Regulatory Compliance Checklist

FFIEC/GLBA · PCI DSS v4.0 · NIST CSF 2.0 · ISO/IEC 27001:2022 · SOC 2

Use this checklist to assess your organization's alignment with key security and compliance frameworks. This is a high-level reference tool — not a substitute for a formal compliance assessment.

FFIEC / GLBA

Federal Financial Institutions Examination Council / Gramm-Leach-Bliley Act

Applies to: Banks, credit unions, mortgage companies, insurance firms, tax preparers, financial advisors, and any business that provides financial products or services to consumers.

☐	Control / Requirement	Category	Priority	Notes
☐	Cybersecurity Assessment Tool (CAT)	Governance & Risk	Required	
☐	Documented information security program	Governance & Risk	Required	
☐	Annual risk assessment of IT systems	Risk Management	Required	
☐	Board-level oversight of cybersecurity program	Governance & Risk	Required	
☐	Multi-factor authentication for all remote access	Access Controls	Required	
☐	Employee security awareness training annually	Awareness & Training	Required	
☐	Vendor/third-party risk management program	Third-Party Risk	Required	
☐	Incident response plan documented and tested	Incident Response	Required	
☐	Safeguards Rule compliance (for GLBA-covered entities)	GLBA Safeguards	Required	
☐	Data encryption for customer financial information	Data Protection	Required	
☐	Access controls and user authentication controls	Access Controls	Required	
☐	Penetration testing or vulnerability assessments	Technical Controls	Recommended	
☐	Continuous monitoring of security controls	Monitoring	Recommended	
☐	Network segmentation and firewall controls	Technical Controls	Recommended	

■	Customer notification procedures for breaches	Incident Response	Required	
■	Audit logs retained for minimum required periods	Logging & Audit	Required	

PCI DSS v4.0

Payment Card Industry Data Security Standard v4.0

Applies to: Any organization that stores, processes, or transmits payment card data — including merchants, payment processors, service providers, and any technology involved in card handling.

■	Control / Requirement	Category	Priority	Notes
■	Install and maintain network security controls (firewalls)	Req 1 – Network Security	Required	
■	Apply secure configurations to all system components	Req 2 – Secure Configs	Required	
■	Protect stored account data with encryption	Req 3 – Data Protection	Required	
■	Protect cardholder data in transit with TLS 1.2+	Req 4 – Encryption in Transit	Required	
■	Protect all systems against malware (AV/EDR)	Req 5 – Anti-Malware	Required	
■	Develop and maintain secure systems and software	Req 6 – Secure Development	Required	
■	Restrict access to cardholder data by business need-to-know	Req 7 – Access Control	Required	
■	Identify users and authenticate access to system components	Req 8 – Identity & Auth	Required	
■	Restrict physical access to cardholder data	Req 9 – Physical Security	Required	
■	Log and monitor all access to network resources and cardholder data	Req 10 – Logging	Required	
■	Test security of systems and networks regularly	Req 11 – Testing	Required	
■	Support information security with org policies and programs	Req 12 – Policies	Required	
■	Maintain a cardholder data environment (CDE) scope document	Scoping	Required	
■	Conduct annual Self-Assessment Questionnaire (SAQ) or QSA audit	Compliance Assessment	Required	

■	Customized approach option documentation (if applicable)	Req 12 – Policies	Best Practice	
■	Targeted risk analysis for applicable requirements	Risk Management	Required	
■	Multi-factor authentication for all access into the CDE	Req 8 – Identity & Auth	Required	

NIST CSF 2.0

National Institute of Standards and Technology Cybersecurity Framework 2.0

Applies to: All organizations. Widely used as a voluntary framework for managing cybersecurity risk — increasingly referenced in contracts, cyber insurance applications, and regulatory guidance.

■	Control / Requirement	Category	Priority	Notes
■	Organizational cybersecurity risk strategy documented (GV.OC)	GOVERN – Context	Required	
■	Cybersecurity roles, responsibilities, and authorities defined (GV.RR)	GOVERN – Roles	Required	
■	Asset inventory maintained for hardware and software (ID.AM)	IDENTIFY – Assets	Required	
■	Risk assessment process documented and performed (ID.RA)	IDENTIFY – Risk	Required	
■	Identity management and access control implemented (PR.AA)	PROTECT – Access	Required	
■	Data security controls implemented for sensitive data (PR.DS)	PROTECT – Data	Required	
■	Security awareness and training program in place (PR.AT)	PROTECT – Training	Required	
■	Protective technology and platform security deployed (PR.PS)	PROTECT – Platform	Recommended	
■	Anomalies and adverse events detected (DE.AE)	DETECT – Events	Required	
■	Continuous security monitoring implemented (DE.CM)	DETECT – Monitoring	Recommended	
■	Incident response plan documented and communicated (RS.MA)	RESPOND – Management	Required	
■	Incident analysis and reporting process defined (RS.AN)	RESPOND – Analysis	Required	
■	Recovery plan developed and maintained (RC.RP)	RECOVER – Recovery	Required	

■	Supply chain / vendor risk management program (GV.SC)	GOVERN – Supply Chain	Recommended	
■	Cybersecurity policy reviewed and approved by leadership (GV.PO)	GOVERN – Policy	Required	
■	Improvement plans developed from incidents and assessments (RS.IM)	RESPOND – Improvement	Best Practice	
■	Communication with stakeholders during incidents (RS.CO)	RESPOND – Comms	Required	

ISO/IEC 27001:2022

International Organization for Standardization / Information Security Management System

Applies to: Organizations pursuing formal ISMS certification or using ISO 27001 as a framework for systematic information security management. Common in enterprise, government, and multinational contexts.

■	Control / Requirement	Category	Priority	Notes
■	Scope of the ISMS documented (Clause 4.3)	Context & Scope	Required	
■	Information security policy established and communicated (Clause 5.2)	Leadership	Required	
■	Information security objectives set (Clause 6.2)	Planning	Required	
■	Risk assessment methodology documented (Clause 6.1.2)	Risk Assessment	Required	
■	Risk treatment plan developed and implemented (Clause 6.1.3)	Risk Treatment	Required	
■	Statement of Applicability (SoA) maintained (Clause 6.1.3)	Annex A Controls	Required	
■	Competence and awareness training for staff (Clause 7.2–7.3)	Support	Required	
■	Documented information (records) management (Clause 7.5)	Support	Required	
■	Internal audit program implemented (Clause 9.2)	Performance	Required	
■	Management review of the ISMS conducted (Clause 9.3)	Performance	Required	
■	Nonconformity and corrective action process (Clause 10.2)	Improvement	Required	
■	Supplier relationships / vendor security controls (Annex A 5.19–5.22)	Annex A Controls	Required	

■	Access control policy and user provisioning (Annex A 5.15–5.18)	Annex A Controls	Required	
■	Cryptographic controls policy (Annex A 8.24)	Annex A Controls	Required	
■	Incident management process (Annex A 5.24–5.28)	Annex A Controls	Required	
■	Business continuity / backup procedures (Annex A 8.13)	Annex A Controls	Required	
■	Threat intelligence program (Annex A 5.7)	Annex A Controls	Best Practice	
■	Secure coding / SSDLC practices (Annex A 8.25–8.31)	Annex A Controls	Recommended	

SOC 2

Service Organization Control 2 — AICPA Trust Services Criteria

Applies to: SaaS companies, cloud service providers, data centers, and technology vendors that store or process customer data. Increasingly required by enterprise customers and regulated industries.

■	Control / Requirement	Category	Priority	Notes
■	CC1: Control environment — values, board oversight, structure (CC1.1–CC1.5)	Common Criteria – CC1	Required	
■	CC2: Communication of security information (CC2.1–CC2.3)	Common Criteria – CC2	Required	
■	CC3: Risk assessment process documented (CC3.1–CC3.4)	Common Criteria – CC3	Required	
■	CC4: Monitoring of controls effectiveness (CC4.1–CC4.2)	Common Criteria – CC4	Required	
■	CC5: Control activities and policies deployed (CC5.1–CC5.3)	Common Criteria – CC5	Required	
■	CC6: Logical access controls (MFA, provisioning, removal) (CC6.1–CC6.8)	Common Criteria – CC6	Required	
■	CC7: System operations monitoring and incident management (CC7.1–CC7.5)	Common Criteria – CC7	Required	
■	CC8: Change management process for system changes (CC8.1)	Common Criteria – CC8	Required	
■	CC9: Risk mitigation including vendor risk (CC9.1–CC9.2)	Common Criteria – CC9	Required	
■	Availability criteria — uptime commitments and monitoring (A1.1–A1.3)	Availability	Recommended	

■	Confidentiality criteria — data handling and disposal (C1.1–C1.2)	Confidentiality	Recommended	
■	Processing Integrity — complete, accurate processing (PI1.1–PI1.5)	Processing Integrity	Recommended	
■	Privacy criteria — personal information lifecycle (P1–P8)	Privacy	Recommended	
■	Penetration testing conducted and findings remediated	Supplemental	Recommended	
■	Continuous monitoring and alerting implemented	Supplemental	Best Practice	
■	Vendor review and evidence collection process	Supplemental	Recommended	
■	Audit report preparation and evidence management	Supplemental	Required	

Compliance Summary

Framework	Items	Completed ✓	In Progress	Gap / Not Started	N/A
FFIEC / GLBA	16	_____	_____	_____	_____
PCI DSS v4.0	17	_____	_____	_____	_____
NIST CSF 2.0	17	_____	_____	_____	_____
ISO/IEC 27001:2022	18	_____	_____	_____	_____
SOC 2	17	_____	_____	_____	_____

Required Baseline control required for compliance

Recommended Strongly advised; expected by auditors

Best Practice Enhances posture; differentiates mature programs