LogZilla for Financial Services

PCI-DSS Compliance, Fraud Detection, and Regulatory Reporting

PCI-DSS	Real-time	SOX	AI
Requirement 10 Ready	Fraud Detection	Audit Trails	Copilot Included

The Financial Services Challenge

Regulatory and Security Pressure:

- **PCI-DSS compliance**: Cardholder data protection
- **SOX requirements**: Financial system audit trails
- **Fraud detection**: Real-time transaction monitoring
- **Examiner scrutiny**: OCC, FDIC, state regulators
- **Cyber threats**: Financial sector is top target

The AI Advantage

Financial-Grade Intelligence:

- **Fraud patterns**: AI detects anomalies in real-time
- **Compliance automation**: PCI, SOX evidence generation
- **Transaction monitoring**: Suspicious activity alerts
- **Examiner-ready reports**: Minutes, not weeks
- **Insider threat detection**: Behavioral analysis

PCI-DSS Requirement 10 Coverage

Requirement	Description	Status
10.1	Audit trail implementation	Supports
10.2	Automated audit trails	Supports
10.3	Record specific events	Supports
10.4	Time synchronization	NTP
10.5	Secure audit trails	Immutable
10.6	Review logs daily	AI-Assisted
10.7	Retain 1 year	Configurable

QSA-Ready: LogZilla provides the audit trail evidence and daily log review documentation required for PCI-DSS assessments.

AI-Powered Fraud Detection

Fraud Analyst prompt: "Analyze all transaction anomalies in the last 24 hours with account takeover indicators."

```
FRAUD DETECTION SUMMARY
Period: Last 24 Hours | Transactions: 2.4M | Alerts: 47
═══════════════════════════════════════════

HIGH PRIORITY ALERTS:

1. ACCOUNT TAKEOVER SUSPECTED
   Account: ****4521 | Customer: J. Smith
   Indicators:
     - Password reset from new device
     - Immediate wire transfer request ($47,500)
     - Destination: First-time recipient
     - Location: 2,400 miles from normal
   Status: BLOCKED - Customer contacted

2. CARD-NOT-PRESENT FRAUD PATTERN
   Cards Affected: 23 (same BIN range)
   Pattern: Small test charges → Large purchases
   Merchant: Online electronics retailer
   Total Attempted: $127,450
   Status: BLOCKED - Cards reissued

TRANSACTION RISK SCORES:
  Low Risk:    2,387,412 (99.4%)
  Medium Risk:     12,341 (0.5%)
  High Risk:          247 (0.01%)
```

AI Use Cases for Financial

Use Case	Traditional	With AI
Fraud pattern detection	Hours/Days	**Real-time**
PCI audit evidence	2-4 weeks	**Minutes**
SOX compliance report	Weeks	**Minutes**
Suspicious activity report	4-8 hours	**30 min**
Examiner data request	Days	**Minutes**

Transaction Monitoring

- **Wire transfers**: Velocity and destination analysis
- **ACH**: Pattern deviation detection
- **Card transactions**: CNP fraud patterns
- **Account changes**: Takeover indicators

SOX Compliance and Audit Trails

Compliance Officer prompt: "Generate SOX Section 404 evidence for financial system access controls Q4 2024."

```
SOX SECTION 404 COMPLIANCE EVIDENCE
Period: Q4 2024 | Systems: Core Banking, GL, Treasury
═══════════════════════════════════

ACCESS CONTROL EFFECTIVENESS:

Core Banking System:
  Privileged Users: 23 (all authorized)
  Access Reviews: Quarterly (completed 10/15, 12/15)
  Segregation of Duties: ✓ No violations
  Failed Auth Attempts: 847 (all investigated)

General Ledger:
  Journal Entry Access: 12 users
  Approval Workflow: ✓ Enforced
  Override Events: 3 (all documented)
  Audit Trail: ✓ Complete

Treasury Management:
  Wire Approval: Dual control enforced
  Limit Exceptions: 0
  Reconciliation: Daily (automated)

EVIDENCE ARTIFACTS GENERATED:
  - access_review_q4.pdf
  - segregation_matrix.xlsx
  - exception_report.pdf
  - audit_trail_summary.csv
```

Regulatory Framework Support

Framework	Coverage
PCI-DSS 4.0	Requirement 10
SOX Section 404	IT Controls
GLBA	Safeguards Rule
FFIEC	CAT Assessment
BSA/AML	SAR Support
NYDFS 500	Cybersecurity

Insider Threat Detection

```
INSIDER THREAT INDICATORS
═══════════════════════════════════

User: analyst_jdoe
Risk Score: 78/100 (elevated)

Behavioral Anomalies:
  - After-hours access: +340% vs baseline
  - Customer record queries: +520%
  - Data export volume: 12GB (10x normal)
  - Accessed terminated employee data

Recommendation: HR/Security review
```

Deployment Options

On-Premises

- Bank data center
- Full data control
- Examiner-ready
- Air-gap option

Private Cloud

- Customer-managed
- Dedicated instance
- Full data control
- Scalable architecture

Hybrid

- Sensitive data on-prem
- Analytics in cloud
- Encrypted transport
- Flexible retention

Why Financial Institutions Choose LogZilla

Metric	Improvement
PCI audit prep time	90% faster
Fraud detection speed	Real-time
Examiner response time	Hours vs Days
SIEM/storage costs	70-90% savings

Financial-Specific Benefits:

- **Compliance**: PCI, SOX, GLBA ready
- **Fraud prevention**: AI-powered detection
- **Examiner-ready**: Evidence on demand
- **Cost reduction**: Consolidate tools

Protect assets, detect fraud, simplify compliance.

sales@logzilla.net | www.logzilla.net