



Absa Third-Party Control Obligations PCI – Payment Card Industry Standards

Version 10

August 2025

Absa Third-Party Control Obligations

PCI – Payment Card Industry Standards

At Absa Bank, protecting the confidentiality, integrity, and availability of information assets remains a top priority. In line with our commitment to a resilient and secure digital ecosystem, only Third-Party that impact the Cardholder Data Environment (CDE) are required to meet defined control and compliance obligations under the applicable PCI Security Standards when engaging with Absa in activities involving cardholder data, payment processing, or cryptographic functions. All Attestation of Compliance must be issued by a certified PCI QSA (Qualified Security Assessor)

PCI Security Standards Overview

As defined by the PCI Security Standards Council, the standards include:

- PCI DSS (Data Security Standard)
- P2PE (Point-to-Point Encryption)
- Secure Software and Secure Software Lifecycle (Secure SLC)
- PTS POI (PIN Transaction Security Point of Interaction)
- PIN Security
- Token Service Provider (TSP)
- Mobile Payments on COTS (MPoC)
- Contactless Payments on COTS (CPoC)
- Software-based PIN Entry on COTS (SPoC)
- PA-DSS (Payment Application DSS, now retired)

Absa Third-Party Control Obligations | PCI - Standards

Applicable Standard	Standard Description	Requirement / Domain	Control Description	Why TP Must Comply	Evidence / Artifacts
TPs must comply with all 12 PCI DSS requirements when transmitting, processing or storing Card Holder Data					
PCI DSS	Comprehensive technical and operational security requirements for any entity that stores, processes, or transmits cardholder data (CHD) or can impact the security of the CHD environment.	Req 1 – Network Security Controls	Deploy and manage firewall/segmentation to protect and isolate the CDE from untrusted networks.	Prevents unauthorized access and reduces attack surface.	PCI DSS Certificate and Attestation of compliance(AOC)
		Req 2 – Secure Configurations	Eliminate vendor defaults; harden configurations across all system components.	Removes easy entry points commonly exploited by attackers.	
		Req 3 – Protect Stored Account Data	Minimize storage; use strong cryptography, truncation, hashing or tokenization when storage is required.	Preserves confidentiality and integrity of sensitive data at rest.	
		Req 4 – Encrypt Transmission of CHD	Use strong cryptography for CHD across open/public networks; disallow insecure protocols.	Prevents interception, eavesdropping and data tampering in transit.	
		Req 5 – Protect Systems from Malware	Deploy anti-malware where applicable; maintain signatures; alert and act on detections.	Reduces risk of exfiltration, ransomware and unauthorized control.	
		Req 6 – Secure Systems & Software	Patch/vulnerability management, secure SDLC, code reviews, and change control.	Mitigates exploitation of known vulnerabilities and coding flaws.	
		Req 7 – Restrict Access by Need-to-Know	Role-based access; least privilege; periodic access reviews.	Limits exposure and insider threat risk.	
		Req 8 – Identify & Authenticate Users	Unique IDs, MFA for administrative and remote access; strong auth lifecycle.	Ensures accountability and blocks unauthorized access.	
		Req 9 – Restrict Physical Access	Access controls for facilities and media; visitor management; device security.	Prevents physical theft/tampering of systems and CHD media.	
		Req 10 – Log & Monitor	Centralized logging, time sync, alerting and routine review of security events.	Enables rapid detection and forensic investigation of incidents.	
		Req 11 – Test Security	Internal/external vulnerability scanning, ASV scans, penetration testing and IDS/IPS.	Finds and fixes weaknesses before attackers do.	
		Req 12 – Security Policy & Governance (incl. 12.8 & 12.9 for TPs)	Documented policies, training, risk management, incident response, and third-party oversight.	Drives consistent security practice and defines TP responsibilities and SLAs.	

Absa Third-Party Control Obligations | PCI - Standards

Applicable Standard	Standard Description	Requirement / Domain	Control Description	Why TP Must Comply	Evidence / Artifacts
Applies to solution providers delivering validated P2PE solutions covering encryption from capture to decryption. Only listed solutions qualify.					
P2PE – Point-to-Point Encryption	Requirements for validated solutions that encrypt account data at the point of interaction and keep it encrypted until it reaches a secure decryption environment under the provider's control.	Domain 1 – POI Devices & Applications	Use PCI-approved POI with SRED; secure loading, configuration and tamper response.	Ensures encryption occurs before data leaves the device.	POI device approval docs, HSM reports, key management logs, solution provider attestation
		Domain 2 – Application Security	Hardened payment application, secure updates, integrity protections.	Prevents compromise of software that handles sensitive data pre-encryption.	
		Domain 3 – Solution Management	Documented processes, supplier oversight, chain of custody, customer guidance.	Maintains end-to-end integrity across all solution components.	
		Domain 4 – Decryption Environment	Hardened, segregated environment with strong access controls and monitoring.	Prevents exposure of cleartext data during decryption.	
		Domain 5 – Cryptographic Key Management	Strong key generation, storage (HSM), distribution, injection and rotation; dual control.	Protects the secrecy and integrity of encryption keys.	
		Domain 6 – Incident Response & Monitoring	Continuous monitoring, tamper/event handling, and customer notifications.	Supports rapid containment and compliance obligations.	

Absa Third-Party Control Obligations | PCI - Standards

Applicable Standard	Standard Description	Requirement / Domain	Control Description	Why TP Must Comply	Evidence / Artifacts
Successor to PA-DSS. Applies to payment software vendors and TPs who must follow secure development, coding, testing, and lifecycle security practices.					
Secure Software Framework (SSF)	Secure Software Standard defines controls for payment software to protect data and resist attacks.	Software 1 – Governance & Risk	Documented security roles, risk assessment, threat modeling for software.	Embeds security accountability and risk awareness in development.	Secure SDLC policy, code review records, test results, software release notes
		Software 2 – Secure Design & Coding	Secure architecture, coding standards, input validation, secrets handling.	Prevents common vulnerabilities (e.g., injection, auth flaws).	
		Software 3 – Protection of Sensitive Data	Proper use of cryptography, key handling, and minimization of sensitive data.	Keeps account data protected within the application boundary.	
		Software 4 – Authentication & Access	Strong authentication, session management, least privilege.	Reduces unauthorized use of application functions/data.	
		Software 5 – Logging & Monitoring	Generate, protect and retain logs; detect anomalies.	Supports detection, investigation and accountability.	
		Software 6 – Vulnerability Management	Patch cadence, SCA, dependency tracking, secure updates.	Limits exposure from third-party and zero-day risks.	

Absa Third-Party Control Obligations | PCI - Standards

Applicable Standard	Standard Description	Requirement / Domain	Control Description	Why TP Must Comply	Evidence / Artifacts
Successor to PA-DSS. Applies to payment software vendors and TPs who must follow secure development, coding, testing, and lifecycle security practices.					
Secure SLC (SSF)	Secure SLC defines a secure software lifecycle for vendors building and maintaining payment software.	SLC 1 – Organization & Policy	Security policies, roles, training for developers and release teams.	Builds a culture of security in the development lifecycle.	SLC audit reports, training records, threat modeling documentation
		SLC 2 – Secure Requirements & Design	Security requirements, threat modeling, design reviews.	Ensures security is addressed before code is written.	
		SLC 3 – Secure Implementation & Verification	Code reviews, static/dynamic testing, remediation workflow.	Detects defects early and improves code quality.	
		SLC 4 – Release & Distribution	Change control, signed builds, release integrity, update delivery security.	Protects customers from tampered or unauthorized releases.	
		SLC 5 – Vulnerability Response	PSIRT process, intake, triage, patching SLAs, customer comms.	Enables fast response to reported flaws and reduces exposure.	
		SLC 6 – Documentation & Guidance	Implementation guidance, hardening steps, secure configs for customers.	Improves secure deployment and operation by merchants/TPs.	

Absa Third-Party Control Obligations | PCI - Standards

Applicable Standard	Standard Description	Requirement / Domain	Control Description	Why TP Must Comply	Evidence / Artifacts
Applies to suppliers/managers of PIN entry devices (PEDs). Covers hardware tamper-resistance, secure PIN entry, and device-level protections.					
PTS POI	Security requirements for payment terminals/POI that capture card data and/or PIN, covering physical, logical and interface protections.	POI 1 – Physical Security & Tamper	Tamper-resistance and evident tamper detection; secure enclosure and sensors.	Prevents hardware compromise and card skimming.	Device lab test reports, PCI approval certificates, chain-of-custody logs
		POI 2 – Logical Security	Secure boot, code signing, access control, firmware integrity.	Stops unauthorized code or configuration changes.	
		POI 3 – SRED (Secure Reading & Exchange of Data)	Secure capture and encryption of PAN data within device.	Ensures PAN is protected immediately on read.	
		POI 4 – Open Protocols	Secure use of external comms protocols (Wi-Fi, Bluetooth, TCP/IP).	Prevents network-borne attacks against POI devices.	
		POI 5 – Device Management & Key Injection	Secure manufacturing, key injection, tracking, and retirement.	Maintains chain of trust across device lifecycle.	
		POI 6 – Interfaces & I/O Security	Lock down debug/service ports and external interfaces.	Prevents side-loading malware or data exfiltration via ports.	

Absa Third-Party Control Obligations | PCI - Standards

Applicable Standard	Standard Description	Requirement / Domain	Control Description	Why TP Must Comply	Evidence / Artifacts
Applies to TPs handling PIN data. Covers PIN processing, transmission, storage, and especially cryptographic key management.					
PIN Security	Requirements for the secure management, processing, and transmission of PIN data during online and offline payment transactions.	PIN 1 – Governance & Roles	Policies, roles, dual control/split knowledge for PIN processes.	Prevents single-person control over PIN-related secrets.	HSM logs, key ceremony records, dual-control evidence, PIN device inspection logs
		PIN 2 – Cryptographic Key Management	Key generation, storage in HSMs, distribution, rotation, destruction.	Protects confidentiality and integrity of PIN encryption keys.	
		PIN 3 – Device Security & Handling	Secure procurement, storage, deployment, inspection of PIN devices.	Reduces risk of tampering and substitution attacks.	
		PIN 4 – Transaction Processing Controls	Format-preserving encryption, TR-31/TR-34 handling, secure PIN block formats.	Ensures PINs remain protected throughout processing.	
		PIN 5 – Monitoring & Incident Response	Event logging, device checks, key compromise procedures.	Enables rapid detection and containment of compromises.	
		PIN 6 – Third-Party/Outsourcing Controls	Contracts, audits, and oversight for service providers handling PIN.	Clarifies responsibilities and compliance coverage across parties.	

Absa External Supplier Control Obligations | PCI - Standards

Applicable Standard	Standard Description	Requirement / Domain	Control Description	Why TP Must Comply	Evidence / Artifacts
Applies to TPs offering tokenization services. Covers secure PAN-token mapping, protection of original PAN, and lifecycle of tokens.					
Token Service Provider (TSP)	Requirements for EMV payment tokenization services covering token issuance, lifecycle, and PAN-token mapping security.	TSP 1 – Token Requestor Onboarding & Authorization	Vet and register requestors; scope, permissions and attestation.	Prevents misuse of tokenization services.	QSA reports
		TSP 2 – PAN-Token Mapping Vault Security	Harden and segment vault; encrypt PAN and mapping; strict access control.	Protects the crown-jewel mapping between PANs and tokens.	
		TSP 3 – Cryptography & Key Management	HSM-based key ops for token generation/derivation; rotation and audit.	Maintains token integrity and trust.	
		TSP 4 – Token Lifecycle & Detokenization	Provisioning, suspension, deletion; secure detokenization flow.	Prevents unauthorized retrieval of PAN from tokens.	
		TSP 5 – Monitoring, Logging & IR	Comprehensive logging, anomaly detection, incident response plans.	Supports detection and regulatory/brand reporting needs.	
		TSP 6 – Data Minimization & Privacy	Limit data collection/retention, apply privacy controls.	Reduces breach impact and compliance exposure.	

Absa External Supplier Control Obligations | PCI - Standards

Applicable Standard	Standard Description	Requirement / Domain	Control Description	Why TP Must Comply	Evidence / Artifacts
SPoC – Secure PIN on COTS devices (smartphones). CPoC – Contactless on COTS devices (no PIN, NFC). MPoC – Unified/mobile frameworks combining SPoC & CPoC.					
Mobile Payments on COTS (MPoC / CPoC / SPoC)	Mobile acceptance standards using Commercial Off-The-Shelf (COTS) devices; MPoC (modular end-to-end), CPoC (contactless on COTS), SPoC (PIN on COTS)..	MPoC – Solution Security	End-to-end security architecture, attestation, update integrity, monitoring.	Provides a validated framework for COTS-based acceptance solutions.	MPoC/CPoC/SPoC validation docs, attestation of compliance, mobile app security test results
		MPoC – Software-based POI	Isolate sensitive processes, runtime protections, anti-tamper checks.	Mitigates malware and rooting/jailbreak risks.	
		CPoC – Contactless Acceptance on COTS	Protect contactless transaction data; secure comms to backend.	Enables safe contactless acceptance without PIN on the COTS device.	
		SPoC – PIN on COTS	Protect PIN entry path via SCRP; isolate and attest PIN capture.	Prevents PIN disclosure when entered on consumer mobile devices.	
		Lifecycle & Device Management	Enrollment, health checks, revocation, telemetry and incident processes.	Ensures only trusted devices participate in payment acceptance.	
		MPoC – Solution Security	End-to-end security architecture, attestation, update integrity, monitoring.	Provides a validated framework for COTS-based acceptance solutions.	

Absa External Supplier Control Obligations | PCI - Standards

Applicable Standard	Standard Description	Requirement / Domain	Control Description	Why TP Must Comply	Evidence / Artifacts
TPs with legacy PA-DSS applications must maintain obligations until migrated. Now superseded by PCI Software Security Framework (SSF).					
PA-DSS (Retired)	Legacy standard for payment applications (retired). Replaced by PCI Secure Software Framework; still useful for legacy apps until fully migrated.	PA-DSS 1 – Secure Authentication & Access	Unique IDs, strong passwords, and secure authentication mechanisms.	Reduces unauthorized access risk in legacy payment apps.	Legacy PA-DSS validation report, vendor implementation guide, patch notes
		PA-DSS 2 – Protect Stored Sensitive Data	Prohibit storage of SAD post-authorization; encrypt CHD where stored.	Limits breach impact and aligns with PCI DSS expectations.	
		PA-DSS 3 – Secure Transmission & Network	Use strong encryption and secure protocols for communications.	Prevents interception of sensitive data in transit.	
		PA-DSS 4 – Logging, Auditing & Time Sync	Generate and protect logs; support merchant compliance evidence.	Supports monitoring and forensic investigations.	
		PA-DSS 5 – Secure Installation & Guides	Provide hardening guides and secure default configurations.	Helps stakeholders deploy apps securely and meet PCI DSS.	
		PA-DSS 6 – Patching & Vulnerability Handling	Provide patches/updates; remediate known vulnerabilities.	Reduces exploitability of legacy systems while migrating to SSF.	