SecureAzCloud Crypto-Agility Assessment Template

Redacted public PDF companion for the XLSX assessment template: crypto inventory fields, long-lived data flag, risk scoring, migration priority, and supplier evidence.

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

The Crypto-Agility Assessment Template converts a cryptographic inventory into a risk-prioritized migration backlog. It is designed to show concrete implementation work: inventory fields, long-lived data flags, risk scoring, supplier readiness, migration effort, evidence links, and P1/P2/P3 prioritization.

Recommended Workflow

- Inventory systems that use public-key cryptography, including TLS, SSH, VPN, PKI, code signing, token signing, S/MIME, device authentication, firmware signing, cloud KMS/HSM, and OT remote access.
- Flag long-lived sensitive data and harvest-now-decrypt-later exposure.
- Score quantum vulnerability, business criticality, external exposure, supplier readiness, and migration effort.
- Prioritize P1/P2/P3 actions and convert P1/P2 items into a migration roadmap with owners, target dates, and evidence links.
- Validate architecture, vendor support, interoperability, performance, logging, and rollback before production deployment.

Core Inventory Fields

Field Group	Representative Fields	Use in Assessment
Asset context	Asset ID, system/service, environment, function, owner, data classification	Defines ownership, scope, and business context.
Data life	Long-lived data flag, confidentiality horizon, regulated data indicator	Identifies data most exposed to harvest-now-decrypt-later risk.
Exposure and criticality	Internet/partner/internal/isolated exposure, business criticality	Weights prioritization based on attack surface and operational importance.
Cryptographic dependency	Function, protocol/use case, algorithm/key type, key size/curve, certificate/key store	Identifies quantum-vulnerable public-key usage and certificate constraints.
Supplier/implementation	Vendor/product, library/provider, firmware/hardware dependency, PQC support status	Captures supply-chain and upgrade readiness.
Risk and priority	Data life score, exposure score, criticality score, quantum vulnerability score, supplier readiness, migration effort, risk score, P1/P2/P3	Converts inventory into migration sequencing.
Evidence	Evidence link, target quarter, notes	Supports auditability and recurring program review.

Default Risk Scoring Model

Factor	Default Weight	High Score Indicates	Evidence Examples
Data Life Score	25%	Long-lived/sensitive data remains valuable after future quantum capability.	Retention schedule, data classification, confidentiality horizon.
External Exposure Score	15%	Asset is internet-facing or partner-accessible.	Attack surface scan, network zone, access path.

Factor	Default Weight	High Score Indicates	Evidence Examples
Criticality Score	20%	Asset supports critical business, safety, regulatory, or customer-trust functions.	BIA, critical service map, RTO/RPO.
Quantum Vulnerability Score	25%	RSA, DH, ECDH, or ECDSA is used for public-key security.	Certificate scan, library report, protocol scan.
Supplier Readiness Score	10%	Vendor roadmap is unknown, unsupported, or lacks tested PQC path.	Vendor response, product roadmap, support contract.
Migration Effort Score	5%	Crypto is embedded, firmware-bound, or requires refactoring.	Architecture record, firmware inventory, change-impact analysis.

Sample Redacted Inventory Rows

Asset	Crypto Use	Risk Drivers	Priority Action
Example customer portal TLS	ECDHE/RSA TLS endpoint	Internet-facing, sensitive data, public-key dependency, certificate chain compatibility.	P1/P2 based on data life and exposure; test TLS/PQC or hybrid support in non-production.
Example code-signing pipeline	RSA artifact signing	Software supply-chain trust and verifier compatibility.	Request signing roadmap; test verification path before production.
Example OT remote-access gateway	VPN/TLS certificate authentication	Safety impact, legacy gateway, partner access, firmware dependency.	P1; require lab validation, maintenance window, vendor guidance, and rollback.
Example cloud data lake encryption	AES-256 with managed KMS	Long-lived sensitive data and KMS/provider lifecycle dependency.	Track KMS/HSM roadmap and key lifecycle; validate no hidden RSA/ECDH wrapper dependency.
Example workload identity federation	OIDC/JWT token signing	Relying-party verification and identity outage risk.	Inventory signing keys and verifiers; pilot compatible migration path.

Deliverables in the XLSX Template

- Start_Here: public/redacted instructions and evidence standard.
- Crypto_Inventory: dropdown-enabled inventory with scoring formulas and P1/P2/P3 prioritization.
- Assessment_Checklist: governance, inventory, architecture, PKI, cloud/IAM, supplier, testing, operations, and training readiness controls.
- Scoring_Model: default scoring weights and interpretation.
- Migration_Roadmap: five-phase migration roadmap from discovery through operationalization.
- Vendor_Questions: supplier roadmap and cryptographic disclosure questions.
- Sources: NIST, CISA, and standards reference map.

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