent Certification Available?	Who conducts the assessment	What period of time is covered	How long is certification good for?	Number of requirements	URL Resource
ISO 27001	All entities Internationally recognized	Information security management	International Organization for Standardization (ISO) and Internal Electrotechnical Commission (IEC)	Yes	ISO suggests using their search tool to identify accreditation bodies and search for assessors from there https://www.iafcertsearch.org/search/accreditation-bodies	Point in time assessment	3 years (with periodic checks)	14 categories 114 controls	https://www.iso.org
SOC 1	All entities U.S. focused	Controls over financial reporting	American Institute of Certified Public Accountants (AICPA)	Yes	CPA must sign the report	Type 1 report = point in time Type 2 report = 3 to 12 months	1 year	Objectives determined by entity based on SLAs; Typically 5 to 20 objectives with 60 to 150 controls	https://us.aicpa.org/interestareas/frc/assuranceadvisoryservices/socforserviceorganizations
SOC 2	All entities	Controls related to security; optional criteria related to confidentiality, availability, processing integrity or privacy at the reporting entity's discression	American Institute of Certified Public Accountants (AICPA)	Yes	CPA must sign the report	Type 1 report = point in time Type 2 report = 3 to 12 months	1 year	5 categories possible 61 criteria possible Typically 80 to 150 controls	https://us.aicpa.org/interestareas/frc/assuranceadvisoryservices/socforserviceorganizations
NIST Cybersecurity Framework	U.S. private-sector owners and operators of critical infrastructure	Cybersecurity management	National Institute of Standards and Technology (NIST) is part of U.S. Department of Commerce	No formal certification, but many third parties perform assessments	n/a	n/a	n/a	5 functions 23 categories 108 subcategories	https://www.nist.gov/cyberframework
COBIT	All entities U.S. focused	IT management best practices	Information Systems Audit and Control Association (ISACA)	No entity certification, but individuals can become certified through ISACA	n/a	n/a	n/a	5 principles 7 aspects 40 objectives	https://www.isaca.org/resources/cobit
HITRUST CSF	All entities	Compliance and risk management	HITRUST Alliance	Yes	HITRUST assessor firm	Point in time assessment, controls must be in place for 90 days	2 years (with interim assessment) 1 year version also	14 categories 19 domains 49 control objectives 156 control references 3 implementation levels	https://hitrustalliance.net/product-tool/hitrust-csf/
CIS	All entities	Cybersecurity management	Center for Internet Security	No, self-assessment only	n/a	n/a	n/a	18 controls 153 safeguards	https://www.cisecurity.org/
HIPAA	Entities that process PHI and ePHI	Privacy and security of PHI	U.S. Department of Health and Human Services (HHS)	No formal certification, but many third parties perform assessments	n/a	n/a	n/a	4 general rules Around 17 requirements	https://www.hhs.gov/hipaa/for-professionals/privacy/index.html
GDPR	Entities that process personal data of citizens of the EU and UK	Personal data use, transfer and retention	EU Law	No formal certification, but some 3rd parties perform assessments	n/a	n/a	n/a	7 principles 11 chapters 99 articles	https://gdpr-info.eu/
PCI DSS	Entities that process credit card information	Security of cardholder data	PCI Security Standards Council	Yes	Qualified security assessors (however, depending on program, may be able to self-assess)	Point in time assessment	1 year	12 requirements may be over 300 subrequirements	https://www.pcisecuritystandards.org/