ATM AVAILABILITY

ATM Security Risk and Capability Maturity Worksheet

A self-assessment

A structured way to evaluate your organization's ATM security capabilities: five maturity levels, seventy capabilities across four domains, and a summary and action plan to record where the gaps are and who is closing them.

Appendix A of the white paper Analysis of Technical Risks and Attack Vectors Targeting ATMs, published separately so it can be printed and filled in.

William Friend

2026-09-04

Introduction

This worksheet provides a structured approach to evaluating your organization's ATM security capabilities. It combines the risk management framework outlined previously with a Capability Maturity Model (CMM) to create a comprehensive self-assessment tool. A maturity model is a framework that describes how well an organization's behaviors, practices, and processes can reliably and sustainably produce required outcomes. Using this model allows you to benchmark your current capabilities, identify realistic goals for improvement, and prioritize investments to address the most significant risks.

The goal is to move from a reactive security posture to one that is proactive, measured, and continuously improving.

Assessment Record

Complete this before scoring. A filled worksheet that does not say which estate it covers, when, or who scored it cannot be compared against next year's.

Field	Entry
Organization / business unit	
Fleet in scope (describe)	
Number of terminals in scope	
Deployment types included	
Operated in-house / by third party	
Assessment date	
Assessors (names and roles)	
Next scheduled re-score	

If the fleet in scope covers more than one materially different population – a through-the-wall branch estate and an off-premise retail estate, or an estate you own alongside one operated for you under contract – run the worksheet once for each. Two honest sheets are worth more than one averaged one.

Part 1: Understanding the Capability Maturity Levels

First, familiarize yourself with the five levels of process maturity. Each level builds upon the previous one, representing a more formal, reliable, and optimized security posture. For each security capability in Part 2, you will assign one of these ratings.

Level	Maturity Level	Description
1	**Initial**	Security processes are unpredictable, poorly controlled, and reactive. There are few defined processes, and success often depends on individual effort or "heroics" in response to an incident. Controls are applied in an ad-hoc, chaotic, or inconsistent manner.
2	**Managed (Repeatable)**	Basic security processes are established, documented, and can be repeated by different team members. The necessary discipline is in place to repeat earlier successes on similar tasks. However, processes may differ between teams and are often reactive, managed on a project-by-project basis.
3	**Defined**	Security processes are well-understood and standardized across the organization. Organization-wide standards, policies, and procedures provide guidance for all projects and ATM fleet segments. The security posture is proactive rather than reactive.
4	**Quantitatively Managed**	The organization uses data-driven processes with quantitative objectives to measure and control the effectiveness of security measures. Security performance is measured, predictable, and aligns with the needs of stakeholders. Analytical tools are often used to report on security events and control performance.
5	**Optimizing**	The organization is focused on continuous improvement. Processes are stable and flexible, allowing the organization to pivot and respond to changes in the threat landscape. Quantitative feedback from processes and the piloting of innovative technologies are used to drive ongoing security enhancements.

How to score. Assign the level your evidence supports, not the one you intend to reach. Name the artifact behind every rating: a dated policy, a configuration baseline, an inspection log, a monitoring dashboard, an exception register. If the only support is that someone in the room believes it, score one level lower.

Three rules keep the result comparable. Score the fleet, not the pilot. Score the practice, not the policy – a standard most of the fleet does not meet is a level 1 with paperwork on top. Where the group is split between two levels, take the lower and record why.

Part 2: Capability Maturity Self-Assessment

The four domains follow the mitigation chapter of the white paper. Domain 1 covers the physical security controls of section 6.1; Domain 2 the logical and cybersecurity controls of section 6.2, including the network controls discussed there; Domain 3 the cardholder data protection techniques of section 6.3; and Domain 4 the compliance obligations of section 6.4 together with the monitoring, auditing and incident response practices of section 6.5. Every capability listed below appears in the mitigation matrix in section 6.6, so a row scored here can be read across to the attack types it defends against.

Instructions: For each security capability listed below, assess your organization's current maturity level using the 1-5 scale defined above. In the "Evidence/Notes" column, briefly justify your rating with specific examples (e.g., "Policy exists but is not enforced," "Automated tool deployed across 95% of fleet," "Quarterly metrics are reviewed by management"). Then, determine a realistic "Target Maturity Level" for your organization and prioritize the need for improvement.

Domain 1: Physical Security Controls

19 capabilities, drawn from section 6 of the white paper.

Capability / Control	Current (1–5)	Evidence / Notes	Target (1–5)	Priority
Site and environment				
Strategic site selection and environmental design (lighting, visibility, sightlines)				
Ram raid barriers (bollards, gates)				
Anchoring systems against rip-out				
Hardware hardening				
Certified high-security safe, grade specified against the site risk				
Reinforced casing against drilling and cutting				
Upgraded cabinet locks (unique or electronically controlled)				
Key management policy for cabinet and safe access				
Top-hat opening, vibration and tilt alarms				
Fascia protection detecting drilling associated with black box attacks				
Gas detection sensors and neutralization				
Cash protection				

Capability / Control	Current (1–5)	Evidence / Notes	Target (1–5)	Priority
Intelligent banknote neutralization (ink or dye staining)				
Glue-based note bonding systems				
Cash-in-machine limits at high-risk locations				
Surveillance				
High-resolution CCTV covering interface, user and surroundings				
Camera tamper protection and tamper detection				
Live CCTV monitoring with a defined response				
Access control				
Vestibule access control				
Technician and cash-in-transit access procedure (MFA or one-time codes)				
Operational procedures				
Regular, documented physical inspections at a risk-based frequency				

Domain 2: Logical and Cybersecurity Controls

26 capabilities, drawn from section 6 of the white paper.

Capability / Control	Current (1–5)	Evidence / Notes	Target (1–5)	Priority
Software integrity and patching				
Operating system and application patch management				
Supported OS baseline, with migration off builds past end of servicing				
Secure development lifecycle for custom ATM applications				
File integrity monitoring				
Endpoint protection				
Endpoint anti-malware and detection and response tooling				
Application control / whitelisting, enforced rather than logging				
Operating system hardening				
Unnecessary services, ports and features disabled				
Kiosk mode hardening preventing desktop or command line access				
Hardening benchmark conformance (CIS benchmarks, DISA STIGs)				
UEFI Secure Boot enabled and enforced				

Capability / Control	Current (1–5)	Evidence / Notes	Target (1–5)	Priority
BIOS/UEFI password protection against configuration change				
Data encryption				
Full disk encryption on the terminal				
HSM-backed key management for PIN encryption keys				
Network security				
TLS 1.2 or higher with mutual certificate validation				
VPN protection of ATM-to-host traffic				
Network segmentation isolating the ATM estate				
Firewall rules at the network edge and on the terminal				
Network access control binding terminals to known ports or addresses				
Message authentication codes on transaction messages				
Peripheral security				
USB and unused ports disabled				
Device control preventing unauthorized peripherals				

Capability / Control	Current (1–5)	Evidence / Notes	Target (1–5)	Priority
Authenticated communication between PC core and dispenser				
Dispenser firmware pairing (unique image bonding or high-level settings)				
Access management				
Multi-factor authentication for technician, administrator and remote access				
Role-based access control on least privilege				
Default credentials changed and password policy enforced				

Domain 3: Cardholder Data Protection Controls

9 capabilities, drawn from section 6 of the white paper.

Capability / Control	Current (1–5)	Evidence / Notes	Target (1–5)	Priority
Anti-skimming and anti-shimming				
Skimmer detection and magnetic-field jamming at the reader				
Physical obstruction (fascia security inserts, card protection plates)				
Card-handling countermeasures (jitter, tamper-resistant card reader)				
Anti-shimming hardware against deep-insert devices				
Card and transaction data				
Full EMV chip implementation with magnetic-stripe fallback minimized				
Dynamic card verification (iCVC/dCVV) checked against the static CVV				
Contactless and cardless transactions offered				
PIN security				
Certified encrypting PIN pads, approval status maintained				
End-to-end PIN encryption from the pad to the authorizing host				

Domain 4: Process and Governance Controls

16 capabilities, drawn from section 6 of the white paper.

Capability / Control	Current (1–5)	Evidence / Notes	Target (1–5)	Priority
Compliance and standards				
PCI DSS adherence across the ATM estate				
PCI PTS POI device approvals maintained against expiry				
PCI PIN Security requirements met as a process				
TR-31 / TR-34 key block compliance				
Alignment to external guidance (NIST, EAST, vendor advisories)				
Real-time monitoring				
Transaction and anomaly monitoring				
ATM status and health monitoring (reboots, outages, sensor alerts, cash levels)				
Network monitoring for unauthorized connections and MitM indicators				
Physical security monitoring (CCTV analytics, alarms, access logs)				
Logging and auditing				

Capability / Control	Current (1–5)	Evidence / Notes	Target (1–5)	Priority
Centralized security logging and SIEM correlation				
Log protection against tampering, with scheduled review				
Security audits, vulnerability assessments and penetration testing				
Response and awareness				
Documented and tested incident response plan				
Industry information sharing (EAST, law enforcement, vendors)				
Staff and technician security awareness training				
Customer education on safe use and spotting tampering				

Part 3: Summary and Action Plan

Instructions: Based on your assessment in Part 2, summarize your findings and create a high-level action plan. Focus on the capabilities with the highest priority and the largest gaps between your current and target maturity levels.

Maturity Summary

Strengths – capabilities at or near their target maturity.

Capability / Control	Domain	Current	Evidence relied on

Weaknesses – capabilities at high priority and low maturity.

Capability / Control	Domain	Current → Target	Why it matters here

Domain averages. Record the mean current maturity for each domain, with the number of capabilities it is averaged over. Do not combine the four into a single score: the domains are not equally weighted and averaging them hides the gap.

Domain	Capabilities	Mean current	Mean target
1 – Physical Security Controls	19		
2 – Logical and Cybersecurity Controls	26		
3 – Cardholder Data Protection Controls	9		
4 – Process and Governance Controls	16		

Action Plan for Improvement

Area for Improvement (Capability/Control)	Identified Gap (Current → Target)	Proposed Actions	Owner / Department	Target Timeline
Example: Upgraded Cabinet Locks	*1 → 3*	*Research and select a high-security lock vendor. Develop a phased rollout plan for the 50 highest-risk ATMs. Update key management policy.*	*Physical Security*	*Q4 2025*