NetSPI™

Matrix: Security Testing Requirements in the Financial Industry

Companies that perform business within the financial industry, including banking, insurance, and investment companies, operate under a rigorous framework of regulations designed to safeguard sensitive data and ensure digital resilience. From FedRAMP to PCI DSS, navigating these requirements, particularly those pertaining to security testing, is critical for compliance and robust defense against evolving cyber threats. The following matrix offers a comprehensive overview of key security testing mandates and recommendations from prominent regulations and standards globally. Familiarity with these governing bodies and their testing requirements is essential for financial institutions to proactively establish effective security postures, mitigate risk, and maintain the trust of their stakeholders and regulators.

To meet these stringent compliance demands, regular and thorough penetration testing across the entire digital estate is no longer a nice-to-have, but a must-have. This includes rigorous testing of internal and external networks, AI projects, mobile applications, APIs, web applications, hybrid cloud environments, and third-party supply chains.

To navigate the complex landscape of regulations, organizations must adopt a proactive and programmatic approach to security testing. This ensures that vulnerabilities are identified and addressed before adversaries can exploit them, supporting both compliance and resilience. The following matrix outlines the essential security testing mandates and recommendations from leading global standards and regulators, providing financial institutions and related businesses with a clear framework to strengthen their security posture and maintain stakeholder trust.

Defining Common Acronyms

3PAO: Third Party Assessment Organization

CAT: Cybersecurity Assessment Tool

DAST: Dynamic Application Security Testing

DORA: Digital Operational Resilience Act

EAL: Evaluation Assurance Level

FedRAMP: US Federal Risk and Authorization Management Program

FFIEC: Federal Financial Institutions Examination Council

GLBA: Gramm-Leach-Bliley Act

ICT: Information and Communications Technology

IoT: Internet of Things

ISO/IEC: International Organization for Standardization/ International Electrotechnical Commission

ITGC: Information Technology General Controls

MAS TRM: Monetary Authority of Singapore Technology Risk Management Guidelines

NIS2: Network and Information Security Directive 2

NYDFS: New York Department of Financial Services

PCI DSS: Payment Card Industry Data Security Standard

PII: Personally Identifiable Information

SOX: Sarbanes-Oxley Act

NetSPI™

Security Testing Requirements in Financial Services

This matrix overviews binding financial regulations (such as PCI DSS, GLBA, DORA, and NIS2) with widely adopted security standards and guidance (such as ISO/IEC 27001/27002).

KEY: Required | Recommended

Regulation / Standard	Summary	Explicit Test Types Required	Cloud Pentesting Required?	On-Prem / Infra Test Required?	Frequency	Third-Party / Regulator Witness?
GLOBAL STANDARDS						
PCI DSS (Global)	Applies to any organization that stores, processes, or transmits cardholder data.	Annual internal and external penetration testing (and after significant changes); quarterly internal and external vulnerability scans; application security testing for public-facing web apps	if cardholder data is in the cloud		**Pentesting:** Annually **Scans:** Quarterly	**Yes**—ASV for scans; Pentesting validation by qualified tester
DORA (EU)	Focuses on operational resilience for critical financial entities.	TLPT (Threat-Led Pentesting), Red Team, Vulnerability Assessments, Threat Modeling	for critical ICT services	for critical on-prem systems	For systems designated as 'Significant' by Testing Authorities, every 3 years (min); more if material changes	**Yes**—qualified external tester; regulator oversight possible
NIS2 (EU)	Broad directive for "essential" and "important" entities, including financial infrastructure.	Appropriate and proportionate technical, operational and organizational measures, such as Pentesting, Vulnerability Scans, Risk Assessments			Variable; risk-based	**Possible,** if required by Member State
MAS TRM (Singapore)	Mandates rigorous testing for financial institutions regulated by the Monetary Authority of Singapore.	Pentesting, Red Teaming encouraged, Secure Code Review (SAST), Vulnerability Scans	for cloud-hosted critical systems		At least annually for internet-facing systems; more for high-risk	**Yes**—independent tester; regulator can request results
U.S. STANDARDS						
FedRAMP (US Federal)	For Cloud Service Providers selling to US federal agencies.	3PAO-performed pentesting, Continuous Vulnerability Scanning, Risk Assessment	part of annual reassessment for all FedRAMP-authorized cloud systems	N/A (cloud-focused)	**Pentesting:** Annually; **Scans:** Monthly+	**Yes**—by FedRAMP-recognized 3PAO
FFIEC Guidelines/CAT (US Banking)	Interagency guidance for federally supervised financial institutions. (CAT is voluntary.)	Pentesting, Red Teaming as part of advanced/best practice			Risk-based, often annual for critical systems; aligned with institution's risk appetite.	**Optional;** recommended for third parties
GLBA (US)	Requires financial institutions to protect consumer financial information.	Safeguards Rule testing per recent FTC guidance includes pentesting and vulnerability assessments			Periodic; risk-based	**Optional**

Security Testing Requirements in Financial Services *(Continued)*

KEY: Required / Recommended

Regulation / Standard	Summary	Explicit Test Types Required	Cloud Pentesting Required?	On-Prem / Infra Test Required?	Frequency	Third-Party/ Regulator Witness?
U.S. STANDARDS *(CONTINUED)*						
SOX (US)	Focuses on controls over financial reporting; security testing supports control effectiveness.	IT General Controls (ITGC) testing	as part of ITGC, but not a direct SOX obligation	as part of ITGC conclusions, but not a direct SOX obligation	Annual	**External Auditor**
State Regulations (e.g., NYDFS 23 NYCRR 500)	Varies by state; NYDFS is a common benchmark for the financial sector.	Risk Assessments, Vulnerability Assessments, Pentesting			Annual pentesting and bi-annual vulnerability assessments, plus additional risk-based testing	**Optional**
ISO/IEC STANDARDS						
ISO/IEC 27001	Risk-based pentesting is an accepted method to meet Annex A controls.	Vulnerability Management, Technical Compliance Reviews			Required by risk-tolerance and ISMS plan and as part of risk audits.	**External auditor for certification**
ISO/IEC 27002	Recommends Pentesting as a method to verify control effectiveness for ISO 27001.	N/A (guidance document)			N/A	N/A
ISO/IEC 27005	Threat modeling and risk assessment drive the selection of appropriate testing.	N/A (risk management)	as part of risk treatment	as part of risk treatment	N/A	N/A
ISO/IEC 27035	Positions testing as a tool to improve incident detection and response readiness.	N/A (incident management)	for pre-paredness	for pre-paredness	N/A	N/A
ISO/IEC 27034-1	Specifies security testing as a verification method within the application security lifecycle but does not specify a fixed set of tests.	Pentesting, Threat Modeling, Code Review	as part of SDLC for cloud apps	as part of SDLC; applies across deployment models; all environments used by the application should be in scope based on risk.	Aligned with development lifecycle	**Optional**
ISO/IEC 15408 (Common Criteria)	Mandates formal pentesting, especially at higher Evaluation Assurance Levels (EAL4+).	Pentesting against defined attack potential	if product is cloud-based	if product has on-prem components	During evaluation	**Yes**—by licensed evaluation lab

Security Testing Requirements in Financial Services *(Continued)*

KEY: Required / Recommended

Regulation / Standard	Summary	Explicit Test Types Required	Cloud Pentesting Required?	On-Prem / Infra Test Required?	Frequency	Third-Party/ Regulator Witness?
ISO/IEC STANDARDS *(CONTINUED)*						
ISO/IEC 29147 & 30111	Testing is used to validate reported vulnerabilities and verify fixes.	N/A (vulnerability disclosure/ handling)	N/A	N/A	As needed	N/A
ISO/IEC 27017 & 27018	Recommends both provider and customer conduct testing to validate cloud security.	N/A (cloud controls/PII)	risk-based, shared responsibility	N/A	Periodic; risk-based	**Optional**
ISO/IEC 27400	Specifies security assessment activities for IoT and connected devices.	Security Assessments, Threat Modeling			Aligned with product lifecycle	**Optional**
ISO/IEC 19790	Requires testing to assess resistance to known attacks for cryptographic module validation.	Pentesting of cryptographic module	if module is software/ cloud-based	if module is hardware	During validation	**Yes**—by accredited lab

Achieve Compliance and More with NetSPI

To protect against evolving threats and maintain compliance, organizations must build an operational approach that prioritizes their commitment to maintaining customer trust. The compliance standards and security testing best practices explained above outline that approach. This includes continuous testing of the areas often exploited by adversaries, such as internal and external networks, mobile applications, and APIs.

NetSPI's comprehensive security testing services empower financial entities to proactively address critical vulnerabilities, strengthen their security postures, and ensure alignment with complex and evolving regulations. Let's advance your security testing strategy together.

Contact NetSPI