

INTERNAL — NOT FOR DISTRIBUTION

POST-QUANTUM CRYPTOGRAPHY MIGRATION ASSESSMENT

PQC Readiness Assessment Report

ATK — self-assessment

OVERALL POSTURE **HIGH**

Report date	2026-10-04	Report ID	ff65e429-58e0-420a
Generated by	VPQ-Audit v1.0.2		

Executive Summary

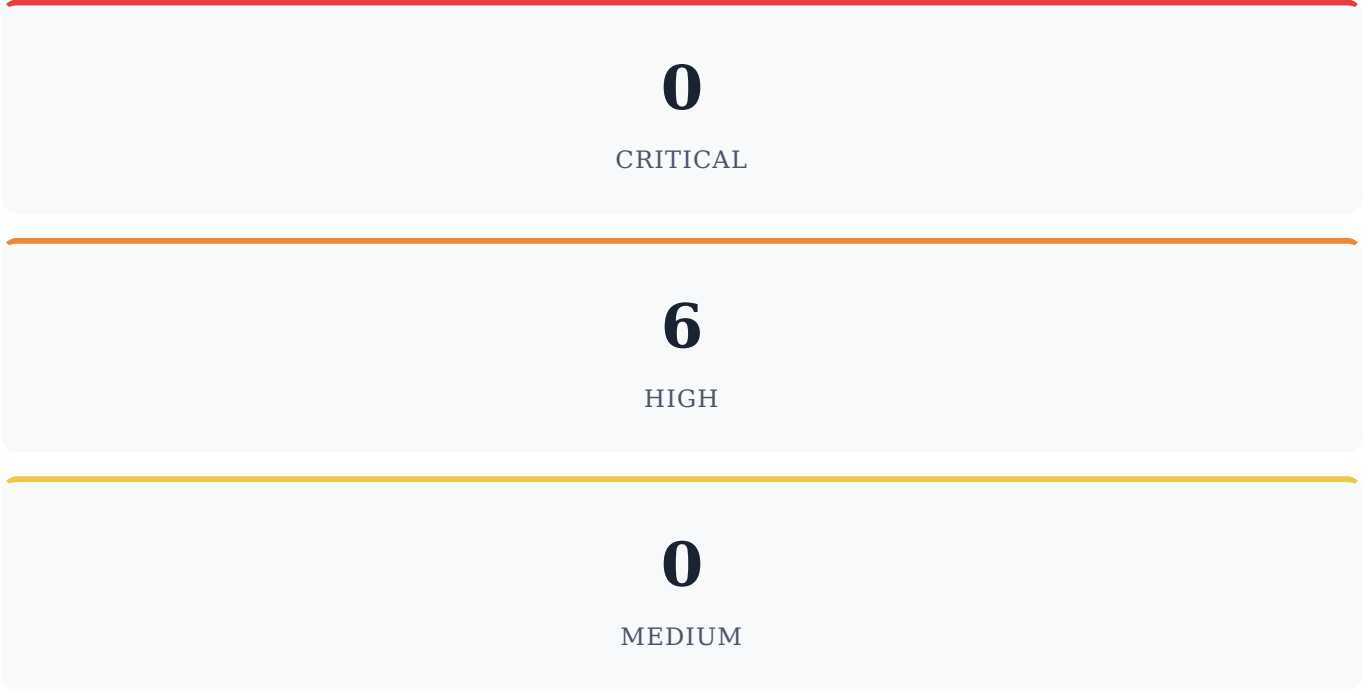
This report assesses ATK — self-assessment's readiness to migrate to post-quantum cryptography (PQC). Overall posture is **HIGH** — a planning item: no action is available until public CAs issue post-quantum certificates (deadline 2030-2035, NIST IR 8547 draft).

Within scope, 42 cryptographic findings were recorded, of which 0 are rated Critical and 24 involve algorithms directly vulnerable to cryptanalytically relevant quantum computers (classical RSA, ECC, Diffie-Hellman). No key exchange in scope is exposed to harvest-now-decrypt-later.

The proposed roadmap follows NIST SP 1800-38: keep the cryptographic inventory current, keep hybrid key exchange enabled, and replace classical certificates and signatures as CAs and vendors ship post-quantum options, ahead of the NIST IR 8547 deadlines (draft: 2030 for 112-bit keys, 2035 for all).

Planning item: The HIGH rating comes only from certificates issued by public CAs. No public CA issues post-quantum web certificates yet, so there is no action available today: track your CA's roadmap and replace them before NIST IR 8547's deadlines (draft: 2035, or 2030 for 112-bit keys such as RSA-2048).

Risk Dashboard



21

LOW

15

SAFE

Key Findings

Cryptographic primitives observed in scope, sorted by residual risk.

RISK	COMPONENT	ALGORITHM	QUANTUM VULN.	LOCATION	REPLACEMENT
HIGH	Certificate Public Key	ECDSA-secp256r1-256	Yes	atkvn.com:443, CN=atkvn.com, leaf cert	ML-DSA-44, ML-DSA-65
HIGH	Certificate Signature	ECDSA-SHA384	Yes	atkvn.com:443, CN=atkvn.com, leaf cert	ML-DSA-44, ML-DSA-65
HIGH	Certificate Public Key	ECDSA-secp256r1-256	Yes	vct.atkvn.com:443, CN=vct.atkvn.com, leaf cert	ML-DSA-44, ML-DSA-65
HIGH	Certificate Signature	ECDSA-SHA384	Yes	vct.atkvn.com:443, CN=vct.atkvn.com, leaf cert	ML-DSA-44, ML-DSA-65
HIGH	Certificate Public Key	ECDSA-secp256r1-256	Yes	vpqaudit.atkvn.com:443, CN=vpqaudit.atkvn.com, leaf cert	ML-DSA-44, ML-DSA-65
HIGH	Certificate Signature	ECDSA-SHA384	Yes	vpqaudit.atkvn.com:443, CN=vpqaudit.atkvn.com, leaf cert	ML-DSA-44, ML-DSA-65
LOW	Bulk Encryption	AES-128-GCM	No	atkvn.com:443, TLSv1.3 cipher suite	AES-256
LOW	Certificate Public Key	ECDSA-secp384r1-384	Yes	atkvn.com:443, CN=YE1, intermediate cert	ML-DSA-65, ML-DSA-87
LOW	Certificate Signature	ECDSA-SHA384	Yes	atkvn.com:443, CN=YE1, intermediate cert	ML-DSA-44, ML-DSA-65
LOW	Certificate Public Key	ECDSA-secp384r1-384	Yes	atkvn.com:443, CN=Root YE, intermediate cert	ML-DSA-65, ML-DSA-87
LOW		ECDSA-SHA384	Yes		

RISK	COMPONENT	ALGORITHM	QUANTUM VULN.	LOCATION	REPLACEMENT
	Certificate Signature			atkvn.com:443, CN=Root YE, intermediate cert	ML-DSA-44, ML-DSA-65
LOW	Certificate Public Key	ECDSA-secp384r1-384	Yes	atkvn.com:443, CN=ISRG Root X2, intermediate cert	ML-DSA-65, ML-DSA-87
LOW	Certificate Signature	RSA-SHA256	Yes	atkvn.com:443, CN=ISRG Root X2, intermediate cert	ML-DSA-65
LOW	Bulk Encryption	AES-128-GCM	No	vct.atkvn.com:443, TLSv1.3 cipher suite	AES-256
LOW	Certificate Public Key	ECDSA-secp384r1-384	Yes	vct.atkvn.com:443, CN=YE1, intermediate cert	ML-DSA-65, ML-DSA-87
LOW	Certificate Signature	ECDSA-SHA384	Yes	vct.atkvn.com:443, CN=YE1, intermediate cert	ML-DSA-44, ML-DSA-65
LOW	Certificate Public Key	ECDSA-secp384r1-384	Yes	vct.atkvn.com:443, CN=Root YE, intermediate cert	ML-DSA-65, ML-DSA-87
LOW	Certificate Signature	ECDSA-SHA384	Yes	vct.atkvn.com:443, CN=Root YE, intermediate cert	ML-DSA-44, ML-DSA-65
LOW	Certificate Public Key	ECDSA-secp384r1-384	Yes	vct.atkvn.com:443, CN=ISRG Root X2, intermediate cert	ML-DSA-65, ML-DSA-87
LOW	Certificate Signature	RSA-SHA256	Yes	vct.atkvn.com:443, CN=ISRG Root X2, intermediate cert	ML-DSA-65
LOW	Bulk Encryption	AES-128-GCM	No	vpqaudit.atkvn.com:443, TLSv1.3 cipher suite	AES-256
LOW	Certificate Public Key	ECDSA-secp384r1-384	Yes	vpqaudit.atkvn.com:443, CN=YE2, intermediate cert	ML-DSA-65, ML-DSA-87
LOW	Certificate Signature	ECDSA-SHA384	Yes	vpqaudit.atkvn.com:443, CN=YE2, intermediate cert	ML-DSA-44, ML-DSA-65
LOW	Certificate Public Key	ECDSA-secp384r1-384	Yes	vpqaudit.atkvn.com:443, CN=Root YE, intermediate cert	ML-DSA-65, ML-DSA-87
LOW	Certificate Signature	ECDSA-SHA384	Yes	vpqaudit.atkvn.com:443, CN=Root YE, intermediate cert	ML-DSA-44, ML-DSA-65
LOW	Certificate Public Key	ECDSA-secp384r1-384	Yes	vpqaudit.atkvn.com:443, CN=ISRG Root X2, intermediate cert	ML-DSA-65, ML-DSA-87

RISK	COMPONENT	ALGORITHM	QUANTUM VULN.	LOCATION	REPLACEMENT
LOW	Certificate Signature	RSA-SHA256	Yes	vpqaudit.atkvn.com:443, CN=ISRG Root X2, intermediate cert	ML-DSA-65
SAFE	TLS Protocol	TLSv1.3	No	atkvn.com:443, supported protocol	—
SAFE	TLS Protocol	TLSv1.2	No	atkvn.com:443, supported protocol	—
SAFE	Cipher Suite	TLS_AES_128_GCM_SHA256	No	atkvn.com:443, TLSv1.3 negotiated cipher suite	—
SAFE	TLS Key Exchange	X25519MLKEM768	No	atkvn.com:443, TLSv1.3 handshake	—
SAFE	Handshake Hash (HKDF)	SHA-256	No	atkvn.com:443, TLSv1.3 key schedule hash	—
SAFE	TLS Protocol	TLSv1.3	No	vct.atkvn.com:443, supported protocol	—
SAFE	TLS Protocol	TLSv1.2	No	vct.atkvn.com:443, supported protocol	—
SAFE	Cipher Suite	TLS_AES_128_GCM_SHA256	No	vct.atkvn.com:443, TLSv1.3 negotiated cipher suite	—
SAFE	TLS Key Exchange	X25519MLKEM768	No	vct.atkvn.com:443, TLSv1.3 handshake	—
SAFE	Handshake Hash (HKDF)	SHA-256	No	vct.atkvn.com:443, TLSv1.3 key schedule hash	—
SAFE	TLS Protocol	TLSv1.3	No	vpqaudit.atkvn.com:443, supported protocol	—
SAFE	TLS Protocol	TLSv1.2	No	vpqaudit.atkvn.com:443, supported protocol	—
SAFE	Cipher Suite	TLS_AES_128_GCM_SHA256	No	vpqaudit.atkvn.com:443, TLSv1.3 negotiated cipher suite	—
SAFE	TLS Key Exchange	X25519MLKEM768	No	vpqaudit.atkvn.com:443, TLSv1.3 handshake	—
SAFE	Handshake Hash (HKDF)	SHA-256	No	vpqaudit.atkvn.com:443, TLSv1.3 key schedule hash	—

Certificate chains

Certificates each endpoint presented, leaf first. Every one of these keys and signatures must move to post-quantum algorithms, and the CA-side ones depend on your certificate provider.

atkvn.com:443

POSITION	SUBJECT	ISSUER	PUBLIC KEY	SIGNATURE	VALID UNTIL
Leaf	atkvn.com	YE1	ECDSA-secp256r1-256	ECDSA-SHA384	2026-12-29
Intermediate	YE1	Root YE	ECDSA-secp384r1-384	ECDSA-SHA384	2028-09-02
Intermediate	Root YE	ISRG Root X2	ECDSA-secp384r1-384	ECDSA-SHA384	2032-09-02
Intermediate	ISRG Root X2	ISRG Root X1	ECDSA-secp384r1-384	RSA-SHA256	2032-09-02

vct.atkvn.com:443

POSITION	SUBJECT	ISSUER	PUBLIC KEY	SIGNATURE	VALID UNTIL
Leaf	vct.atkvn.com	YE1	ECDSA-secp256r1-256	ECDSA-SHA384	2026-12-29
Intermediate	YE1	Root YE	ECDSA-secp384r1-384	ECDSA-SHA384	2028-09-02
Intermediate	Root YE	ISRG Root X2	ECDSA-secp384r1-384	ECDSA-SHA384	2032-09-02
Intermediate	ISRG Root X2	ISRG Root X1	ECDSA-secp384r1-384	RSA-SHA256	2032-09-02

vpqaudit.atkvn.com:443

POSITION	SUBJECT	ISSUER	PUBLIC KEY	SIGNATURE	VALID UNTIL
Leaf	vpqaudit.atkvn.com	YE2	ECDSA-secp256r1-256	ECDSA-SHA384	2026-12-29
Intermediate	YE2	Root YE	ECDSA-secp384r1-384	ECDSA-SHA384	2028-09-02
Intermediate	Root YE	ISRG Root X2	ECDSA-secp384r1-384	ECDSA-SHA384	2032-09-02
Intermediate	ISRG Root X2	ISRG Root X1	ECDSA-secp384r1-384	RSA-SHA256	2032-09-02

Migration Roadmap

Recommended phases aligned to NIST SP 1800-38 transition guidance.

Phase 1 — Quick Wins

3-6
months

24 person-
hours

Migrate TLS Key Exchange: X25519MLKEM768

Effort: 8h Risk: Low (hybrid mode backward compatible) Priority: 5

Migrate Bulk Encryption: AES-128-GCM

Effort: 16h Risk: Low Priority: 5

Phase 2 — Core Migration

6-18
months

136 person-
hours

Migrate Certificate Public Key: ECDSA-secp256r1-256

Effort: 24h Risk: Medium Priority: 1

Migrate Certificate Public Key: ECDSA-secp384r1-384

Effort: 24h Risk: Medium Priority: 4

Migrate Certificate Signature: ECDSA-SHA384

Effort: 24h Risk: Medium Priority: 4

Migrate Certificate Signature: RSA-SHA256

Effort: 24h Risk: Medium (CA ecosystem not fully ready) Priority: 4

Migrate Handshake Hash (HKDF): SHA-256

Effort: 40h Risk: Medium Priority: 5

Cost Estimation

Total effort

191 person-hours

Estimated timeline

3 months

Effort in engineer-hours — multiply by your own blended rate. Estimates carry a $\pm 30\%$ / $+50\%$ confidence band.

Compliance Snapshot

Mapped against NIST and the compliance frameworks enabled for this deployment.

PARTIAL

NIST FIPS 203 (ML-KEM)

Transition to ML-KEM for key encapsulation

No quantum-vulnerable key exchange detected.

FAIL

NIST FIPS 204 (ML-DSA)

Transition to ML-DSA for digital signatures

24 quantum-vulnerable signature/certificate(s) found. ML-DSA (Dilithium) should replace RSA/ECDSA/DSA signatures.

Remediation: Plan certificate migration to ML-DSA when CA ecosystem supports it.

FAIL

NIST SP 800-131A

Remove deprecated cryptographic algorithms

Deprecated algorithms in use: ECDSA-SHA384, ECDSA-secp256r1-256, ECDSA-secp384r1-384

Remediation: Replace with approved alternatives (AES-256, SHA-256+, RSA-2048+/ECDSA-P256+).

PASS

NIST SP 800-57

Minimum cryptographic key lengths

All key lengths meet minimum requirements.

FAIL

CNSA 2.0 — Commercial National Security Algorithm Suite (NSA) — CNSA2-KEX: Key establishment: ML-KEM-1024

Replace classical key establishment (RSA, (EC)DH) with ML-KEM-1024 (FIPS 203). This is the harvest-now-decrypt-later (HNDL) exposure — highest priority for channels carrying long-lived confidential data.

6 findings violate this control. Examples: RSA-SHA256, X25519MLKEM768

Remediation: Replace deprecated primitives with AES-256, SHA-256+, RSA-2048+/ECDSA-P256+. Deploy hybrid post-quantum KEX (X25519MLKEM768) on high-sensitivity channels.

FAIL

CNSA 2.0 — Commercial National Security Algorithm Suite (NSA) — CNSA2-SIG: Digital signatures: ML-DSA-87 (firmware: LMS/XMSS)

Replace classical signatures (RSA, ECDSA) with ML-DSA-87 (FIPS 204); for firmware signing use stateful LMS/XMSS (NIST SP 800-208). Risk is forgery once a CRQC exists — deadline-driven, not HNDL.

21 findings violate this control. Examples: ECDSA-SHA384, ECDSA-secp256r1-256, ECDSA-secp384r1-384

Remediation: Replace deprecated primitives with AES-256, SHA-256+, RSA-2048+/ECDSA-P256+.

FAIL

CNSA 2.0 — Commercial National Security Algorithm Suite (NSA) — CNSA2-SYM: Symmetric & hash: AES-256, SHA-384/512

Use AES-256 and SHA-384/SHA-512. Symmetric/hash primitives face only Grover (halved security) — increasing key size suffices; lower post-quantum priority than KEX/signatures.

3 findings violate this control. Examples: AES-128-GCM

Remediation: Replace deprecated primitives with AES-256, SHA-256+, RSA-2048+/ECDSA-P256+.

PARTIAL

CNSA 2.0 — Commercial National Security Algorithm Suite (NSA) — CNSA2-HYBRID: Transition: PQ hybrid on sensitive channels

During transition, enable hybrid (e.g. X25519MLKEM768) on sensitive channels for immediate HNDL protection with interoperability. (NSA prefers pure-PQ for NSS at the target state.)

Control requires procedural verification; no direct evidence from automated scan.

Remediation: Deploy hybrid post-quantum KEX (X25519MLKEM768) on high-sensitivity channels.

PARTIAL

CNSA 2.0 — Commercial National Security Algorithm Suite (NSA) — CNSA2-ROADMAP: Migration roadmap & timeline

Maintain a migration roadmap with per-asset-class deadlines (software signing 2030; web/cloud 2033; networking/VPN 2030; OS 2033) prioritized by data secrecy lifetime (Mosca inequality).

Control requires procedural verification; no direct evidence from automated scan.

Remediation: Document a PQC migration roadmap following NIST SP 1800-38.

PARTIAL

EU Coordinated Implementation Roadmap for the Transition to PQC (2025) — Milestone 1 — 31.12.2026: First steps: cryptographic asset management, dependency maps, risk analysis

First Steps include: support mature cryptographic asset management, create dependency maps, perform quantum risk analysis, include the supply chain, develop a timeline and an implementation plan; PQC planning and pilots for high- and medium-risk use cases initiated.

Control requires procedural verification; no direct evidence from automated scan.

Remediation: Document a PQC migration roadmap following NIST SP 1800-38.

PARTIAL

EU Coordinated Implementation Roadmap for the Transition to PQC (2025) — Milestone 2 — 31.12.2030: PQC transition for high-risk use cases completed

"High-risk use cases should be transitioned to PQC as soon as possible, no later than the end of 2030"; quantum-safe software and firmware upgrades enabled by default.

Control requires procedural verification; no direct evidence from automated scan.

Remediation: Deploy hybrid post-quantum KEX (X25519MLKEM768) on high-sensitivity channels.

FAIL

EU Coordinated Implementation Roadmap for the Transition to PQC (2025) — Milestone 3 — 31.12.2035: Medium-risk use cases completed; low-risk as far as feasible

By 2035 the PQC transition for medium-risk use cases is completed, and for low-risk use cases as much as feasible.

24 findings violate this control. Examples: ECDSA-SHA384, ECDSA-secp256r1-256, ECDSA-secp384r1-384, RSA-SHA256

PARTIAL

FINMA Guidance 05/2026 — Quantum computing — §3.1: Board-adopted strategy and PQC roadmap by mid-2027

FINMA recommends that the work be based on a strategy adopted by the board of directors, with an implementation plan setting milestones and priorities, target dates for complete migration and for critical business processes. "FINMA recommends that a PQC roadmap be drawn up by mid-2027 at the latest."

Control requires procedural verification; no direct evidence from automated scan.

Remediation: Document a PQC migration roadmap following NIST SP 1800-38.

PARTIAL

FINMA Guidance 05/2026 — Quantum computing — §3.2: Risk analysis and a continuously updated cryptographic inventory

Analyse all business processes to identify encryption, signature and authentication technologies across all ICT systems, in-house, outsourced or as a service; the inventory covers data in transit (VPN, TLS, HTTPS), stored data, digital signatures, key management and authentication, shows which algorithms are quantum-vulnerable (e.g. RSA, ECDSA, EdDSA, DH, EC-DH), and drives a migration plan commensurate with the risk.

Control requires procedural verification; no direct evidence from automated scan.

PARTIAL

FINMA Guidance 05/2026 — Quantum computing — §3.3: Protect critical data against harvest-now-decrypt-later

FINMA recommends taking the risk of harvest-now-decrypt-later attacks into account: data that must stay protected in the long term should be given priority and protected using PQC algorithms; hybrid schemes are frequently cited for this.

Control requires procedural verification; no direct evidence from automated scan.

Remediation: Enable hybrid key exchange (X25519MLKEM768) first on channels that carry data needing long-term confidentiality.

N/A

FINMA Guidance 05/2026 — Quantum computing — §3.4: Crypto-agility as a requirement for systems procured or developed

Crypto-agility (swapping algorithms without major architectural change) is recommended as a requirement for ICT systems and applications to be procured or developed.

Not automatically checked.

N/A

FINMA Guidance 05/2026 — Quantum computing — §3.5: External service providers migrate too

Outsourced functions and external interfaces create dependencies: service providers must also switch to quantum-safe cryptography, planned with them over release cycles; responsibility stays with the outsourcing institution (FINMA Circular 2018/3).

Not automatically checked.

PARTIAL

UK NCSC — Timelines for migration to PQC (2025) — By 2028: Define goals, full discovery, initial migration plan

"Define your migration goals, carry out a full discovery exercise, build an initial plan."

Control requires procedural verification; no direct evidence from automated scan.

Remediation: Document a PQC migration roadmap following NIST SP 1800-38.

PARTIAL

UK NCSC — Timelines for migration to PQC (2025) — By 2031: Highest-priority migration done, plan refined

"Carry out your early, highest-priority PQC migration activities, refine your plan."

Control requires procedural verification; no direct evidence from automated scan.

Remediation: Deploy hybrid post-quantum KEX (X25519MLKEM768) on high-sensitivity channels.

FAIL

UK NCSC — Timelines for migration to PQC (2025) — By 2035: Migration of all systems, services and products complete

"Complete migration to PQC of all your systems, services and products."

24 findings violate this control. Examples: ECDSA-SHA384, ECDSA-secp256r1-256, ECDSA-secp384r1-384, RSA-SHA256

PASS

NIST IR 8547 (initial public draft) — Transition to PQC Standards — Tables 2 & 4 — 112-bit: 112-bit quantum-vulnerable keys deprecated after 2030

RSA, ECDSA, finite-field and elliptic-curve DH at 112 bits of security strength (e.g. RSA-2048, P-224): "Deprecated after 2030".

No violations detected within scope.

FAIL

NIST IR 8547 (initial public draft) — Transition to PQC Standards — Tables 2 & 4 — all strengths: All quantum-vulnerable algorithms disallowed after 2035

Quantum-vulnerable digital signatures (RSA, ECDSA, EdDSA) and key establishment (DH, ECDH, RSA) at every security strength: "Disallowed after 2035". Replacements: FIPS 203 (ML-KEM), FIPS 204 (ML-DSA), FIPS 205 (SLH-DSA).

24 findings violate this control. Examples: ECDSA-SHA384, ECDSA-secp256r1-256, ECDSA-secp384r1-384, RSA-SHA256

PARTIAL

NIST SP 1800-38 — Migration to Post-Quantum Cryptography — SP1800-38-1: Cryptographic discovery

Inventory every cryptographic algorithm, key, and certificate in use across all systems and applications.

Control requires procedural verification; no direct evidence from automated scan.

FAIL

NIST SP 1800-38 — Migration to Post-Quantum Cryptography — SP1800-38-2: Risk assessment

Identify quantum-vulnerable primitives (classical RSA, ECC, DH) and assess harvest-now-decrypt-later risk.

24 findings violate this control. Examples: ECDSA-SHA384, ECDSA-secp256r1-256, ECDSA-secp384r1-384, RSA-SHA256

Remediation: Deploy hybrid post-quantum KEX (X25519MLKEM768) on high-sensitivity channels.

PARTIAL

NIST SP 1800-38 — Migration to Post-Quantum Cryptography — SP1800-38-3: Migration planning

Build a phased migration roadmap (discovery → hybrid → PQ-only) with timelines and cost estimates.

Control requires procedural verification; no direct evidence from automated scan.

Remediation: Document a PQC migration roadmap following NIST SP 1800-38.

PARTIAL

NIST SP 1800-38 — Migration to Post-Quantum Cryptography — SP1800-38-4: Deploy hybrid key exchange

Deploy hybrid key exchange (e.g., X25519MLKEM768) on high-sensitivity channels before moving to PQ-only.

Control requires procedural verification; no direct evidence from automated scan.

Remediation: Deploy hybrid post-quantum KEX (X25519MLKEM768) on high-sensitivity channels.

PARTIAL

NIST SP 1800-38 — Migration to Post-Quantum Cryptography — SP1800-38-5: Crypto-agility & monitoring

Systems must allow algorithm changes without a full rebuild (crypto-agility); continuously monitor algorithm inventory.

Control requires procedural verification; no direct evidence from automated scan.

PARTIAL

PCI DSS v4.0.1 — cryptography requirements — Req. 12.3.3: Cipher suite and protocol inventory, reviewed every 12 months

"Cryptographic cipher suites and protocols in use are documented and reviewed at least once every 12 months, including at least: an up-to-date inventory of all cryptographic cipher suites and protocols in use, including purpose and where used; active monitoring of industry trends regarding continued viability of all cryptographic cipher suites and protocols in use; documentation of a plan to respond to anticipated changes in cryptographic vulnerabilities."

Control requires procedural verification; no direct evidence from automated scan.

Remediation: Export the 12.3.3 inventory (report format 'pci-12.3.3', CSV): one row per protocol and cipher suite with where it is used and its status; fill in the purpose column; repeat the assessment yearly and compare runs with the before/after report. Document the response plan: post-quantum migration is the anticipated change.

PASS

PCI DSS v4.0.1 — cryptography requirements — Req. 4.2.1: Strong cryptography for PAN over open, public networks

Only trusted keys and certificates are accepted; certificates are valid and not expired or revoked; the protocol supports only secure versions or configurations, with no fallback to insecure versions, algorithms or key sizes; encryption strength is appropriate for the methodology in use.

No violations detected within scope.

Sign-off

PREPARED BY

REVIEWED BY

APPROVED BY