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, 102 capabilities across four domains, a summary and action plan to record where the gaps are and who is closing them, and reference notes for the controls that need 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

2026-09-05

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.

A worked example

Generic level descriptions invite generous scoring. Anchor each rating to behavior you would recognize in another institution. Patch management, scored honestly:

Level	What it looks like
1	Patched quarterly, or not at all.
2	Patched when something forces it, by whoever is available.
3	A written standard sets the interval, and the fleet mostly meets it.
4	The interval is measured and reported – release to production inside ten days, with the exceptions counted.
5	That interval holds consistently, is measured against a risk metric, and drives change when it slips.

Note what separates 4 from 5, and 3 from 4. It is not whether the activity happens. It is whether the interval is **named**, whether performance against it is **measured**, and whether the measurement **changes anything**. Every group in Part 2 carries a short anchor in the same form.

Three principles behind the anchors

A control with no maintenance plan is not a mature control. Bollards rust, gates jam, lighting fails, detection floods the queue with false positives. Installing something scores at the middle of the scale. Servicing it against an SLA, and measuring whether the service happens, is what scores at the top.

If it is outsourced and the interval is not in the contract, it does not score above the middle. Patching, vulnerability remediation, site services, gate maintenance and key control are all commonly delegated. Delegating the work without contracting the timescale leaves you accountable for an outcome nobody has committed to.

Some ceilings are set by your vendor, not by you. Where the terminal application requires an administrative auto-login, or the hardware predates a protection, record the constraint in the evidence column and score what is actually true. The purpose is an accurate picture, not a good one.

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.

Most capabilities below appear in the mitigation matrix in section 6.6, and those rows can be read across to the attack types they defend against, which the accompanying spreadsheet shows against each row. The rest come from operating practice rather than from the paper, and are here because practitioners score them. Part 4 gives the reference notes for the rows that need them.

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

30 capabilities.

Capability / Control	Current (1–5)	Evidence / Notes	Target (1–5)	Priority
Site and environment — *1:* sites chosen ad hoc, conditions noticed when a customer complains · *5:* documented siting criteria, a scheduled inspection route, and a remediation SLA that is measured				
Strategic site selection against documented risk criteria				
Site services sustaining lighting, visibility, sightlines and cleanliness				
Accessibility compliance checked on the site route (see notes)				
Ram raid barriers selected against site risk and customer impact				
Barrier and gate servicing under SLA, covering corrosion and jamming				
Anchoring systems against rip-out				
Hardware hardening — *1:* whatever the machine shipped with · *5:* safe grade, attack designations and lock generation specified per site risk and verified on delivery				
Certified high-security safe, grade specified against site risk (see notes)				
Explosive and gas resistance designated separately from the tool-attack grade				
Reinforced casing against drilling and cutting				
Upgraded cabinet locks (unique or electronically controlled)				

Capability / Control	Current (1–5)	Evidence / Notes	Target (1–5)	Priority
Safe lock generation and time-to-open, with audited one-time access				
Key management policy for cabinet and safe access				
Key control in vendor contracts, with lost-key liability stated				
Physical key audits, counted and reconciled on a schedule				
Top-hat opening, vibration and tilt alarms				
Fascia drilling detection against black box entry (see notes)				
Gas detection sensors and neutralization				
Cash protection — *1:* the safe is the only thing between an attacker and spendable cash · *5:* degradation specified for irreversibility, with limits set by site risk and reviewed				
Intelligent banknote neutralization by ink, dye or glue bonding (see notes)				
Cash-in-machine limits at high-risk locations				
Surveillance — *1:* a camera exists and the footage is pulled after the event · *5:* coverage includes the cash pocket, is tamper-alarmed, and is monitored live against a response SLA				
High-resolution CCTV covering interface, user and surroundings				
Camera tamper protection and tamper detection				
Cash-pocket camera covering the dispenser opening				

Capability / Control	Current (1–5)	Evidence / Notes	Target (1–5)	Priority
Live CCTV monitoring with a defined, time-bound response				
Camera analytics or edge AI at unattended sites, on a documented privacy basis				
Access control — *1:* shared codes and standing access · *5:* individually attributable, time-bound access with every open reconciled to a work order				
Vestibule access control				
Technician and cash-in-transit access procedure (MFA or one-time codes)				
Operational procedures — *1:* inspections happen when someone is passing · *5:* a risk-based route covering every tamper vector, staff equipped to recognize devices, and on-site time measured and falling				
Documented physical inspections at a risk-based frequency				
Inspection scope covering skimming, card trapping and dispenser tampering				
Inspection staff equipped with a current guide and sample devices				
On-site time measured and reduced to limit technician exposure				

Domain 2: Logical and Cybersecurity Controls

34 capabilities.

Capability / Control	Current (1–5)	Evidence / Notes	Target (1–5)	Priority
Software integrity and patching — *1:* patched quarterly or not at all · *5:* a named interval from vendor release to production, met consistently and measured against a risk metric				
Operating system and application patch management against a defined interval				
Patching interval written into the contract where patching is outsourced				
Supported OS baseline, with migration off builds past end of servicing				
Secure development lifecycle for custom ATM applications				
File integrity monitoring				
Vulnerability management — *1:* vulnerabilities surface at the annual audit · *5:* continuous detection across the fleet feeding a contracted remediation SLA that is measured				
Continuous vulnerability detection across the estate				
Vulnerability scanning inside the software delivery lifecycle				
Remediation SLA for vulnerabilities, contracted where remediation is outsourced				
Endpoint protection — *1:* signature anti-virus, if anything · *5:* enforced application control with detection and response, tuned and monitored				
Endpoint anti-malware and detection and response tooling				
Application control / whitelisting, enforced rather than logging				

Capability / Control	Current (1–5)	Evidence / Notes	Target (1–5)	Priority
Operating system hardening — *1:* the vendor's default build · *5:* a benchmarked baseline enforced fleet-wide, with drift detected and the privileged auto-login removed				
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				
BIOS/UEFI passwords, unique per machine and rotated				
Hardware BIOS reset path disabled or physically obstructed				
Terminal application running without a privileged auto-login account				
Data encryption — *1:* data at rest is unprotected · *5:* full disk encryption fleet-wide with hardware-backed key custody				
Full disk encryption on the terminal				
HSM-backed key management for PIN encryption keys				
Network security — *1:* the estate shares the corporate network · *5:* segmented, authenticated, encrypted and bound to known endpoints, with the message layer authenticated too				
TLS 1.2 or higher with mutual certificate validation				
VPN protection of ATM-to-host traffic				
Network segmentation isolating the ATM estate				

Capability / Control	Current (1–5)	Evidence / Notes	Target (1–5)	Priority
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 and bus security — *1:* ports are open and nobody knows what is inside the machine · *5:* an enumerated component inventory, alarms on additions, and an authenticated path to the dispenser				
USB and unused ports disabled				
Device control preventing unauthorized peripherals				
Component inventory control detecting hardware added to the machine				
Protection against direct memory access over the internal expansion bus (see notes)				
Authenticated communication between PC core and dispenser				
Dispenser firmware pairing (unique image bonding or high-level settings)				
Access management — *1:* shared accounts and vendor defaults · *5:* individual, multi-factor, least-privilege access reviewed on a cycle				
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

15 capabilities.

Capability / Control	Current (1–5)	Evidence / Notes	Target (1–5)	Priority
Anti-skimming and anti-shimming — *1:* no detection, or alerts nobody acts on · *5:* capability inventoried machine by machine, with a response SLA and a tracked false-positive rate				
Skimmer detection at the card reader				
Magnetic-field jamming at the card reader				
Detection response plan with a time-bound SLA and tracked false-positive rate				
Fleet inventory of anti-skimming capability, machine by machine				
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 — *1:* magnetic stripe accepted without constraint · *5:* EMV throughout, fallback constrained and monitored, dynamic verification checked				
Full EMV chip implementation with magnetic-stripe fallback minimized				
Dynamic card verification (iCVC/dCVV) checked against the static CVV				
Contactless and cardless transactions offered				

Capability / Control	Current (1–5)	Evidence / Notes	Target (1–5)	Priority
PIN security — *1:* the pads are certified, somewhere · *5:* part number, hardware and firmware version and approval letter held per device, verified against the deployed fleet, with custody and destruction records (see notes)				
Certified encrypting PIN pads in use				
Per-device approval evidence: part number, hardware and firmware version, approval letter				
Deployed fleet verified against approved configurations and approval expiry				
Chain of custody and certificate of destruction for retired PIN pads				
End-to-end PIN encryption from the pad to the authorizing host				

Domain 4: Process and Governance Controls

23 capabilities.

Capability / Control	Current (1–5)	Evidence / Notes	Target (1–5)	Priority
Compliance and standards — *1:* compliance is asserted at audit time · *5:* obligations mapped to owners and evidenced continuously between audits				
PCI DSS adherence across the ATM estate				
PCI PIN Security requirements met as a process				
TR-31 / TR-34 key block compliance				
Alignment to external guidance (NIST CSF, FFIEC, vendor advisories)				
Transaction and machine-behavior monitoring — *1:* card-fraud monitoring bought from the processor, and nothing watching the machine · *5:* machine patterns monitored in their own right, with velocity trips that disable individual functions automatically (see notes)				
Card and account fraud monitoring on ATM transactions				
Dispense-versus-journal reconciliation of what the machine actually paid out				
Transaction reversal fraud detection				
Withdrawal velocity monitoring				
Decline-burst detection indicating card or PIN testing				
Deposit velocity monitoring for cash and check, including altered items				

Capability / Control	Current (1–5)	Evidence / Notes	Target (1–5)	Priority
Granular function disablement on a velocity trip, without taking the terminal out of service				
Estate monitoring — *1:* faults are reported by customers · *5:* health, network and physical signals correlated in one view with defined response paths				
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 — *1:* logs stay on the terminal until it is reimaged · *5:* centralized, tamper-evident, correlated and actually reviewed				
Centralized security logging and SIEM correlation				
Log protection against tampering, with scheduled review				
Assurance and improvement — *1:* assessed once, if at all · *5:* independent testing plus this assessment re-run on a defined cadence, with the deltas owned				
Security audits, vulnerability assessments and penetration testing				
This assessment repeated on a defined cadence, with deltas reviewed by an owner				
Response, sharing and awareness — *1:* the response plan is untested and the organization learns about attacks from the news · *5:* a tested plan, bulletins owned and actioned, and incidents contributed back to the industry				
Documented and tested incident response plan				

Capability / Control	Current (1–5)	Evidence / Notes	Target (1–5)	Priority
Vendor security bulletins subscribed, owned and acted on				
Participation in industry crime-intelligence sharing (see notes)				
Staff and technician security awareness training, with current attack samples				
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	30		
2 – Logical and Cybersecurity Controls	34		
3 – Cardholder Data Protection Controls	15		
4 – Process and Governance Controls	23		

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*

Part 4: Reference Notes

Context for the rows that cannot be scored honestly without it. Nothing here is scored; it is here so a rating is a judgement rather than a guess.

Safe grades

Safes, ATM safes and their bases are graded under EN 1143-1, the CEN standard, from grade 0 up to grade VI. The grade is a measured resistance to a tool attack, expressed in resistance units, and it is awarded against two separate thresholds:

- **partial access** – an opening large enough to remove the contents
- **complete access** – full opening of the unit

ATM safes are graded on both, because an opening far short of a full breach is enough to empty a cassette. Two consequences follow. A grade quoted without saying which threshold it refers to is ambiguous. And a higher grade always costs more resistance for partial access than the grade below it, so specifying up a grade buys resistance against exactly the attack an ATM actually faces.

A tool-attack grade says nothing about explosives or gas. Resistance to explosive attack is a separate optional designation, EX, as is GAS, each tested and certified in its own right. A grade IV safe with no EX designation has not been tested against a gas attack. Where solid and gas explosive attacks are part of the local threat picture, the designation has to be specified alongside the grade, and confirmed on the certificate rather than assumed from the grade.

Grades and test structure for ATM, aperture and IT safes: `ecb-s.com/_data/RL_ECB-S_R16_IT_and_aperture_safes_201210.pdf`. The standard itself: `knowledge.bsigroup.com`.

PIN pad approval evidence

Approval is granted to a *specific combination* of device, hardware version and firmware version, not to a model name. A part number alone does not establish that a deployed terminal is compliant, and a firmware update can move a device off its approval. Under PTS POI v6 and later, firmware approval expires on a three-year cycle independently of the device's own approval date, so a device can be inside its approval window while its firmware is outside.

What that makes worth holding per device: part number, hardware version, firmware version, the approval number, the approval letter, and its expiry. Then a periodic reconciliation of what is deployed against what is approved. That is a different exercise from checking that the model appears on the list at all.

Approved device list, searchable by approval number: `listings.pcisecuritystandards.org/assessors_and_solutions/pin_transaction_devices`. Each entry links to the approval detail for that hardware and firmware combination, which is the document to file against the device.

Accessibility compliance

Section 707 of the 2010 ADA Standards for Accessible Design covers ATMs: reach ranges and clear floor space, operable parts that can be told apart by touch, privacy of input and output, speech output through a standard connector, display contrast and character height, and Braille instructions for initiating speech mode. These are site conditions, and they decay like any other. A missing Braille label or a dead audio jack is a compliance failure found by complaint unless something checks for it on a schedule. That is why they sit inside the site services route rather than in the governance domain.

Standards: ada.gov/law-and-regs/design-standards/2010-stds. Plain-language guidance: access-board.gov/ada/chapter/ch07.

Cash degradation

Ink and dye staining, and glue bonding, are both intelligent banknote neutralization; glue is a variant of the same idea rather than a separate class of control. The mechanisms differ in what they leave behind. Staining marks the notes, which remain notes. Glue bonds the stack into a solid block. Specify against the outcome you want, marked or unusable, rather than against the category name, and confirm which one a quoted system delivers.

Bus-level attacks

The row on direct memory access refers to the terminal's internal PCI Express expansion bus, not to the PCI payment standards named elsewhere in this worksheet. A device attached to that bus can read and write system memory directly, without the operating system mediating, which puts it underneath most endpoint controls. Mitigations are IOMMU or kernel DMA protection, pre-boot DMA protection, and physically disabling or blocking unused slots.

Machine-behavior monitoring

Card and account fraud monitoring is a mature purchasable product. Monitoring the machine's own behavior largely is not, and where it exists it is usually built in-house against terminal and switch data. Scoring low here often reflects the market rather than the organization. The gap is still where ATM-specific attacks show themselves, so it is worth scoring rather than omitting.

The highest-value pattern is the simplest to state and the rarest to find: **reconcile what the dispenser firmware reports it paid out against what the application and the host recorded.** A machine that physically dispensed a hundred-dollar note while the host recorded a one-dollar withdrawal has told you about a logical dispense attack, in its own logs, at the time it happened.

Industry information sharing

Two channels, plus whatever closed forums your own network reaches:

- **Vendor security bulletins**, from the hardware manufacturer and the service
  - provider separately. These are frequently different companies publishing
  - different advisories. The capability is not subscribing; it is having a named owner who
  - acts on them and can show what changed as a result.
- **A crime intelligence database.** ATMIA operates the Crisis and Crime
  - Management Intelligence System, a global ATM crime database, with incident
  - reporting and periodic trend analysis:
  - `atmia.com/security/ccmis`. The top of
  - this ladder is contributing incidents back, not only consuming reports.

Beyond the public channels, most markets have closed practitioner forums that work by introduction rather than by application. They are not listed here. Ask a peer institution, your hardware vendor or your processor what they attend; the answer is usually a name you will not find by searching.

Regional practice

Two controls are common in Europe and rare in the United States. **Fascia drilling detection** — sensing the drilling or cutting of the fascia that precedes a black box attack, and putting the terminal into a protective state — was developed largely in response to European attack patterns and appears in the countermeasure guidance published by the European Association for Secure Transactions: `association-secure-transactions.eu`. **Glue-based note bonding** has a similar distribution. A US operator scoring these at 1 is describing the market, not a failure of theirs; record that in the evidence column and set the target accordingly.