MYTHOS SYSTEMS

PERMANENT LIBRARY PUBLICATION

ENGINEERING STANDARDS LIBRARY / CYBERSECURITY AND NETWORK SECURITY

Post-Quantum Cryptography and Crypto-Agility Standard

Defines cryptographic inventory, agility, approved algorithms, hybrid migration, testing, and lifecycle.

PERMANENT DOCUMENT ID
MYTHOS-SEC-0001

PUBLICATION
Candidate Standard

ASSURANCE SURFACE
7 Atomic Criteria / 6 Families

PERMANENT PUBLICATION IDENTITY

Post-Quantum Cryptography and Crypto-Agility Standard

Defines cryptographic inventory, agility, approved algorithms, hybrid migration, testing, and lifecycle.

DOCUMENT ID
MYTHOS-SEC-0001

VERSION
1.0.0-candidate

STATUS
Candidate Standard

PUBLISHER
Mythos Systems

PUBLICATION DATE
2026-07-23

SCHEDULED REVIEW
2027-01-23

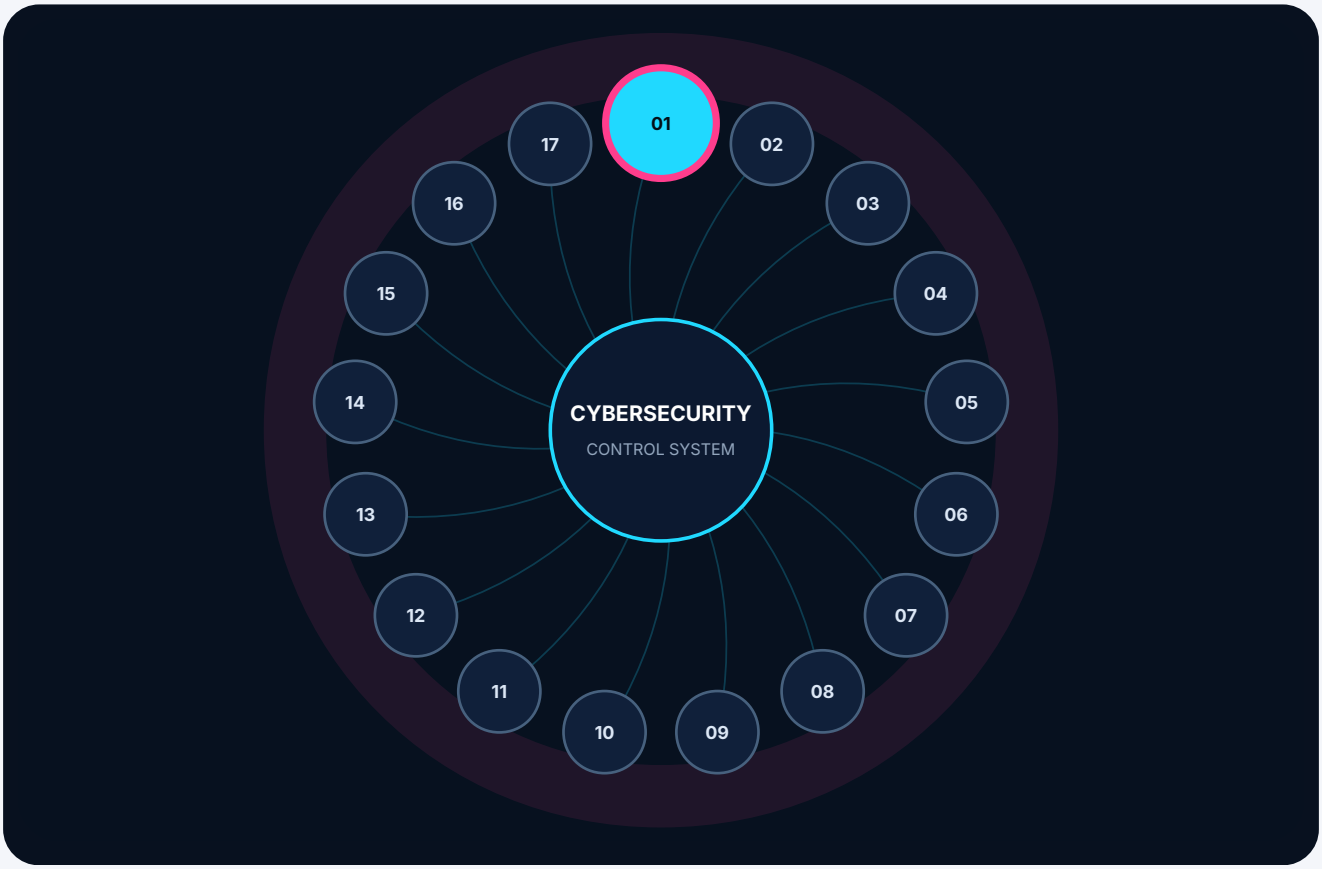
CLASSIFICATION
Public

7	6	4	1
ATOMIC CRITERIA	CAPABILITY FAMILIES	ASSESSMENT PROFILES	PERMANENT IDENTITY

Publication doctrine. This standard establishes durable requirements for its defined scope. Interpretation must preserve the permanent document identity, recorded evidence, and formal revision history.

DOMAIN CONTROL SYSTEM

MYTHOS-SEC-0001 inside the cybersecurity and network security standard constellation



Connected assurance

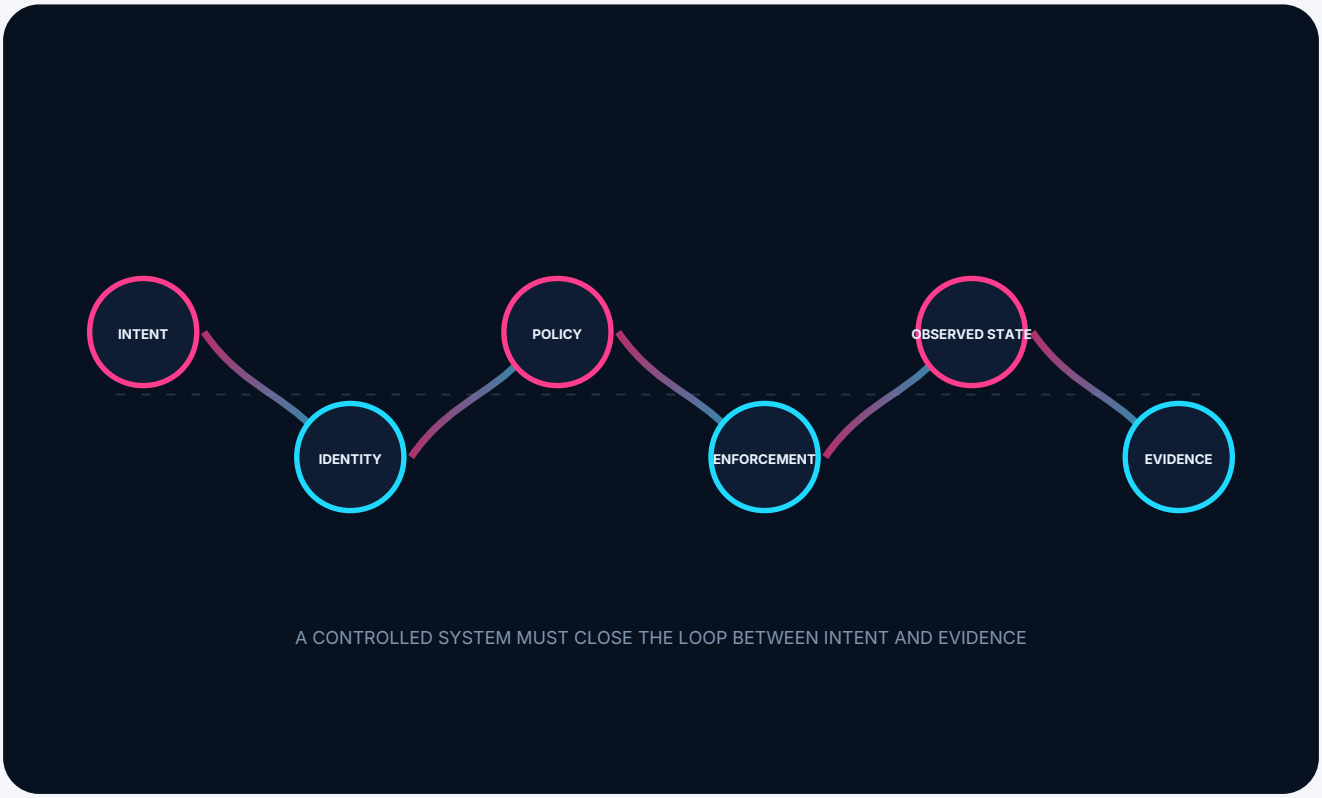
Architecture, policy, implementation, operations, and evidence are evaluated as one controlled system.

Specialization rule

Companion standards may add precision, but they cannot silently weaken this publication's requirements.

CLOSED-LOOP ARCHITECTURE

Intent becomes trustworthy only when observed state returns as evidence



State separation

Desired, approved, deployed, observed, historical, and simulated states must remain distinguishable.

Recoverable change

Material change requires validation, authorization, monitoring, containment, and a credible recovery path.

EVALUATION TOPOLOGY

The capability families and atomic criteria of MYTHOS-SEC-0001

Capability families

Families expose the major engineering surfaces and preserve the source weighting model.

Atomic criteria

Each criterion carries a question, maturity spectrum, evidence expectations, assessment method, and operational signals.

NAVIGATION

Contents

ENGINEERING DOCTRINE

0. Executive Mandate

Traditional evaluation of cryptographic security in the AI era is insufficient.

"Quantum-proof" is a marketing term. The reality is that Harvest Now, Decrypt Later (HNDL) attacks are actively exfiltrating encrypted data today, knowing that quantum computers will break RSA and ECC in the near future. Furthermore, the rapid advancement of AI has led to the proliferation of AI Bill of Materials (AIBOMs) and complex model supply chains where cryptographic integrity is entirely opaque.

This standard exists because:

1. **Hardcoded Cryptography is high-risk architectural constraint:** Systems that hardcode RSA or X25519 into their application logic will require multi-year, architecture-breaking migrations when those algorithms are deprecated. Cryptographic agility - the ability to swap algorithms via configuration without rewriting code - is a mandatory prerequisite for production survival.
2. **PQC is a Migration, Not a Switch:** Post-Quantum Cryptography (PQC) algorithms (ML-KEM, ML-DSA) are new and lack the decades of cryptanalysis that classical algorithms have. Deploying them in isolation is a risk. Production systems MUST implement hybrid classical + PQC modes.
3. **Cryptographic Inventory is Missing:** Organizations do not know where their cryptography is. AI models, weights, container images, and execution environments contain thousands of transitive dependencies with unknown cryptographic primitives. A cryptographic Bill of Materials (CBOM/AIBOM) is required for governance.
4. **AI Supply Chains are Unverified:** Model weights and agent skills are downloaded and executed with minimal cryptographic verification. A poisoned model weight file can backdoor an entire infrastructure. PQC signatures (ML-DSA) must be used to verify AI artifacts.

This document establishes the **Mythos Post-Quantum & Crypto-Agility Standard (MPQCAS)**, a comprehensive, evidence-based methodology for evaluating cryptographic systems against quantum threats, agility requirements, and supply chain integrity.

ENGINEERING DOCTRINE

Part I. Scope and Applicability

1.1 In Scope

This standard covers the evaluation of:

- Post-Quantum Cryptography (PQC) algorithms (ML-KEM/ML-DSA, SLH-DSA)
- Hybrid classical + PQC key exchange and signatures
- Cryptographic agility (algorithm registries, rotation, migration)
- Cryptographic inventory (CBOM/AIBOM)
- Hardware-backed roots of trust (TPM, TEE, HSM)
- PQC in AI supply chains (signed model weights, verified inferences)
- Air-gapped and sovereign crypto deployment

1.2 Out of Scope

- General network security architecture (covered in MYTHOS-NET-0004)
- Zero-trust policy enforcement (covered in MYTHOS-SEC-0003)

1.3 Audience

- Security engineers and architects designing crypto-agile infrastructure
- Platform engineering teams managing TLS/IPsec fabrics
- AI governance, risk, and compliance teams
- Standards bodies seeking a reference PQC methodology

ENGINEERING DOCTRINE

Part II. Definitions and Taxonomy

2.1 Cryptographic Dimensions

Dimension	Definition
PQC	Post-Quantum Cryptography. Algorithms resistant to Shor's algorithm (e.g., ML-KEM, ML-DSA).
Crypto-Agility	The ability to swap cryptographic primitives (e.g., X25519 to ML-KEM) via configuration without code changes.
HNDL	Harvest Now, Decrypt Later. The practice of exfiltrating encrypted data now to decrypt it when quantum computers mature.
Hybrid Mode	The simultaneous use of a classical algorithm and a PQC algorithm, requiring both to be broken to compromise the system.
AIBOM	AI Bill of Materials. An inventory of cryptographic assets, model weights, and dependencies.

2.2 The PQC Doctrine

> Quantum-proof is marketing. Crypto-agility is architecture. A model that cannot rotate its signatures is a liability. A weight that is not signed with PQC is a backdoor.

ENGINEERING DOCTRINE

Part III. Evaluation Methodology

3.1 Scoring Model

Each capability is scored from 0 to 5.

Score	Meaning
0	Fails basic task; hardcoded classical crypto
1	Basic PQC support but hardcoded
2	Functional but lacks hybrid or agility support
3	Solid production performance; hybrid PQC, basic agility
4	Strong performance; full agility, AIBOM, hardware roots
5	Best-in-class; sets the standard for PQC and agility

Weighting

Category	Weight	Rationale
PQC Enforcement & NIST Compliance	25%	ML-KEM/ML-DSA mandatory for production
Crypto-Agility	20%	Hardcoded crypto is un-migratable
Hybrid Mode & Rollback	15%	PQC in isolation is a cryptanalysis risk
Cryptographic Inventory (AIBOM)	15%	Unknown crypto cannot be governed
Hardware-Backed Roots	10%	Software crypto is exfiltratable
AI Supply Chain Integrity	10%	Unsigned models are an attack surface
Operational Lifecycle	5%	Crypto must be governed like software

Total: 100%

A system MUST score at least 3.0 in PQC Enforcement & NIST Compliance to be considered for production use.

EVALUATION AND ASSURANCE SYSTEM

Capability claims are bounded by evidence, context, and reproducible assessment.

7 atomic criteria across 6 capability families define the evaluation surface of this standard.

4.1 / CAPABILITY FAMILY

PQC Enforcement and NIST Compliance

SOURCE WEIGHT 25%

4.1.1
Algorithm Standardization

4.1.2
Migration Triggers

MYTHOS-SEC-0001-EVAL-4.1.1

Algorithm Standardization

FAMILY	SOURCE REFERENCE	WEIGHT CONTEXT	ASSESSMENT POSTURE
PQC Enforcement and NIST Compliance	**4.1.1**	**25%**	**Evidence-led**

Does the system use NIST-standardized PQC algorithms?

0
Uses deprecated or custom PQC algorithms

1
Uses early PQC candidates (Kyber/ Dilithium) not finalized

2
Uses NIST FIPS 203 (ML-KEM) but not FIPS 204 (ML-DSA)

3
Uses ML-KEM and ML-DSA

4
Uses ML-KEM, ML-DSA, and SLH-DSA for stateless hash-based signatures

5
Full NIST FIPS 203/204/205 compliance; verified by cryptographic evaluation suite

ENGINEERING INTERPRETATION

This criterion evaluates whether algorithm standardization is governed as an operating capability rather than a one-time configuration. Assessment must distinguish intended design, approved implementation, observed behavior, historical evidence, and unresolved risk.

REQUIRED EVIDENCE

- approved architecture or policy record
- current configuration or platform export
- change and exception records
- monitoring, test, or assessment evidence

ASSESSMENT PROCEDURE

1. Examine authoritative design, policy, configuration, and lifecycle records.
2. Interview the accountable owner and operators responsible for the control.
3. Test a representative positive, negative, failure, and recovery scenario.

EXAMINE - INTERVIEW - TEST

COMMON FAILURE PATTERNS

- The control exists only in diagrams or policy text.
- Observed state differs from approved intent without a governed exception.
- Evidence cannot establish scope, time, owner, or operating effectiveness.

OPERATIONAL MEASURES

- coverage of in-scope assets or flows
- age and closure rate of unresolved findings
- percentage of changes passing pre-deployment validation
- time to detect and contain control failure

DECISION BOUNDARY

A maturity score is valid only for the assessed scope and evidence period. Documentation alone does not establish operating effectiveness.

MYTHOS-SEC-0001-EVAL-4.1.2

Migration Triggers

FAMILY	SOURCE REFERENCE	WEIGHT CONTEXT	ASSESSMENT POSTURE
PQC Enforcement and NIST Compliance	4.1.2	25%	Evidence-led

Does the system automatically flag classical cryptography for migration?

0
No migration tracking

1
Manual inventory of classical crypto

2
Automated scanning for RSA/ECC

3
Automated scanning + risk scoring (HNDL exposure)

4
Automated migration triggers based on data retention and threat models

5
Leading migration governance: automated triggers, documented fallbacks, and continuous monitoring

ENGINEERING INTERPRETATION

This criterion evaluates whether migration triggers is governed as an operating capability rather than a one-time configuration. Assessment must distinguish intended design, approved implementation, observed behavior, historical evidence, and unresolved risk.

REQUIRED EVIDENCE

- cryptographic inventory, algorithm registry, key records, certificate data, and compatibility tests
- approved architecture or policy record
- current configuration or platform export

ASSESSMENT PROCEDURE

1. test rotation, hybrid negotiation, rollback, revocation, and algorithm-policy enforcement
2. Examine authoritative design, policy, configuration, and lifecycle records.

EXAMINE - INTERVIEW - TEST

COMMON FAILURE PATTERNS

- hardcoded algorithms, unknown dependencies, missing rollback, and unverifiable keys
- The control exists only in diagrams or policy text.

OPERATIONAL MEASURES

- inventory coverage
- deprecated algorithm count
- rotation success rate
- coverage of in-scope assets or flows

DECISION BOUNDARY

A maturity score is valid only for the assessed scope and evidence period. Documentation alone does not establish operating effectiveness.

4.2 / CAPABILITY FAMILY

Crypto-Agility

SOURCE WEIGHT 20%

4.2.1
Algorithm Registry

MYTHOS-SEC-0001-EVAL-4.2.1

Algorithm Registry

FAMILY	SOURCE REFERENCE	WEIGHT CONTEXT	ASSESSMENT POSTURE
Crypto-Agility	4.2.1	20%	Evidence-led

Can algorithms be swapped via configuration without code changes?

0
Algorithms hardcoded in application logic

1
Config files exist but require restarts and manual validation

2
Dynamic algorithm selection but limited to classical primitives

3
Versioned algorithm registry supporting PQC primitives

4
Dynamic algorithm rotation without service restart

5
Leading agility: versioned registry, zero-downtime rotation, automated compatibility testing

ENGINEERING INTERPRETATION

This criterion evaluates whether algorithm registry is governed as an operating capability rather than a one-time configuration. Assessment must distinguish intended design, approved implementation, observed behavior, historical evidence, and unresolved risk.

REQUIRED EVIDENCE

- cryptographic inventory, algorithm registry, key records, certificate data, and compatibility tests
- approved architecture or policy record
- current configuration or platform export

ASSESSMENT PROCEDURE

1. test rotation, hybrid negotiation, rollback, revocation, and algorithm-policy enforcement
2. Examine authoritative design, policy, configuration, and lifecycle records.

EXAMINE - INTERVIEW - TEST

COMMON FAILURE PATTERNS

- hardcoded algorithms, unknown dependencies, missing rollback, and unverifiable keys
- The control exists only in diagrams or policy text.

OPERATIONAL MEASURES

- inventory coverage
- deprecated algorithm count
- rotation success rate
- coverage of in-scope assets or flows

DECISION BOUNDARY

A maturity score is valid only for the assessed scope and evidence period. Documentation alone does not establish operating effectiveness.

4.3 / CAPABILITY FAMILY

Hybrid Mode and Rollback

SOURCE WEIGHT 15%

4.3.1
Hybrid Key Exchange

MYTHOS-SEC-0001-EVAL-4.3.1

Hybrid Key Exchange

FAMILY	SOURCE REFERENCE	WEIGHT CONTEXT	ASSESSMENT POSTURE
Hybrid Mode and Rollback	4.3.1	15%	Evidence-led

Does the system support hybrid classical + PQC key establishment?

0
No hybrid support

1
Hybrid support but hardcoded ratios

2
Configurable hybrid (e.g., X25519 + ML-KEM-768)

3
Full hybrid support with automated fallback to classical if PQC fails

4
Cryptographically bound hybrid (both keys must be broken)

5
Leading hybrid governance: formal verification of binding, automated rollback, and policy-driven mode selection

ENGINEERING INTERPRETATION

This criterion evaluates whether hybrid key exchange is governed as an operating capability rather than a one-time configuration. Assessment must distinguish intended design, approved implementation, observed behavior, historical evidence, and unresolved risk.

REQUIRED EVIDENCE

- approved architecture or policy record
- current configuration or platform export
- change and exception records
- monitoring, test, or assessment evidence

ASSESSMENT PROCEDURE

1. Examine authoritative design, policy, configuration, and lifecycle records.
2. Interview the accountable owner and operators responsible for the control.
3. Test a representative positive, negative, failure, and recovery scenario.

EXAMINE - INTERVIEW - TEST

COMMON FAILURE PATTERNS

- The control exists only in diagrams or policy text.
- Observed state differs from approved intent without a governed exception.
- Evidence cannot establish scope, time, owner, or operating effectiveness.

OPERATIONAL MEASURES

- coverage of in-scope assets or flows
- age and closure rate of unresolved findings
- percentage of changes passing pre-deployment validation
- time to detect and contain control failure

DECISION BOUNDARY

A maturity score is valid only for the assessed scope and evidence period. Documentation alone does not establish operating effectiveness.

4.4 / CAPABILITY FAMILY

Cryptographic Inventory (AIBOM)

SOURCE WEIGHT 15%

4.4.1
CBOM/AIBOM Generation

MYTHOS-SEC-0001-EVAL-4.4.1

CBOM/AIBOM Generation

FAMILY	SOURCE REFERENCE	WEIGHT CONTEXT	ASSESSMENT POSTURE
Cryptographic Inventory (AIBOM)	4.4.1	15%	Evidence-led

Does the system generate a cryptographic Bill of Materials?

0
No inventory

1
Manual inventory of top-level crypto

2
Automated scanning of direct dependencies

3
Automated CBOM generation including transitive dependencies

4
CBOM includes AI weights, model identities, and inference signatures

5
Leading AIBOM: automated, signed, transparency-logged, and continuously monitored

ENGINEERING INTERPRETATION

This criterion evaluates whether cbom/aibom generation is governed as an operating capability rather than a one-time configuration. Assessment must distinguish intended design, approved implementation, observed behavior, historical evidence, and unresolved risk.

REQUIRED EVIDENCE

- cryptographic inventory, algorithm registry, key records, certificate data, and compatibility tests
- approved architecture or policy record
- current configuration or platform export

ASSESSMENT PROCEDURE

1. test rotation, hybrid negotiation, rollback, revocation, and algorithm-policy enforcement
2. Examine authoritative design, policy, configuration, and lifecycle records.

EXAMINE - INTERVIEW - TEST

COMMON FAILURE PATTERNS

- hardcoded algorithms, unknown dependencies, missing rollback, and unverifiable keys
- The control exists only in diagrams or policy text.

OPERATIONAL MEASURES

- inventory coverage
- deprecated algorithm count
- rotation success rate
- coverage of in-scope assets or flows

DECISION BOUNDARY

A maturity score is valid only for the assessed scope and evidence period. Documentation alone does not establish operating effectiveness.

4.5 / CAPABILITY FAMILY

Hardware-Backed Roots

SOURCE WEIGHT 10%

4.5.1
TEE/TPM/HSM Integration

MYTHOS-SEC-0001-EVAL-4.5.1

TEE/TPM/HSM Integration

FAMILY	SOURCE REFERENCE	WEIGHT CONTEXT	ASSESSMENT POSTURE
Hardware-Backed Roots	4.5.1	10%	Evidence-led

Are PQC keys protected by hardware roots of trust?

0
No hardware integration

1
Basic TPM integration for classical keys

2
HSM support but no PQC integration

3
TPM/TEE integration for PQC keys

4
Remote attestation of PQC keys

5
Leading hardware governance: TEE-protected PQC, remote attestation, and automated key lifecycle

ENGINEERING INTERPRETATION

This criterion evaluates whether tee/tpm/hsm integration is governed as an operating capability rather than a one-time configuration. Assessment must distinguish intended design, approved implementation, observed behavior, historical evidence, and unresolved risk.

REQUIRED EVIDENCE

- approved architecture or policy record
- current configuration or platform export
- change and exception records
- monitoring, test, or assessment evidence

ASSESSMENT PROCEDURE

1. Examine authoritative design, policy, configuration, and lifecycle records.
2. Interview the accountable owner and operators responsible for the control.
3. Test a representative positive, negative, failure, and recovery scenario.

EXAMINE - INTERVIEW - TEST

COMMON FAILURE PATTERNS

- The control exists only in diagrams or policy text.
- Observed state differs from approved intent without a governed exception.
- Evidence cannot establish scope, time, owner, or operating effectiveness.

OPERATIONAL MEASURES

- coverage of in-scope assets or flows
- age and closure rate of unresolved findings
- percentage of changes passing pre-deployment validation
- time to detect and contain control failure

DECISION BOUNDARY

A maturity score is valid only for the assessed scope and evidence period. Documentation alone does not establish operating effectiveness.

4.6 / CAPABILITY FAMILY

AI Supply Chain Integrity

SOURCE WEIGHT 10%

4.6.1
Model Weight Signing

MYTHOS-SEC-0001-EVAL-4.6.1

Model Weight Signing

FAMILY	SOURCE REFERENCE	WEIGHT CONTEXT	ASSESSMENT POSTURE
AI Supply Chain Integrity	4.6.1	10%	Evidence-led

Are AI model weights and artifacts signed with PQC signatures?

0
No signing

1
Classical signatures (Ed25519)

2
PQC signatures but not verified at load time

3
PQC signatures (ML-DSA) verified at load time

4
PQC signatures + transparency log (Rekor)

5
Leading integrity: PQC signatures, transparency log, and remote attestation

ENGINEERING INTERPRETATION

This criterion evaluates whether model weight signing is governed as an operating capability rather than a one-time configuration. Assessment must distinguish intended design, approved implementation, observed behavior, historical evidence, and unresolved risk.

REQUIRED EVIDENCE

- approved architecture or policy record
- current configuration or platform export
- change and exception records
- monitoring, test, or assessment evidence

ASSESSMENT PROCEDURE

1. Examine authoritative design, policy, configuration, and lifecycle records.
2. Interview the accountable owner and operators responsible for the control.
3. Test a representative positive, negative, failure, and recovery scenario.

EXAMINE - INTERVIEW - TEST

COMMON FAILURE PATTERNS

- The control exists only in diagrams or policy text.
- Observed state differs from approved intent without a governed exception.
- Evidence cannot establish scope, time, owner, or operating effectiveness.

OPERATIONAL MEASURES

- coverage of in-scope assets or flows
- age and closure rate of unresolved findings
- percentage of changes passing pre-deployment validation
- time to detect and contain control failure

DECISION BOUNDARY

A maturity score is valid only for the assessed scope and evidence period. Documentation alone does not establish operating effectiveness.

LIFECYCLE AND ASSURANCE

Part V. The Mythos PQC Suite (MPQCS)

Traditional crypto benchmarks measure speed. The MPQCS measures agility, PQC enforcement, and supply chain integrity.

5.1 Suite Composition

5.1.1 MPQCS-Agility

- **Algorithm Rotation:** 100+ tests verifying zero-downtime rotation between classical and PQC algorithms.
- **Downgrade Resistance:** 50+ tests verifying the system rejects forced classical downgrades.

5.1.2 MPQCS-SupplyChain

- **Weight Verification:** 100+ tests verifying ML-DSA signatures on model weights before load.
- **AIBOM Completeness:** 50+ tests verifying transitive dependencies are inventoried.

5.2 Execution Protocol

PUBLICATION BOUNDARY

Candidate standard. Permanent identity. Evidence before authority.

Approval requires designated technical, security, legal, accessibility, and governance review with recorded findings and dispositions.