Rocket® software

DORA and PCI DSS Audit Readiness for Banks: A Practical Checklist

Staying ahead of evolving regulations like the Digital Operational Resilience Act (DORA) and Payment Card Industry Data Security Standard (PCI DSS) is critical for maintaining operational integrity and customer trust.

This checklist helps you benchmark your current audit readiness for core banking systems, identify potential gaps, and understand the significant costs associated with inaction.

The cost of inaction: Quantifying the risk

Failing to meet DORA and PCI DSS compliance standards exposes your bank to severe consequences that extend far beyond audit findings. Understanding these financial and reputational costs underscores the urgency of modernizing your security controls.

Regulatory fines:

Non-compliance can lead to staggering financial penalties. DORA allows for fines up to €10 million or 2% of total annual worldwide turnover, whichever is higher. PCI DSS violations can result in monthly penalties ranging from $5,000 to $100,000 and increased transaction fees from payment card brands.

Operational disruption:

A security breach or failed audit can trigger mandatory operational shutdowns, forensic investigations, and system remediation efforts. The average cost of a data breach in the financial industry reached $5.9 million in 2023, driven by downtime and recovery expenses.

Reputational damage:

Customer trust is a bank's most valuable asset. A public breach erodes confidence, leading to customer churn and difficulty attracting new business. The long-term impact on your brand's reputation can far exceed the immediate financial costs.

Audit-readiness checklist

Use the following checklist to evaluate your current security posture for core systems and identify areas for improvement.

01 Identity and access management (IAM)

Implement multi-factor authentication (MFA)

Do you enforce MFA for all users accessing core banking systems, especially those with privileged access? *(DORA Article 9; PCI DSS Requirement 8.3)*

Enforce the principle of least privilege

Is user access strictly limited to the minimum data and functions required for their job role? *(DORA Article 9; PCI DSS Requirement 7.2)*

Centralize access control

Can you manage access policies for host systems from a central IAM platform to ensure consistency with enterprise-wide rules?

Implement multi-factor authentication (MFA):

Do you enforce MFA for all users accessing core banking systems, especially those with privileged access? *(DORA Article 9; PCI DSS Requirement 8.3)*

Enforce the principle of least privilege

Is user access strictly limited to the minimum data and functions required for their job role? *(DORA Article 9; PCI DSS Requirement 7.2)*

02 Security controls and network management

Encrypt data in transit

Is all sensitive data, including cardholder information and personally identifiable information (PII), protected with strong encryption (e.g., TLS 1.2 or higher) during transmission? *(DORA Article 9; PCI DSS Requirement 4.1)*

Isolate critical systems

Are your core banking systems segmented from less secure networks to prevent unauthorized lateral movement? *(PCI DSS Requirement 1.3)*

Secure remote access

Do you enforce unique authentication credentials and MFA for all remote access sessions into your core systems? *(PCI DSS Requirement 8.4)*

Manage system configurations securely

Have you disabled unnecessary services and default accounts on your host systems to reduce the attack surface? *(PCI DSS Requirement 2.2)*

03 Audit trails and monitoring

Generate comprehensive audit logs

Does your system create detailed, immutable logs for all user activity, including logins, commands executed, and data accessed? *(DORA Article 10; PCI DSS Requirement 10.2)*

Centralize log management

Are all audit logs from core banking systems consolidated into a central security information and event management (SIEM) tool for continuous monitoring? *(PCI DSS Requirement 10.5)*

Protect audit trails from tampering

Are access controls in place to prevent the alteration or deletion of log data? *(PCI DSS Requirement 10.6)*

Review logs daily

Do you have automated alerts and a formal process for reviewing logs daily to detect and respond to suspicious activity? *(PCI DSS Requirement 10.4)*

Retain logs for at least one year

Are audit trails stored for a minimum of 12 months, with at least the last three months immediately available for analysis? *(PCI DSS Requirement 10.3)*

Partner with Rocket Software for seamless compliance

Completing this checklist is the first step toward building a more secure and compliant banking operation. If you identify gaps in your environment, you don't have to navigate them alone. Rocket Software can help you close these vulnerabilities with advanced access solutions designed for mission-critical systems.

With Rocket® Secure Host Access™, you can achieve comprehensive compliance adherence, seamless IAM integration, and flawless audit excellence.
We empower you to modernize your legacy infrastructure while maintaining a secure, user-friendly experience. Partner with us to protect your sensitive data, enhance your security posture, and confidently prepare for your next audit.

Rocket® software

Modernization. **Without Disruption.**™

Visit RocketSoftware.com

MAR-17718_DORA _PCI_DSS_Audit_A_Practical_Checklist_infographic_v4