ATM Security Assessment

Methodology and Testing Checklist

Document Version	1.0
Prepared By	Lorikeet Security
Contact	lorikeetsecurity.com

1. Executive Overview

> *A structured, vendor-neutral framework for assessing ATM security across physical, software, network, and compliance domains.*

Lorikeet Security delivers ATM penetration testing engagements through a structured, multi-phase methodology aligned to industry standards including PCI DSS v4.0, PCI PTS, NIST SP 800-series, and EMVCo specifications. Our approach is designed to be vendor-agnostic and covers all major ATM platforms including NCR, Diebold Nixdorf, Hyosung, and Nautilus Hyosung.

Each assessment is scoped and authorized prior to commencement, with explicit written authorization covering all active testing activities. Destructive testing (e.g., cash dispenser simulation) is conducted under controlled conditions with the customer's operations team present or on standby.

2. Assessment Methodology

> *Engagements follow a three-phase model: Reconnaissance and Threat Modeling, Active Assessment, and Reporting.*

Phase 1: Scoping and Threat Modeling

Prior to active testing, Lorikeet Security conducts a structured scoping exercise to establish the attack surface and define testing boundaries. This phase includes:

- ATM vendor and model identification; firmware and OS version enumeration
- Network topology review: ATM VLAN placement, upstream routing, firewall policy
- Compliance framework identification (PCI DSS, PCI PTS, FFIEC, OCC as applicable)
- Threat modeling against known ATM attack categories (jackpotting, skimming, network MitM, logical attacks)
- Rules of engagement documentation and written authorization collection

Phase 2: Active Assessment

The active assessment phase is organized into eight distinct testing domains (detailed in Section 4). Testing is conducted in order of risk and operational impact, with safety controls in place for any tests involving the cash dispenser or physical enclosure.

Testing approaches used across domains include:

Black-box: Black-box testing

- No prior access to ATM configuration, OS, or application source code
- Simulates an external attacker or compromised insider with physical access

Gray-box: Gray-box testing

- OS-level access provided; no application source code
- Simulates a compromised operator account or maintenance access scenario

White-box: White-box testing

- Full configuration, network diagrams, and application documentation provided
- Used for compliance gap analysis and cryptographic review

Phase 3: Reporting and Debrief

Upon completion of testing, Lorikeet Security delivers formal findings report structured as follows:

- Executive summary with risk posture assessment and critical findings
- Technical findings with CVSS scoring, reproduction steps, and evidence
- Compliance gap matrix mapped to applicable PCI DSS and PCI PTS requirements
- Prioritized remediation roadmap with short-term and long-term recommendations
- Attestation letter confirming scope and testing completion

A debrief call is conducted with the customer's security and operations teams following report delivery to walk through findings and answer questions.

3. Scope of Assessments

> *Standard scope encompasses the ATM unit, its OS environment, connected network segment, and all customer-facing input/output devices.*

The following components are included in a standard ATM security assessment:

Component	Scope Details
ATM Host OS	Windows Embedded, Windows 10/11 IoT, or Linux distribution running on the ATM unit
ATM Application Layer	XFS middleware, vendor application stack, and all installed third-party agents
Physical Unit	Enclosure, card reader, EPP/PIN pad, cash dispenser, maintenance ports
Network Segment	ATM-facing switch port, VLAN, firewall rules, and upstream routing to banking host
Communication Channel	TLS configuration between ATM and transaction processing host
Key Management	HSM configuration, PIN block handling, key storage and injection procedures
Logging and Monitoring	Audit log completeness, SIEM integration, alert configuration

Component	Scope Details
Compliance Posture	PCI DSS v4.0 requirements, PCI PTS device approval status

Out-of-scope by default (requires explicit authorization): core banking systems, payment processing hosts, card management platforms, and any ATM units not listed in the signed statement of work.

4. Tools and Techniques

> *Lorikeet Security uses a combination of commercial, open-source, and proprietary tools depending on the testing domain.*

Domain	Tools	Techniques
Physical Testing	Custom skimmer detection kit, specialized inspection tools, lock bypass tools	Physical intrusion simulation, tamper seal inspection, enclosure bypass attempts
Network Analysis	Wireshark, Nmap, Nessus, OpenVAS, custom scripts	Packet capture, VLAN hopping, TLS inspection, firewall rule review
OS / Software	Metasploit, Burp Suite, Sysinternals, Volatility, custom XFS tools	Privilege escalation, service enumeration, application logic analysis
Firmware	Binwalk, Ghidra, IDA Pro, JTAG/UART adapters	Firmware extraction, static analysis, binary reversing
Cryptography	OpenSSL, custom key analysis tools, protocol analyzers	Certificate review, key storage inspection, cipher suite analysis
Dispenser Testing	Custom XFS command harness (authorized simulation only)	Command injection testing, authentication bypass attempts

5. Testing Checklist by Domain

> *The following checklist covers all eight assessment domains. Each test case references the applicable compliance standard and assigned risk level.*

Risk Level Key: Critical = Immediate remediation required | High = Remediate within 30 days | Medium = Remediate within 90 days | Low = Informational

ID	Test Case	Standard	Risk Level
1. Physical Security and Tampering Assessment			
PHY-01	Inspect enclosure tamper-evident seals and physical integrity of all panels	PCI PTS POI	**High**
PHY-02	Attempt forced entry and tool-based enclosure bypass under controlled conditions	PCI PTS POI	**Critical**
PHY-03	Evaluate card slot for presence of external skimming overlays and shimming devices	PCI DSS 9.9	**Critical**

ID	Test Case	Standard	Risk Level
PHY-04	Assess PIN pad overlay detection mechanisms and anti-shimming features	PCI PTS POI	Critical
PHY-05	Review physical lock quality, key management, and access control to the safe compartment	PCI DSS 9.4	High
PHY-06	Evaluate camera coverage, lighting, and tamper alarm sensor coverage at installation site	PCI DSS 9.1	Medium
PHY-07	Assess cable management for exposed USB, serial, or maintenance ports accessible without tools	PCI DSS 6.2	High
PHY-08	Review anti-jackpotting physical controls (top hat sensors, vibration sensors, jitter mechanism)	Vendor / NIST	Critical
2. Software and Firmware Vulnerability Analysis			
SW-01	Identify OS version, patch level, and EOL status of Windows Embedded / Linux variant	PCI DSS 6.3	High
SW-02	Enumerate installed software, third-party components, and identify unpatched CVEs	PCI DSS 6.3	High
SW-03	Test for application whitelisting enforcement (e.g., AppLocker, UEFI allowlist policies)	NIST SP 800-167	Critical
SW-04	Analyze XFS (eXtension for Financial Services) middleware for insecure device command handling	CEN/XFS	Critical
SW-05	Attempt privilege escalation from operator-level access to SYSTEM/root within the ATM OS	NIST SP 800-53	Critical
SW-06	Review firmware update mechanisms for authenticity verification and rollback protections	NIST SP 800-147	High
SW-07	Assess ATM management software agent for unauthenticated command execution vulnerabilities	PCI DSS 6.4	High
SW-08	Identify and test exposed maintenance interfaces (RDP, VNC, vendor-specific remote tools)	PCI DSS 2.2	High
3. Network Segmentation and Encryption Review			
NET-01	Verify ATM VLAN is isolated from corporate and POS networks; test for VLAN hopping	PCI DSS 1.3	Critical
NET-02	Inspect TLS version and cipher suite configuration on all ATM-to-host communications	PCI DSS 4.2	High
NET-03	Test for man-in-the-middle susceptibility on the ATM-to-switch network segment	PCI DSS 4.2	Critical
NET-04	Review firewall rules governing ATM outbound and inbound traffic; identify overly permissive rules	PCI DSS 1.2	High
NET-05	Verify host-based firewall is active and restrictive on the ATM OS	PCI DSS 1.4	Medium
NET-06	Assess DNS configuration for potential DNS spoofing or hijacking vectors	NIST SP 800-81	Medium
NET-07	Verify certificate pinning or mutual TLS (mTLS) enforcement for banking host connections	PCI DSS 4.2	High
NET-08	Review wireless connectivity (if present) for WPA3 enforcement and rogue AP susceptibility	PCI DSS 4.1	High
4. Card Reader and PIN Pad Security Testing			
CR-01	Inspect EMV chip reader for correct implementation and downgrade attack resistance	EMVCo / PCI PTS	Critical

ID	Test Case	Standard	Risk Level
CR-02	Test for NFC/contactless reader firmware vulnerabilities and relay attack susceptibility	PCI PTS POI	High
CR-03	Verify magnetic stripe fallback restrictions; test for magstripe-only transaction bypass	PCI DSS 8.5	High
CR-04	Assess PIN pad for head bus monitoring attack susceptibility (hardware key logging)	PCI PTS HSM	Critical
CR-05	Verify EPP (Encrypting PIN Pad) is PCI PTS-approved and within validity period	PCI PTS POI	High
CR-06	Test card reader interoperability handling for malformed card data injection scenarios	ISO/IEC 7816	Medium
CR-07	Verify anti-shimming jitter mechanism is active and functioning on card reader	PCI PTS POI	Critical
5. Cash Dispenser Attack Simulation			
CD-01	Test cash dispenser bus (USB/RS-232) for unauthorized command injection (black box jackpotting simulation)	Vendor / NIST	Critical
CD-02	Verify dispenser controller requires authenticated session before executing dispense commands	Vendor / PCI DSS	Critical
CD-03	Assess logical jackpotting resistance via OS-level dispenser driver command spoofing	PCI DSS 6.4	Critical
CD-04	Review audit trail integrity for dispense events; test for log tampering or suppression	PCI DSS 10.3	High
CD-05	Verify physical tamper response on the safe door triggers system lockout	PCI PTS POI	High
CD-06	Assess whether standalone malware (e.g., Ploutus, Tyupkin variants) execution is prevented by whitelisting	NIST SP 800-167	Critical
6. Boot Integrity and Secure Boot Validation			
BOOT-01	Verify UEFI Secure Boot is enabled and enforcing an approved signature database	NIST SP 800-147	Critical
BOOT-02	Attempt to boot from external media (USB, optical); confirm BIOS prevents unauthorized boot devices	PCI DSS 6.2	High
BOOT-03	Verify BIOS/UEFI is password-protected and firmware settings are locked	PCI DSS 2.2	High
BOOT-04	Inspect full-disk encryption status (BitLocker, LUKS) and TPM-binding configuration	PCI DSS 3.5	Critical
BOOT-05	Test for cold boot attack exposure; assess memory scrubbing on shutdown/reboot	NIST SP 800-111	High
BOOT-06	Verify boot measurement chain using TPM attestation logs (PCR values)	NIST SP 800-155	High
7. Cryptographic Implementation Review			
CRYPT-01	Verify PIN block encryption uses AES-128 or higher; confirm 3DES is being phased out per PCI timeline	PCI PTS HSM / DSS	Critical
CRYPT-02	Review key injection procedures for ZMK/ZPK/TPK; verify dual control and split knowledge	PCI PTS HSM	Critical
CRYPT-03	Assess HSM (Hardware Security Module) integration; verify keys never appear in plaintext outside HSM	PCI PTS HSM	Critical
CRYPT-04	Verify master key (LMK) management and rotation policy; test for hardcoded or default keys	PCI DSS 3.6	Critical

ID	Test Case	Standard	Risk Level
CRYPT-05	Review certificate authority chain and certificate expiration management for all TLS endpoints	PCI DSS 4.2	High
CRYPT-06	Assess use of cryptographically secure RNG; verify no use of predictable PRNG in key generation	NIST SP 800-90A	High
CRYPT-07	Review key storage at rest; confirm no symmetric keys are stored in plaintext configuration files	PCI DSS 3.4	Critical
8. PCI Standards Compliance Testing			
PCI-01	Validate cardholder data environment (CDE) scope and network segmentation boundaries per PCI DSS v4.0	PCI DSS 1.x	High
PCI-02	Verify no prohibited account data (CVV2, PIN, full track data) is retained post-authorization	PCI DSS 3.2	Critical
PCI-03	Review access control and authentication for ATM management systems; verify MFA enforcement	PCI DSS 8.x	High
PCI-04	Confirm all ATM components are on a supported hardware/software version eligible for PCI PTS approval	PCI PTS POI	High
PCI-05	Audit logging completeness: verify all access, configuration changes, and transaction events are logged	PCI DSS 10.x	High
PCI-06	Review vulnerability management program; confirm ATM patching cadence meets PCI DSS requirements	PCI DSS 6.3	Medium
PCI-07	Assess physical security controls at ATM site against PCI DSS Requirement 9 site requirements	PCI DSS 9.x	Medium
PCI-08	Verify third-party/vendor access is governed by formal agreements and restricted by need-to-know	PCI DSS 12.8	High

6. Compliance Standards Reference

> *Lorikeet Security aligns ATM assessments to the following primary standards.*

Standard	Relevance to ATM Security
PCI DSS v4.0	Primary compliance framework for cardholder data environments; covers network security, access control, cryptography, logging, and vulnerability management across all ATM components that store, process, or transmit cardholder data.
PCI PTS POI	Governs the physical and logical security requirements for Point of Interaction devices including EPP/PIN pads and card readers. All physical cardholder input devices must be PCI PTS-approved and within their approval period.
PCI PTS HSM	Covers Hardware Security Module requirements for key management, PIN block encryption, and key injection procedures. Directly applicable to ATM HSM configuration and LMK/ZMK/ZPK lifecycle.
NIST SP 800-53	Provides security and privacy controls for federal information systems; used as a supplemental framework for access control, system integrity, and audit/accountability requirements.
NIST SP 800-147	BIOS and UEFI protection guidelines; directly applied during boot integrity validation testing.
NIST SP 800-167	Application whitelisting guidelines; used as the basis for evaluating ATM application whitelisting controls against jackpotting malware threats.

Standard	Relevance to ATM Security
EMVCo Specifications	Governs chip card transaction processing standards; used during card reader testing to verify correct EMV implementation and downgrade attack resistance.
CEN/XFS (ISO 9564)	Industry standard for ATM device communication middleware; applied during XFS layer analysis and cash dispenser command injection testing.

7. Deliverables and Engagement Model

> *Standard deliverables for every ATM security assessment engagement.*

Lorikeet Security provides the following deliverables upon engagement completion:

Final Report: Penetration Test Report

- Executive summary with overall risk posture and critical findings
- Technical findings with CVSS v3.1 scoring, reproduction steps, screenshots, and tool output
- Compliance gap matrix (PCI DSS / PCI PTS requirement-level mapping)
- Prioritized remediation roadmap

Evidence Package: Raw Evidence Package

- Network captures, tool output logs, and screenshots organized by finding
- Delivered via encrypted archive; password shared via separate channel

Attestation Letter: Attestation Letter

- Signed letter confirming scope, testing dates, and engagement completion
- Suitable for submission to auditors and QSAs

Debrief Session: Debrief Session

- Live walkthrough of findings with the customer's security and operations teams
- Q&A and remediation guidance

Typical engagement timelines range from 5 to 15 business days depending on the number of ATM units in scope, the depth of testing required (black-box vs. white-box), and the availability of the customer's operations team for coordinated testing windows.