

Post-Quantum Cryptography Migration and Algorithm Portfolio Standard



Architecture & Assurance Map

A compact reasoning model for implementation, assessment, and evidence review.



OPERATING POSITION

Cryptography is a migration program, not an algorithm selection exercise.

EVIDENCE PATH

inventory -> policy -> algorithm portfolio -> deployment -> attestation -> rotation

READINESS SIGNALS

agility, hybrid transition, key lifecycle, side-channel and implementation evidence

PERMANENT PUBLICATION IDENTITY

Post-Quantum Cryptography Migration and Algorithm Portfolio Standard			DOCUMENT ID MYTHOS-QTC-0002 VERSION 1.0.0-candidate STATUS Candidate Standard PUBLISHER Mythos Systems PUBLICATION DATE 2026-07-24 SCHEDULED REVIEW 2027-01-24 CLASSIFICATION Public
18 ATOMIC CRITERIA	6 ASSURANCE VIEWS	4 IMPLEMENTATION PROFILES	1 PERMANENT IDENTITY

Publication doctrine. This publication establishes durable requirements for its defined scope. Interpretation must preserve the permanent document identity, required evidence, controlled exceptions, source currency, and formal revision history.

EMERGING TECHNOLOGY AND ASSURANCE TOPOLOGY

Quantum Technology and Computing

A trustworthy post-quantum cryptography migration program is a governed path from research claim through baseline, experiment, safety and security challenge, transition decision, bounded operation, and preserved evidence.

CLASSIFY

Separate established practice, candidate standard, reproduced result, vendor claim, implementation hypothesis, and open research.

EXPERIMENT

Declare baseline, configuration, uncertainty, scenario coverage, stop conditions, and independent reproduction before conclusions.

CONSTRAIN

Identity, policy, safety envelopes, physical boundaries, cryptographic authority, and human intervention limit consequence.

TRANSITION

Adoption, pilot, production, rollback, supplier exit, lifecycle, and retirement decisions remain evidence-bearing and reversible.

EVIDENCE-BOUND TRANSITION FLOW



No novelty claim becomes an operational claim without reproduced evidence and an explicit authority decision

INTERPRETATION AND ASSURANCE

How to apply this publication

Normative intent

Requirements define outcomes and constraints. Implementations may vary, but evidence must demonstrate equivalent control.

Evidence over assertion

Vendor documentation and design intent are not equivalent to reproduced behavior. Record evidence grade and uncertainty.

Risk-proportional depth

Higher consequence, autonomy, sensitivity, and irreversibility require stronger isolation, review, verification, and recovery.

Controlled exception

Exceptions require an owner, rationale, compensating control, residual-risk acceptance, expiration, and reevaluation trigger.

Normalized assessment scale

0	1	2	3	4	5
ABSENT	AD HOC	PARTIAL	OPERATIONAL	ADVANCED	LEADING

A numeric score must never hide a failed mandatory gate, missing evidence, untested workload, or unacceptable residual risk.

INTERACTIVE NAVIGATION

Contents

Executive mandate	6
Scope and applicability	7
Definitions and taxonomy	8
Architecture and trust model	9
Governance and accountability	10
Normative control system	11
Evidence and assessment	16
Assurance views and metrics	17
Failure modes and adversarial scenarios	19
Implementation profiles and lifecycle	20
Adoption roadmap and conformance	22
Source authority and revision control	24

Navigation doctrine

Bookmarks and internal links are conveniences. Permanent document identity, criterion identifiers, evidence references, and revision history remain authoritative.

MYTHOS-QTC-0002 / QUANTUM TECHNOLOGY

0. Executive Mandate

Research value, transition discipline, and non-negotiable evidence boundaries

MANDATE

Organizations evaluating post-quantum cryptography migration **MUST** separate research from operational authority, establish a reproducible baseline, constrain safety and security consequence, disclose uncertainty, and require a documented transition or rejection decision.

Required outcomes

- Establish a durable, product-neutral evidence system for post-quantum cryptography migration.
- Prevent novelty, investment, vendor prestige, roadmap language, or laboratory success from substituting for operational proof.
- Require representative performance, adversarial, failure, recovery, safety, privacy, and lifecycle evidence.
- Keep pilots bounded by identity, authority, environment, duration, budget, stop conditions, and rollback.
- Preserve rejected alternatives, limitations, residual risk, source currency, and reassessment triggers.

Decision boundary: conformance supports a bounded engineering assurance position. It does not prove scientific consensus, regulatory approval, universal safety, quantum advantage, cryptographic perfection, autonomous competence, or commercial viability.

MYTHOS-QTC-0002 / QUANTUM TECHNOLOGY

1. Scope and Applicability

Research, pilot, transition, operational, and retirement boundaries

IN SCOPE

- Research, architecture, acquisition, experiment, pilot, transition, operation, and retirement of post-quantum cryptography migration.
- Hardware, software, models, data, protocols, facilities, people, suppliers, providers, physical processes, and evidence.
- Laboratory, simulation, testbed, shadow, pilot, canary, production, and field deployment states.
- Claims, benchmarks, uncertainty, safety, security, privacy, economics, interoperability, support, and exit.

OUT OF SCOPE

- Scientific truth inferred from a single benchmark, simulation, provider, hardware generation, or laboratory configuration.
- Safety, regulatory, export, spectrum, airspace, clinical, cryptographic, or standards approval not granted by the responsible authority.
- Roadmap forecasts, token price, patent counts, press releases, or investment treated as engineering evidence.
- Hidden production use of research components outside the declared transition and assurance boundary.

Applicability triggers

- The capability is novel, rapidly changing, weakly standardized, difficult to reproduce, or dependent on immature suppliers.
- A claim concerns safety, security, privacy, physical action, critical infrastructure, cryptographic trust, or consequential autonomy.
- The system requires specialized facilities, scarce hardware, spectrum, foundry, cryogenic, optical, robotics, or field-test dependencies.
- Failure or lock-in may create long-lived data, capital, infrastructure, workforce, or regulatory consequences.
- A research component is proposed for pilot, customer, production, public, or externally relied-upon use.

MYTHOS-QTC-0002 / QUANTUM TECHNOLOGY

2. Definitions and Taxonomy

Controlled language for architecture, governance, and assessment

AUTHORITY

The right to approve, deny, constrain, or execute an action. Model output is not authority.

EVIDENCE

A reproducible source, trace, measurement, test, record, signed artifact, or documented observation supporting a claim.

ASSURANCE VIEW

A defined perspective such as governance, architecture, security, operations, privacy, or human oversight.

ATOMIC CRITERION

A uniquely identified requirement that can be assessed, evidenced, excepted, and revised independently.

IMPLEMENTATION PROFILE

A risk-proportional set of required depth, evidence, and gates for a class of use.

CONTROLLED EXCEPTION

A time-bounded deviation with owner, rationale, compensating control, residual risk, expiration, and review trigger.

DETERMINISTIC MECHANISM

A component whose inputs, policy, state transition, and side effects can be constrained and verified.

SOURCE AUTHORITY

The documented basis for treating a source as reliable for a defined claim, context, jurisdiction, and time.

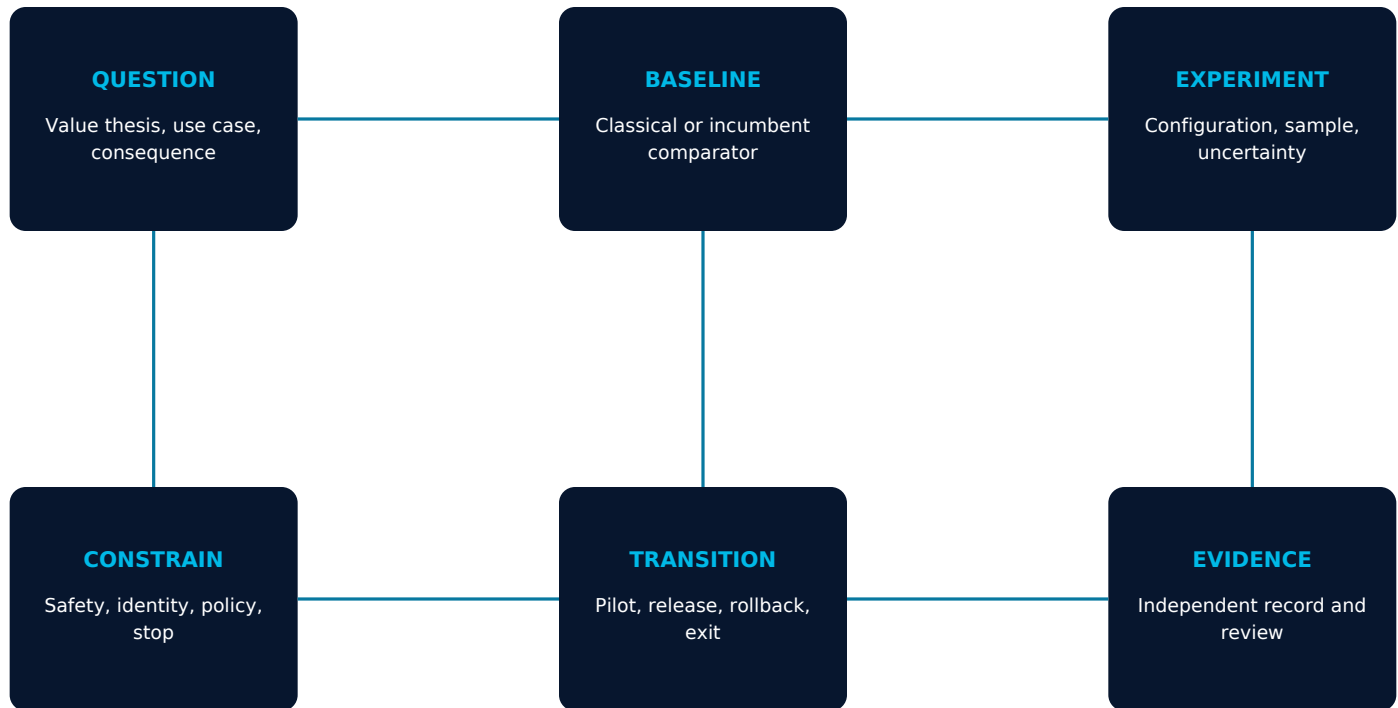
REASSESSMENT TRIGGER

A change, incident, drift signal, dependency revision, or time boundary requiring renewed evaluation.

MYTHOS-QTC-0002 / QUANTUM TECHNOLOGY

3. Architecture and Trust Model

Separation of research, authority, physical systems, runtime, and evidence



Mandatory trust boundaries

- Research systems **MUST NOT** inherit production identity, secrets, authority, data, networks, or physical control by convenience.
- Claims **MUST** retain the exact hardware, software, model, protocol, calibration, environment, workload, and observation boundary.
- Safety, cryptographic, physical, spectrum, autonomy, and human-intervention constraints **MUST** remain independently enforceable.
- Transition **MUST** have a named decision authority, acceptance criteria, monitored pilot, rollback, supplier exit, and retirement path.
- Evidence **MUST** remain reviewable when a vendor, cloud, token network, laboratory, model, robot, or quantum backend is unavailable.

4. Governance and Accountability

Decision rights, separation of duties, and lifecycle ownership

ACCOUNTABLE OWNER

Accepts scope, risk tolerance, funding, and residual risk.

SYSTEM OWNER

Maintains architecture, inventory, operating boundaries, and change control.

SECURITY / PRIVACY

Defines threat, identity, data, isolation, monitoring, and incident requirements.

EVALUATION AUTHORITY

Designs representative tests, gates releases, and preserves reproducibility.

OPERATIONS

Maintains availability, rollback, recovery, evidence, and incident handling.

HUMAN OVERSIGHT

Reviews consequential decisions, exceptions, disputed outcomes, and harm signals.

DECISION PRINCIPLE

No single actor should be able to define the objective, grant authority, execute the consequential action, suppress evidence, and approve the result. Separation must be technical where consequence requires it.

MYTHOS-QTC-0002 / QUANTUM TECHNOLOGY

5. Normative Control System

Atomic criteria 01-04 of 18

MYTHOS-QTC-0002-C01

Cryptographic Discovery and Dependency Graph

The organization **MUST** define, implement, verify, and maintain cryptographic discovery and dependency graph for the declared post-quantum cryptography migration boundary. The record **MUST** identify accountable ownership, evidence state, exact configuration, assumptions, affected people and systems, failure and recovery behavior, uncertainty, transition authority, and reassessment triggers. Quantum and classical resources, calibration or algorithm state, comparator, statistical confidence, provider dependency, and reproducibility artifacts **MUST** remain explicit.

MINIMUM EVIDENCE algorithm, hardware, backend, qubit, calibration, compiler, runtime, and provider inventory

MYTHOS-QTC-0002-C02

Protected-Data Lifetime and Quantum Risk Horizon

The organization **MUST** define, implement, verify, and maintain protected-data lifetime and quantum risk horizon for the declared post-quantum cryptography migration boundary. The record **MUST** identify accountable ownership, evidence state, exact configuration, assumptions, affected people and systems, failure and recovery behavior, uncertainty, transition authority, and reassessment triggers. Quantum and classical resources, calibration or algorithm state, comparator, statistical confidence, provider dependency, and reproducibility artifacts **MUST** remain explicit.

MINIMUM EVIDENCE classical baseline; resource estimate; noise and uncertainty model; acceptance thresholds

MYTHOS-QTC-0002-C03

Algorithm Portfolio and Approved Parameter Sets

The organization **MUST** define, implement, verify, and maintain algorithm portfolio and approved parameter sets for the declared post-quantum cryptography migration boundary. The record **MUST** identify accountable ownership, evidence state, exact configuration, assumptions, affected people and systems, failure and recovery behavior, uncertainty, transition authority, and reassessment triggers. Quantum and classical resources, calibration or algorithm state, comparator, statistical confidence, provider dependency, and reproducibility artifacts **MUST** remain explicit.

MINIMUM EVIDENCE captured circuit, parameters, seeds, shots, mapping, calibration snapshot, and result data

MYTHOS-QTC-0002-C04

ML-KEM Deployment and Encapsulation Policy

The organization **MUST** define, implement, verify, and maintain ml-kem deployment and encapsulation policy for the declared post-quantum cryptography migration boundary. The record **MUST** identify accountable ownership, evidence state, exact configuration, assumptions, affected people and systems, failure and recovery behavior, uncertainty, transition authority, and reassessment triggers. Quantum and classical resources, calibration or algorithm state, comparator, statistical confidence, provider dependency, and reproducibility artifacts **MUST** remain explicit.

MINIMUM EVIDENCE cross-backend, simulator, independent reproduction, and statistical comparison evidence

MYTHOS-QTC-0002 / QUANTUM TECHNOLOGY

5. Normative Control System

Atomic criteria 05-08 of 18

MYTHOS-QTC-0002-C05

ML-DSA, SLH-DSA, and Signature Policy

The organization MUST define, implement, verify, and maintain ml-dsa, slh-dsa, and signature policy for the declared post-quantum cryptography migration boundary. The record MUST identify accountable ownership, evidence state, exact configuration, assumptions, affected people and systems, failure and recovery behavior, uncertainty, transition authority, and reassessment triggers. Quantum and classical resources, calibration or algorithm state, comparator, statistical confidence, provider dependency, and reproducibility artifacts MUST remain explicit.

MINIMUM EVIDENCE cryptographic inventory, hybrid profile, interoperability tests, downgrade tests, and revocation plan

MYTHOS-QTC-0002-C06

Backup KEM and Algorithm-Diversity Strategy

The organization MUST define, implement, verify, and maintain backup kem and algorithm-diversity strategy for the declared post-quantum cryptography migration boundary. The record MUST identify accountable ownership, evidence state, exact configuration, assumptions, affected people and systems, failure and recovery behavior, uncertainty, transition authority, and reassessment triggers. Quantum and classical resources, calibration or algorithm state, comparator, statistical confidence, provider dependency, and reproducibility artifacts MUST remain explicit.

MINIMUM EVIDENCE quantum-channel, timing, authentication, trusted-node, detector, or key-lifecycle evidence

MYTHOS-QTC-0002-C07

Hybrid Classical-PQC Composition

The organization MUST define, implement, verify, and maintain hybrid classical-pqc composition for the declared post-quantum cryptography migration boundary. The record MUST identify accountable ownership, evidence state, exact configuration, assumptions, affected people and systems, failure and recovery behavior, uncertainty, transition authority, and reassessment triggers. Quantum and classical resources, calibration or algorithm state, comparator, statistical confidence, provider dependency, and reproducibility artifacts MUST remain explicit.

MINIMUM EVIDENCE facility, energy, cooling, queue, cost, availability, support, and exit evidence

MYTHOS-QTC-0002-C08

Certificate, PKI, Code-Signing, and Trust-Store Migration

The organization MUST define, implement, verify, and maintain certificate, pki, code-signing, and trust-store migration for the declared post-quantum cryptography migration boundary. The record MUST identify accountable ownership, evidence state, exact configuration, assumptions, affected people and systems, failure and recovery behavior, uncertainty, transition authority, and reassessment triggers. Quantum and classical resources, calibration or algorithm state, comparator, statistical confidence, provider dependency, and reproducibility artifacts MUST remain explicit.

MINIMUM EVIDENCE bounded claim, limitation register, promotion gate, fallback, and long-term evidence package

MYTHOS-QTC-0002 / QUANTUM TECHNOLOGY

5. Normative Control System

Atomic criteria 09-12 of 18

MYTHOS-QTC-0002-C09

Protocol, Library, Hardware, and Vendor Compatibility

The organization MUST define, implement, verify, and maintain protocol, library, hardware, and vendor compatibility for the declared post-quantum cryptography migration boundary. The record MUST identify accountable ownership, evidence state, exact configuration, assumptions, affected people and systems, failure and recovery behavior, uncertainty, transition authority, and reassessment triggers. Quantum and classical resources, calibration or algorithm state, comparator, statistical confidence, provider dependency, and reproducibility artifacts MUST remain explicit.

MINIMUM EVIDENCE algorithm, hardware, backend, qubit, calibration, compiler, runtime, and provider inventory

MYTHOS-QTC-0002-C10

Key, Ciphertext, Signature, and Bandwidth Sizing

The organization MUST define, implement, verify, and maintain key, ciphertext, signature, and bandwidth sizing for the declared post-quantum cryptography migration boundary. The record MUST identify accountable ownership, evidence state, exact configuration, assumptions, affected people and systems, failure and recovery behavior, uncertainty, transition authority, and reassessment triggers. Quantum and classical resources, calibration or algorithm state, comparator, statistical confidence, provider dependency, and reproducibility artifacts MUST remain explicit.

MINIMUM EVIDENCE classical baseline; resource estimate; noise and uncertainty model; acceptance thresholds

MYTHOS-QTC-0002-C11

Randomness, Side Channel, and Implementation Validation

The organization MUST define, implement, verify, and maintain randomness, side channel, and implementation validation for the declared post-quantum cryptography migration boundary. The record MUST identify accountable ownership, evidence state, exact configuration, assumptions, affected people and systems, failure and recovery behavior, uncertainty, transition authority, and reassessment triggers. Quantum and classical resources, calibration or algorithm state, comparator, statistical confidence, provider dependency, and reproducibility artifacts MUST remain explicit.

MINIMUM EVIDENCE captured circuit, parameters, seeds, shots, mapping, calibration snapshot, and result data

MYTHOS-QTC-0002-C12

Downgrade, Negotiation, and Algorithm-Confusion Resistance

The organization MUST define, implement, verify, and maintain downgrade, negotiation, and algorithm-confusion resistance for the declared post-quantum cryptography migration boundary. The record MUST identify accountable ownership, evidence state, exact configuration, assumptions, affected people and systems, failure and recovery behavior, uncertainty, transition authority, and reassessment triggers. Quantum and classical resources, calibration or algorithm state, comparator, statistical confidence, provider dependency, and reproducibility artifacts MUST remain explicit.

MINIMUM EVIDENCE cross-backend, simulator, independent reproduction, and statistical comparison evidence

MYTHOS-QTC-0002 / QUANTUM TECHNOLOGY

5. Normative Control System

Atomic criteria 13-15 of 18

MYTHOS-QTC-0002-C13**Inventory Coverage and Migration Wave Planning**

The organization **MUST** define, implement, verify, and maintain inventory coverage and migration wave planning for the declared post-quantum cryptography migration boundary. The record **MUST** identify accountable ownership, evidence state, exact configuration, assumptions, affected people and systems, failure and recovery behavior, uncertainty, transition authority, and reassessment triggers. Quantum and classical resources, calibration or algorithm state, comparator, statistical confidence, provider dependency, and reproducibility artifacts **MUST** remain explicit.

MINIMUM EVIDENCE cryptographic inventory, hybrid profile, interoperability tests, downgrade tests, and revocation plan

MYTHOS-QTC-0002-C14**Interoperability Lab and Negative Testing**

The organization **MUST** define, implement, verify, and maintain interoperability lab and negative testing for the declared post-quantum cryptography migration boundary. The record **MUST** identify accountable ownership, evidence state, exact configuration, assumptions, affected people and systems, failure and recovery behavior, uncertainty, transition authority, and reassessment triggers. Quantum and classical resources, calibration or algorithm state, comparator, statistical confidence, provider dependency, and reproducibility artifacts **MUST** remain explicit.

MINIMUM EVIDENCE quantum-channel, timing, authentication, trusted-node, detector, or key-lifecycle evidence

MYTHOS-QTC-0002-C15**Performance, Capacity, and Availability Evidence**

The organization **MUST** define, implement, verify, and maintain performance, capacity, and availability evidence for the declared post-quantum cryptography migration boundary. The record **MUST** identify accountable ownership, evidence state, exact configuration, assumptions, affected people and systems, failure and recovery behavior, uncertainty, transition authority, and reassessment triggers. Quantum and classical resources, calibration or algorithm state, comparator, statistical confidence, provider dependency, and reproducibility artifacts **MUST** remain explicit.

MINIMUM EVIDENCE facility, energy, cooling, queue, cost, availability, support, and exit evidence

MYTHOS-QTC-0002 / QUANTUM TECHNOLOGY

5. Normative Control System

Atomic criteria 16-18 of 18

MYTHOS-QTC-0002-C16**Emergency Revocation and Algorithm Withdrawal**

The organization **MUST** define, implement, verify, and maintain emergency revocation and algorithm withdrawal for the declared post-quantum cryptography migration boundary. The record **MUST** identify accountable ownership, evidence state, exact configuration, assumptions, affected people and systems, failure and recovery behavior, uncertainty, transition authority, and reassessment triggers. Quantum and classical resources, calibration or algorithm state, comparator, statistical confidence, provider dependency, and reproducibility artifacts **MUST** remain explicit.

MINIMUM EVIDENCE bounded claim, limitation register, promotion gate, fallback, and long-term evidence package

MYTHOS-QTC-0002-C17**Legacy Decommissioning and Long-Lived Data Protection**

The organization **MUST** define, implement, verify, and maintain legacy decommissioning and long-lived data protection for the declared post-quantum cryptography migration boundary. The record **MUST** identify accountable ownership, evidence state, exact configuration, assumptions, affected people and systems, failure and recovery behavior, uncertainty, transition authority, and reassessment triggers. Quantum and classical resources, calibration or algorithm state, comparator, statistical confidence, provider dependency, and reproducibility artifacts **MUST** remain explicit.

MINIMUM EVIDENCE algorithm, hardware, backend, qubit, calibration, compiler, runtime, and provider inventory

MYTHOS-QTC-0002-C18**Migration Evidence, Exceptions, and Reassessment**

The organization **MUST** define, implement, verify, and maintain migration evidence, exceptions, and reassessment for the declared post-quantum cryptography migration boundary. The record **MUST** identify accountable ownership, evidence state, exact configuration, assumptions, affected people and systems, failure and recovery behavior, uncertainty, transition authority, and reassessment triggers. Quantum and classical resources, calibration or algorithm state, comparator, statistical confidence, provider dependency, and reproducibility artifacts **MUST** remain explicit.

MINIMUM EVIDENCE classical baseline; resource estimate; noise and uncertainty model; acceptance thresholds

MYTHOS-QTC-0002 / QUANTUM TECHNOLOGY

6. Evidence and Assessment

Reproduce, compare, challenge, observe, recover, and trace

EXAMINE

Research papers, standards, designs, bills of material, protocols, source, models, data, calibration, configurations, contracts, and claims.

REPRODUCE

Repeat the experiment or assessment with captured versions, seeds, parameters, environment, uncertainty, and acceptance criteria.

COMPARE

Use an honest incumbent, classical, manual, or alternative baseline with equivalent outcome, data, scale, and resource accounting.

CHALLENGE

Apply adversarial input, environmental variation, dependency loss, fault injection, safety cases, security tests, and boundary conditions.

OBSERVE

Measure field or production-like quality, latency, energy, drift, physical behavior, interventions, failures, maintenance, and user impact.

TRACE

Link claim, authority, experiment, configuration, evidence, decision, pilot, change, incident, rollback, and reassessment.

Evidence grades

A

Independently reproduced, current, representative, uncertainty-bounded, integrity-protected, and operationally relevant.

B

Reproduced by the implementing organization with strong provenance, comparator, challenge, and declared limitations.

C

Partial, laboratory-only, simulation-heavy, inherited, or indirect evidence with material uncertainty and dependencies.

D

Roadmap, assertion, demonstration, benchmark excerpt, patent, token metric, press release, or vendor statement without...

MYTHOS-QTC-0002 / QUANTUM TECHNOLOGY

7. Assurance Views

Six perspectives required for a complete assurance claim

GOVERNANCE

Ownership, purpose, risk tolerance, policy, exception, and decision rights.

ARCHITECTURE

Boundaries, dependencies, failure modes, state, data flow, and portability.

SECURITY

Identity, authorization, isolation, secrets, abuse resistance, and incident response.

OPERATIONS

Reliability, performance, cost, observability, change, recovery, and support.

PRIVACY / RIGHTS

Purpose limitation, minimization, consent, access, correction, deletion, and egress.

HUMAN / SOCIETAL

Usability, accessibility, disclosure, contestability, impact, and human control.

Conformance requires a defensible position across every applicable view. A strong aggregate score cannot compensate for an unowned system, a failed mandatory gate, untested recovery, or evidence below the accepted grade.

7.2 Evaluation Metrics and Decision Gates

Measures expose utility, uncertainty, safety, physical limits, transition cost, and lifecycle burden

UTILITY

Task outcome, comparator delta, coverage, quality, accuracy, mission success, and stakeholder value.

UNCERTAINTY

Confidence, calibration, variance, sample coverage, reproducibility, sensitivity, and unresolved assumptions.

PERFORMANCE

Latency, throughput, fidelity, range, precision, bandwidth, scale, density, and availability.

SAFETY / SECURITY

Hazard exposure, unsafe action, exploitability, spoofing, physical consequence, intervention, and containment.

RESOURCE

Energy, power, cooling, spectrum, shots, qubits, memory, materials, facility, operator, and maintenance demand.

MATURITY

Standards state, supply chain, interoperability, tooling, skills, support, qualification, and lifecycle readiness.

ECONOMICS

Acquisition, operation, provider, token, facility, migration, insurance, support, and opportunity cost.

TRANSITION

Pilot escape, rollback time, incumbent fallback, portability, lock-in, retirement, and evidence completeness.

Decision gate: thresholds **MUST** be declared before assessment, include an incumbent baseline and uncertainty statement, and identify any safety, security, cryptographic, physical, reproducibility, or rollback failure that blocks transition.

MYTHOS-QTC-0002 / QUANTUM TECHNOLOGY

8. Failure Modes and Adversarial Scenarios

Challenge assumptions before the system is trusted with consequential work

QUANTUM ADVANTAGE OVERCLAIM

A narrow or non-comparable experiment is presented as useful superiority over classical methods.

REQUIRED: PREVENT | DETECT | CONTAIN | RECOVER | EVIDENCE

CALIBRATION INVALIDATION

Backend drift or missing calibration state makes results irreproducible or misleading.

REQUIRED: PREVENT | DETECT | CONTAIN | RECOVER | EVIDENCE

CRYPTOGRAPHIC TRANSITION FAILURE

Legacy algorithms, protocol gaps, or downgrade paths survive after PQC migration claims.

REQUIRED: PREVENT | DETECT | CONTAIN | RECOVER | EVIDENCE

QUANTUM CHANNEL COMPROMISE

Trusted nodes, detectors, timing, classical authentication, or devices violate the stated security model.

REQUIRED: PREVENT | DETECT | CONTAIN | RECOVER | EVIDENCE

RESOURCE-ESTIMATION COLLAPSE

Logical qubit, error correction, runtime, facility, or cost assumptions invalidate the roadmap.

REQUIRED: PREVENT | DETECT | CONTAIN | RECOVER | EVIDENCE

PROVIDER AND EVIDENCE LOSS

Remote hardware, queue behavior, configuration, or experiment records cannot be independently reproduced.

REQUIRED: PREVENT | DETECT | CONTAIN | RECOVER | EVIDENCE

Adversarial testing MUST protect people and production systems. Use isolated environments, synthetic or minimized data, bounded authority, kill switches, explicit legal and ethical review, and documented stop conditions.

9. Implementation Profiles

Risk-proportional implementation without weakening mandatory boundaries

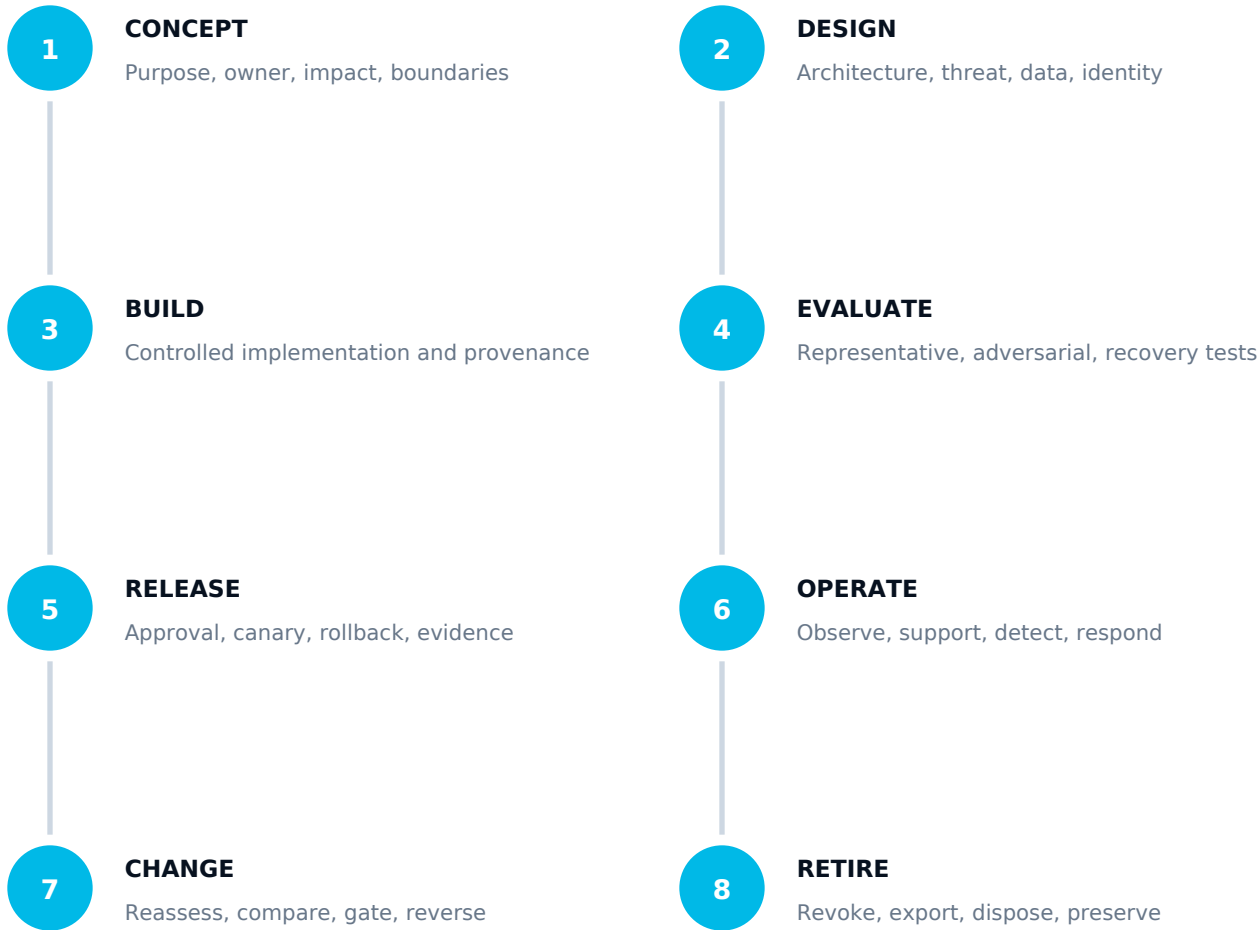
FOUNDATIONAL TYPICAL SCOPE Low consequence, limited autonomy, non-sensitive data, reversible outputs. MINIMUM DEPTH Named owner; inventory; basic evaluation; access control; logging; rollback; annual review.	ADVANCED TYPICAL SCOPE Business-critical workflow, sensitive data, multiple tools or providers, moderate autonomy. MINIMUM DEPTH Formal threat model; representative evaluation; approval gates; isolated execution; tested recovery; quarterly review.	HIGH ASSURANCE TYPICAL SCOPE Safety, security, regulated, financial, identity, or broadly consequential use. MINIMUM DEPTH Independent challenge; strongest identity; deterministic enforcement; comprehensive evidence; canary release; continuous monitoring.
---	---	---

Profile selection rule

Choose the highest profile triggered by consequence, autonomy, sensitivity, scale, irreversibility, external dependency, or inability to rapidly detect and recover. Tailoring may strengthen controls; it may not erase a mandatory gate without a controlled exception.

9.2 Operational Lifecycle

Evidence-bearing operation from concept through retirement



LIFECYCLE INVARIANT

Every stage **MUST** leave sufficient evidence for the next authority to understand what was intended, what changed, what was tested, what failed, what was accepted, what remains uncertain, and how to recover or exit.

MYTHOS-QTC-0002 / QUANTUM TECHNOLOGY

10. Adoption Roadmap

A sequenced path from uncontrolled capability to evidence-bearing operation

0-30 DAYS**Establish ownership and truth**

Inventory systems and dependencies; classify risk; freeze unsupported claims; identify immediate privilege, data, and evidence gaps.

31-90 DAYS**Create enforceable boundaries**

Define policy; isolate execution; implement identity and approval gates; establish representative evaluation and baseline telemetry.

3-6 MONTHS**Prove recovery and operating control**

Exercise failure, rollback, revocation, incident, provider exit, and state-recovery scenarios; mature evidence packaging.

6-12 MONTHS**Scale assurance**

Automate control checks; expand workload coverage; independent challenge; portfolio metrics; controlled exception expiry; continuous reassessment.

Adoption is complete only when operating evidence demonstrates the selected profile in the actual deployment context. Documentation alone is not conformance.

10.2 Conformance and Exception Statement

What an assurance claim must contain

SYSTEM / SERVICE Named, versioned capability and deployment boundary.	PROFILE Foundational, Advanced, or High Assurance with trigger rationale.
SCOPE Workloads, users, data, tools, regions, providers, and exclusions.	CRITERIA Pass, partial, fail, not applicable, and exception status for every criterion.
EVIDENCE Artifact references, evidence grade, date, environment, and reproducibility.	LIMITATIONS Known failure modes, unsupported workloads, uncertainty, and residual risk.
EXCEPTIONS Owner, rationale, compensating control, expiration, and approval.	VALIDITY Assessment date, change boundary, review date, and reassessment triggers.

Prohibited claim: “compliant” without the named scope, profile, evidence date, limitations, exceptions, and authority accepting residual risk.

MYTHOS-QTC-0002 / QUANTUM TECHNOLOGY

11. Source Authority and Reference Register

Primary sources informing interpretation; verify current status at assessment time

NIST CSF 2.0

Cybersecurity Framework 2.0

<https://doi.org/10.6028/NIST.CSWP.29>

Enterprise governance and cybersecurity outcome framework.

NIST PQC Standards

Post-Quantum Cryptography Project

<https://csrc.nist.gov/projects/post-quantum-cryptography>

FIPS 203, 204, and 205, HQC selection, and continuing migration guidance.

NIST SP 800-53 Rev. 5

Security and Privacy Controls for Information Systems and Organizations

<https://doi.org/10.6028/NIST.SP.800-53r5>

Broad organizational control baseline for technology systems and services.

ETSI QKD

Quantum Key Distribution Industry Specification Group

<https://www.etsi.org/committee/qkd>

QKD component, interface, security, deployment, and interoperability specifications.

NIST Quantum Science

Quantum Science Programs and Testbeds

<https://www.nist.gov/quantum-science>

Official NIST research across quantum computing, communications, networking, sensing, and metrology.

ISO/IEC 4879:2024

Quantum Computing - Terminology and Vocabulary

<https://www.iso.org/standard/80432.html>

International terminology foundation for quantum computing concepts.

NIST Quantum Networks

Quantum Networks at NIST

<https://www.nist.gov/pml/productsservices/quantum-networks-nist>

Quantum-network concepts, components, applications, and metropolitan research testbeds.

Source currency rule: authorities, specifications, laws, provider services, hardware, protocols, standards status, and research evidence MUST be checked at assessment time. This publication records a 2026-07-24 source snapshot.

11.2 Revision History and Decision Register

Permanent identity, controlled change, and publication integrity

VERSION	DATE	STATE	SUMMARY
1.0.0-candidate	2026-07-24	Candidate	Permanent-publication edition; source refresh; expanded criteria, evidence, assurance, and lifecycle guidance.
Next review	2027-01-24	Scheduled	Review source currency, threat evolution, operating evidence, adoption feedback, and proposed revisions.

Publication decisions

- PERMANENT IDENTITY** The document ID remains stable across revisions; batch or production sequence metadata is not public identity.
- CHANGE CONTROL** Normative changes require rationale, impact analysis, affected-criterion mapping, and approval.
- SUPERSESSION** A superseded edition remains traceable; current routes and catalogs identify the active edition.
- CORRECTION** Material errors require a recorded correction, affected-evidence analysis, and notification appropriate to impact.
- ARCHIVAL INTEGRITY** Published artifacts receive hashes, metadata, and a release manifest sufficient for independent verification.