

FinTech & Financial Services Compliance Assessment

Evaluate your technology vendor's readiness across PCI DSS, SOX, GLBA, DORA, and AML/KYC obligations.

Contents

- 01 Regulatory Frameworks Covered
- 02 PCI DSS Controls
- 03 SOX IT General Controls
- 04 AML / KYC Obligations
- 05 DORA (Digital Operational Resilience Act)
- 06 Scoring Guide
- 07 Next Steps

01 – REGULATORY FRAMEWORKS COVERED

- PCI DSS v4.0
- SOX Section 404
- GLBA
- DORA (EU)
- AML / KYC

This assessment covers the primary regulatory and compliance frameworks your technology vendor must address. Each section below maps directly to one or more of these frameworks.

02 - PCI DSS CONTROLS

- Cardholder data environment (CDE) scoped and documented
- Network segmentation between CDE and other systems
- Penetration test conducted within last 12 months
- Vulnerability scans conducted quarterly
- Strong cryptography on all cardholder data transmissions
- Multi-factor authentication on CDE administrative access
- File integrity monitoring on critical system files

03 – SOX IT GENERAL CONTROLS

- Change management process documented and enforced
- Access provisioning tied to role-based approval workflow
- Privileged access reviewed quarterly
- Logical access controls over financial systems documented
- IT controls tested by internal audit annually
- Segregation of duties enforced in financial systems

04 - AML / KYC OBLIGATIONS

- Customer Due Diligence (CDD) procedures documented
- Enhanced Due Diligence (EDD) applied to high-risk customers
- Transaction monitoring system calibrated and tested
- SAR filing process documented
- OFAC / sanctions screening real-time or same-day
- Record retention for 5 years minimum

05 – DORA (DIGITAL OPERATIONAL RESILIENCE ACT)

- ICT risk management framework documented
- Major ICT incident classification and reporting procedure defined
- Threat-led penetration testing (TLPT) plan in place
- Third-party ICT provider register maintained
- Business continuity and disaster recovery tested

SCORING GUIDE

Score 1 point for each confirmed item. 24–27: Compliant. 17–23: Needs remediation. Below 17: Urgent review required.

NEXT STEPS

If your score falls below the compliant threshold, The Algorithm offers a structured gap remediation programme:

1. Technical gap audit (2 weeks)
2. Remediation roadmap with prioritised backlog
3. Engineering sprint to close critical gaps
4. Evidence package for regulatory review

Contact us at contact@the-algo.com or visit the-algo.com/contact

Ready to talk?

We audit your current vendor, map the gaps, and present a structured migration plan — no commitment required.

the-algo.com/contact