SecureAzCloud PQC Cloud & Workload Identity Migration Checklist

Redacted public checklist covering certificates, workload identities, PKI, TLS/mTLS, token signing, key lifecycle, SaaS dependencies, and cloud/IAM migration controls.

Version: v1.0 | Updated: 2026-06-07 | Maintainer: SecureAzCloud | Public URL: https://cyberautomationx.github.io/Post-Quantum-Migration-Hub/

This artifact is a public/redacted planning aid. It uses example rows and does not include any organization-specific secrets, hostnames, IP addresses, customer data, proprietary architecture, or key material.

Purpose and Outcome

This checklist converts PQC readiness into practical cloud and identity migration tasks. It focuses on certificates, workload identities, PKI, TLS/mTLS, token signing, key lifecycle, SaaS dependencies, CI/CD signing, provider-managed services, vendor readiness, and non-production pilot evidence.

CISA 2026 Product-Category Alignment

CISA's January 2026 product-category release for PQC adoption identifies hardware and software categories and explicitly references cloud services, web software, and endpoint security. This artifact maps cloud/IAM migration tasks to those categories and to adjacent dependencies such as identity, PKI, SaaS, KMS/HSM, and signing systems.

Checklist Coverage

Domain	Checklist Focus	Evidence
Governance	Cloud/IAM ownership, change control, tenant/account/project scope, risk acceptance, exception handling.	Charter, RACI, decision records.
Certificates and TLS/mTLS	Managed certificates, private/public CA, certificate automation, TLS endpoints, API gateways, proxies, service mesh.	Certificate scans, CA exports, TLS scan, proxy/gateway config.
PKI	CA roadmap, certificate profiles, chain-size and relying-party constraints, renewal automation.	CA profile, vendor roadmap, test results.
Workload identities	Service principals, managed identities, IAM roles, service accounts, SPIFFE/SPIRE, service mesh identities, CI/CD identities.	IAM exports, trust-bundle map, service mesh config.
Token signing/federation	OIDC, OAuth, SAML, JWT, federation metadata, verifier libraries, relying parties.	IdP config, signing-key inventory, relying-party test results.
Key lifecycle	KMS/HSM, secrets managers, envelope encryption, key wrapping, backup, recovery, rotation, destruction.	KMS/HSM export, key policy, recovery test.
SaaS and suppliers	Vendor roadmap, cryptographic disclosure, support windows, product-category alignment, procurement language.	Vendor response, contract clause, support commitment.
Testing and operations	Non-production pilot, interoperability, performance, logging, rollback, incident runbooks.	Pilot report, change record, rollback evidence.

Representative Cloud/IAM Checklist Items

Priority	Task	Why It Matters
P1	Inventory managed TLS/mTLS endpoints, certificate issuers, validity periods, algorithms, and termination layers.	Certificate and TLS dependencies are common PQC blockers.
P1	Inventory workload identities: service principals, managed identities, IAM roles, Kubernetes service accounts, SPIFFE/SPIRE IDs, service mesh identities, and CI/CD identities.	Machine identity often relies on certificates, tokens, or signed assertions.
P1	Map OIDC/OAuth/SAML/JWT token-signing algorithms and relying-party verifier libraries.	Issuer readiness is insufficient if relying parties cannot validate.

Priority	Task	Why It Matters
P1	Request cloud, SaaS, IdP, CA, KMS/HSM, and signing vendors' PQC roadmaps and test evidence.	Supplier-controlled cryptography determines feasible timelines.
P1	Pilot TLS/mTLS, token signing, API gateways, service mesh, artifact signing, logging, and rollback in non-production.	Migration should be proven before production rollout.
P2	Update runbooks for certificate renewal failures, trust-bundle distribution, token-signing key changes, and rollback.	Cloud identity outages can be broad and fast-moving.

Pilot Acceptance Criteria

• TLS/mTLS tests complete with acceptable handshake success, error rate, latency, certificate-chain handling, and logging.

• OIDC/OAuth/SAML/JWT test tokens validate across P1 relying parties or have documented exceptions.

• Artifact signing and verification work across build, registry, deployment, and enforcement points.

• KMS/HSM/secrets lifecycle tests demonstrate rotation, recovery, logging, and rollback.

• Operational runbooks include owner, decision authority, monitoring signals, rollback command path, and evidence-retention requirements.

Deliverables in the XLSX Template

• Checklist: cloud/IAM migration controls with status, priority, owner, due date, evidence link, and notes.

• Workload_Identity_Inventory: structured machine-identity inventory for cloud-native and CI/CD systems.

• Certificate_and_Key_Map: TLS, mTLS, token signing, certificate, KMS/HSM, and key lifecycle mapping.

• CISA_Category_Map: product-category alignment for cloud, web software, endpoint/data-at-rest, SaaS, IAM, and CI/CD signing.

• Pilot_Test_Plan: test cases for TLS, token signing, artifact signing, key lifecycle, and rollback.

Source and Standards Map

Public sources used to align this artifact. URLs are included for auditability.

Source	Artifact Alignment	Public URL
NIST FIPS 203 - Module-Lattice-Based Key-Encapsulation Mechanism Standard (ML-KEM)	PQC key establishment/key encapsulation planning for TLS, VPN, API, and machine-to-machine trust dependencies.	https://csrc.nist.gov/pubs/fips/203/final
NIST FIPS 204 - Module-Lattice-Based Digital Signature Standard (ML-DSA)	Digital signature migration planning for certificates, code signing, artifact signing, identity token signing, and PKI roadmaps.	https://csrc.nist.gov/pubs/fips/204/final
NIST FIPS 205 - Stateless Hash-Based Digital Signature Standard (SLH-DSA)	Hash-based signature planning for conservative signature-use cases where size/performance tradeoffs are acceptable.	https://csrc.nist.gov/pubs/fips/205/final
NIST NCCoE Migration to Post-Quantum Cryptography	Cryptographic discovery, inventory, risk-prioritization, and interoperability-testing workflow.	https://www.nccoe.nist.gov/applied-cryptography/migration-to-pqc
NIST CSWP 39 - Considerations for Achieving Crypto Agility	Crypto-agility strategy, governance, algorithm/configuration abstraction, operational continuity, and lifecycle planning.	https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.39.pdf
CISA - Product Categories for Technologies That Use Post-Quantum Cryptography Standards	2026 product-category reference for PQC adoption, including cloud services, web software, and endpoint security categories.	https://content.govdelivery.com/accounts/USDHSCISA/bulletins/405c246
CISA/NSA/NIST - Quantum-Readiness: Migration to Post-Quantum Cryptography	Quantum-readiness roadmap, cryptographic inventory, vendor engagement, and supply-chain dependency assessment.	https://www.cisa.gov/resources-tools/resources/quantum-readiness-migration-post-quantum-cryptography
CISA - Post-Quantum Considerations for Operational Technology	OT/ICS/SCADA migration considerations for safety, performance, vendor dependency, and operational continuity.	https://www.cisa.gov/resources-tools/resources/post-quantum-considerations-operational-technology
NIST SP 800-82 Rev. 3 - Guide to Operational Technology Security	OT security planning that accounts for performance, reliability, safety, and physical process constraints.	https://csrc.nist.gov/pubs/sp/800/82/r3/final
NIST SP 800-161 Rev. 1 Update 1 - Cybersecurity Supply Chain Risk Management Practices	Supplier roadmap, procurement, support-window tracking, and supply-chain risk-management evidence.	https://csrc.nist.gov/publications/search?keywords-lg=800-161
NIST Cybersecurity Framework 2.0	Govern, Identify, Protect, Detect, Respond, and Recover framing for migration governance and risk communication.	https://www.nist.gov/cyberframework