COMPLIANCE AUDIT REPORT

PCI-DSS 4.0 Assessment

AegisPay Financial Services Pvt

Report Generated: January 05, 2026 at 12:20

80%

Overall Compliance Score

POSTURE: GOOD

Generated by ComplianceOS Agentic Platform

EXECUTIVE SUMMARY

This report presents the findings of an automated compliance assessment conducted against PCI-DSS 4.0 requirements. The assessment evaluated 14 control requirements across 6 key security domains. The organization achieved a compliance score of 80%, with 12 requirements fully satisfied and 4 gaps identified requiring remediation.

Key Metrics

Metric	Value
Compliance Score	80%
Security Posture	GOOD
Requirements Assessed	14
Requirements Met	12
Gaps Identified	4
Critical Issues	0

PCI-DSS 4.0 COMPLIANCE CHECKLIST

ID	Category	Requirement	Status
1.1	Network Security	Install and maintain network security controls	PASS
1.2	Network Security	Secure all system components from unauthorized access	PASS
2.1	Secure Configurati	Apply secure configurations to all system components	PASS
3.1	Data Protection	Protect stored account data using encryption	FAIL
3.2	Data Protection	Sensitive authentication data is not stored after authorization	FAIL
4.1	Transmission Secur	Protect cardholder data with strong cryptography during transmiss	PASS
5.1	Malware Protection	Protect all systems against malware	PASS
6.1	Secure Development	Develop and maintain secure systems and software	PASS
7.1	Access Control	Restrict access to system components by business need-to-know	PASS
8.1	Identity Managemen	Identify users and authenticate access to system components	PASS
9.1	Physical Security	Restrict physical access to cardholder data	PASS
10.1	Logging & Monitori	Log and monitor all access to system components and cardholder da	PASS
11.1	Security Testing	Test security of systems and networks regularly	PASS
12.1	Security Policy	Support information security with organizational policies	PASS

DETAILED FINDINGS

Finding #1: Encrypt stored cardholder data

Severity: High

Description: Using Tool: RiskScorer

Finding #2: Encrypt stored cardholder data

Severity: High

Description: Risk Scored: High (Impact: High)

Finding #3: Encrypt stored cardholder data

Severity: High

Description: Auto-Remediation DISABLED. Finding requires manual review.

Finding #4: Encrypt stored cardholder data

Severity: High

Description: Based on the provided regulation (GDPR Art. 30), the policy is missing a clear data retention schedule. RISK: HIGH.

MISSING SECURITY CONTROLS

Based on the 80% compliance score, the following security controls require attention:

1. [3.1] Data Protection

Requirement: Protect stored account data using encryption

- Implement AES-256 encryption for all sensitive data at rest

- Use TLS 1.3 for data in transit

2. [3.2] Data Protection

Requirement: Sensitive authentication data is not stored after authorization

- Implement AES-256 encryption for all sensitive data at rest

- Use TLS 1.3 for data in transit

RECOMMENDATIONS

Based on the 4 gap(s) identified, we recommend the following immediate actions:

1. Prioritize Critical and High severity findings for immediate remediation
2. Develop a remediation timeline with specific milestones
3. Assign ownership for each finding to appropriate team members
4. Implement compensating controls where immediate fixes are not possible
5. Schedule a follow-up assessment within 30 days
6. Document all remediation activities for audit evidence

This report was automatically generated by ComplianceOS Agentic AI Platform.
Assessment Date: 2026-01-05
Report Version: 2.0