CANDIDATE STANDARD

Mythos Extension Ecosystem Standard

Govern extensions, plugins, publishers, provenance, admission, capabilities, isolation, updates, and revocation.

PERMANENT ID
MYTHOS-FND-0008

PUBLICATION CLASS
CANDIDATE STANDARD

VERSION / STATUS
1.0.0-candidate / CANDIDATE

PERMANENT PUBLICATION IDENTITY

Mythos Extension Ecosystem Standard

Universal Requirements for Plugins, Connectors, Skills, Packages, Integrations, Marketplaces, and Third-Party Execution

Document ID
MYTHOS-FND-0008

Version
1.0.0-candidate

Status
Candidate Standard

Review date
2027-09-17

Publication position
This is a permanent candidate standard in the Mythos Engineering Standards Library. Candidate status means the content is ready for structured implementation and review, but it is not represented as external certification, regulatory approval, or independent assurance.

PROFILE	CONTROLS	CADENCE	EVIDENCE
3 LEVELS	18	TRIGGERED	ASSESSABLE
Foundational / Advanced / High Assurance	Atomic normative controls	Annual plus material-change review	Examine / Interview / Test / Measure

Reader orientation

Dimension	Engineering position
Primary domain	Foundation and Governance
Audience	Platform and ecosystem architects; Extension and connector developers; Security and supply-chain teams; Marketplace operators; Administrators and assessors
Publisher / owner	Mythos Systems / Standards Program
Public classification	Public technical standard
Canonical route	/library/standards/foundation/mythos-fnd-0008/

Expected outcomes

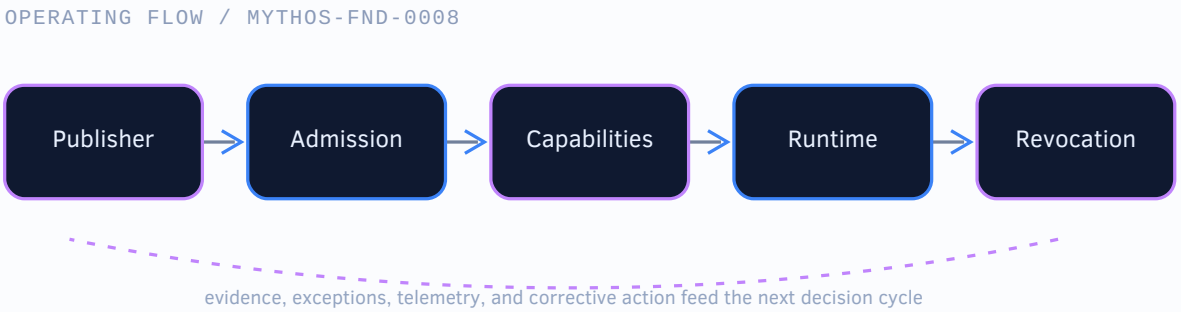
- Enable useful extensibility through explicit, least-privilege contracts.
- Constrain supply-chain, tenant-isolation, data-exfiltration, and persistence risks.
- Make extension behavior, provenance, authority, and lifecycle assessable.
- Support open ecosystems without requiring blind trust in publishers or marketplaces.

SOURCE / FRESHNESS POSITION

Authority and source posture

Validated 2026-09-17
Primary authority versions were revalidated for this regeneration on 2026-09-17. Current-source updates are reflected where a newer stable version was identified; active drafts are labeled as such and do not silently replace current final authorities.

FOUNDATION OPERATING DOCTRINE



The source lineage for this edition is the enterprise candidate source set produced in July 2026. Normative controls are preserved; editorial, visual, metadata, and authority-freshness changes are recorded as revision lineage rather than presented as new control substance.

NAVIGATION

Contents

The table of contents is page-aware and internally linked. Control-level navigation follows on the next pages.

NORMATIVE SYSTEM

Control index

Every control is independently addressable and assessable. Page references link directly to the control record.

Document Control

Field	Value
Document ID	MYTHOS-FND-0008
Standard	Extension Ecosystem
Version	1.0.0-candidate
Status	Candidate Standard
Classification	Public
Publisher	Mythos Systems
Program	Mythos Engineering Standards Program
Accountable Owner	Mythos Systems Standards Program
Technical Review	Required
Source and Citation Review	Required
Assessment Review	Required
Accessibility and Publication Review	Required
Supersedes	No published edition; evolves source draft 0.2.0
Next Review	2027-09-17 or earlier on trigger

Revision Record

Version	Date	Status	Material Change
1.0.0-candidate	2026-09-17	Candidate Standard	Permanent-publication regeneration: source-preserving editorial system, richer information design, current authority revalidation, stable public metadata, and release QA.
0.2.0	2026-07-18	Working Draft	Source control standard
1.0.0-candidate	2026-07-22	Candidate Standard	Enterprise report architecture, executive direction, target operating model, profiles, maturity, authority register, and source-preserving reconstruction

How to Use This Standard

Executive Reading Path

Read Part I, the target-state architecture in Part III, the profile table in Part V, and the assurance dashboard in Part VI.

Engineering Reading Path

Read Parts II through V, then use the normative controls in Part IV as implementation and design requirements.

Assessment Reading Path

Read the conformance requirements in Part II, every applicable control's evidence and assessment procedure in Part IV, and the assessment, maturity, confidence, and traceability provisions in Parts VI and VII.

Normative and Informative Content

Uppercase **MUST**, **MUST NOT**, **SHOULD**, **SHOULD NOT**, and **MAY** statements are normative when used under the requirements-language provisions of this document. Executive findings, examples, implementation patterns, reference architectures, mappings, and external-authority descriptions are informative unless explicitly incorporated into an adopting organization's binding policy, contract, or regulatory obligation.

FOUNDATION STANDARD / STRUCTURAL PART

Part I – Executive Direction

1. Executive Overview

An extension ecosystem converts external code into part of the product trust boundary. Without explicit contracts, publisher identity, permission brokerage, isolation, update integrity, runtime evidence, and emergency revocation, extensions become an ambient-authority and software-supply-chain risk. This standard defines the controls required to support extensibility without surrendering platform integrity or user sovereignty.

The institutional objective is to govern extension identity, contracts, publisher trust, supply chain, permissions, isolation, data use, updates, runtime accountability, marketplace integrity, revocation, uninstall, and interoperability. Adoption should produce a controlled operating state in which leadership can understand the material risks, engineering teams can act on explicit requirements, assessors can test implementation and operating effectiveness, and the organization can support every conformance or trust claim with current evidence.

2. Executive Findings and Required Direction

Finding	Enterprise Exposure	Required Direction
Installation mistaken for authorization	Extensions often inherit broad access because a user installed them.	Separate installation, enablement, capability grants, and task-specific authorization.
Publisher and artifact ambiguity	Users cannot prove who produced the extension or whether it changed.	Require verified publisher identity, signing, provenance, and immutable artifact identity.
Weak isolation	Extensions execute inside the host process or unrestricted user context.	Use sandboxing, resource limits, brokered interfaces, and explicit egress.
Secret and data leakage	Extensions receive raw credentials or unrestricted workspace data.	Broker secret use and enforce declared data-purpose boundaries.
Revocation and uninstall gaps	Compromised or abandoned extensions remain active or leave orphaned authority.	Support emergency disablement, revocation, complete uninstall, and orphan handling.

3. Business and Operational Impact

3.1 Strategic Impact

This standard converts a discipline that is often dependent on individual expertise into an organization-wide system of ownership, records, controls, review, and evidence. It reduces decision ambiguity and makes material assumptions visible before they become embedded in products or operations.

3.2 Delivery and Cost Impact

Adoption requires investment in accountable roles, authoritative records, validation, tooling, and review. That cost should be measured against avoidable rework, delayed releases, incidents, regulatory exposure, duplicated platforms, failed integrations, and unsupported product claims.

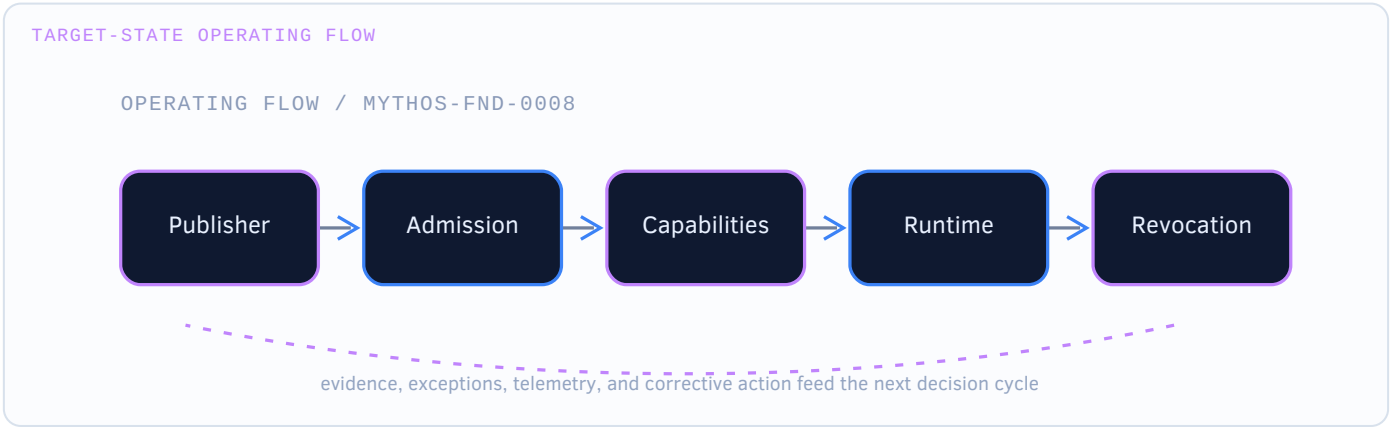
3.3 Security, Privacy, and Trust Impact

The standard requires security, privacy, integrity, resilience, and delegated authority to be considered within the primary operating model rather than as downstream approvals. This reduces the likelihood that unsafe boundaries become structurally expensive to correct.

3.4 Workforce and Organizational Impact

The organization must distinguish accountable ownership, implementation, approval, and independent challenge. Adoption may expose gaps in authority, skills, evidence, or cross-functional participation that require leadership action.

4. Target-State Summary



The target state contains the following institutional components:

#	Target-State Component
1	Extension classification and ownership
2	Versioned extension contract
3	Publisher and artifact identity
4	Build and dependency provenance
5	Admission and review
6	Least-privilege capability grants
7	Runtime isolation and resource control
8	Brokered secrets
9	Egress and external-service governance
10	Data-use boundaries
11	Secure update and rollback
12	Runtime accountability
13	Conformance and adversarial testing
14	Transparent listing and ranking

#	Target-State Component
15	Emergency disablement and revocation
16	Uninstall and orphan handling
17	Incident coordination
18	Interoperability and exit

```
Enterprise obligations and risk appetite
    ↓
Accountable ownership and governance
    ↓
Versioned policies, contracts, and authoritative records
    ↓
Engineering implementation and automated enforcement
    ↓
Operational telemetry, evidence, and exception handling
    ↓
Independent assessment and leadership review
    ↓
Corrective action, controlled change, and continuous improvement
```

5. Leadership Responsibilities

Role	Accountability
Platform owner	Owns extension trust model and enforcement boundary.
Ecosystem governance lead	Owns admission, listing, ranking, incident, and publisher policy.
Extension publisher	Owns code, dependencies, disclosures, support, and security response.
Security reviewer	Reviews threat model, permissions, isolation, and supply chain.
Runtime engineering	Implements sandbox, broker, quotas, events, and revocation.
Marketplace operations	Maintains listing integrity, complaints, and emergency communications.
User or enterprise administrator	Approves installation and scoped grants.
Independent assessor	Tests conformance and adversarial resistance.

Leadership must ensure that exceptions are explicit, risk-owned, time-bounded, monitored, and retired. A maturity score or successful audit sample does not replace accountability for known nonconformance or residual risk.

FOUNDATION STANDARD / STRUCTURAL PART

Part II – Standard Foundation

6. Purpose and Objectives

- Enable useful extensibility through explicit, least-privilege contracts.
- Constrain supply-chain, tenant-isolation, data-exfiltration, and persistence risks.
- Make extension behavior, provenance, authority, and lifecycle assessable.
- Support open ecosystems without requiring blind trust in publishers or marketplaces.

7. Scope

Applies to plugins, extensions, connectors, agents, skills, themes with executable behavior, packages, webhooks, drivers, providers, adapters, marketplace artifacts, and remotely hosted extension services.

8. Intended Audience

- Platform and ecosystem architects
- Extension and connector developers
- Security and supply-chain teams
- Marketplace operators
- Administrators and assessors

9. Requirements Language and Conformance

The key words **MUST**, **MUST NOT**, **SHOULD**, **SHOULD NOT**, and **MAY** are normative only when written in uppercase and are interpreted in accordance with RFC 2119 and RFC 8174.

A conformance claim MUST identify the assessed scope, standard version, selected assurance profile, tailoring decisions, evidence period, assessor, and unresolved findings. Profiles are cumulative unless a control explicitly states otherwise.

- **Foundational:** broadly applicable minimum controls.
- **Advanced:** stronger governance, automation, scale, and independent verification.
- **High Assurance:** continuous or independent validation, stronger isolation, adversarial testing, formal analysis, or cryptographic evidence where warranted.

10. Normative References from Source Draft

- **RFC 2119** — Key words for use in RFCs to Indicate Requirement Levels. https://www.rfc-editor.org/rfc/rfc2119
- **RFC 8174** — Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words. https://www.rfc-editor.org/rfc/rfc8174

- **MYTHOS-GOV-0001** — Mythos Engineering Standards Authoring and Benchmark Framework, Version 0.1.0. ../governance/01_MYTHOS_STANDARDS_AUTHORING_AND_BENCHMARK_FRAMEWORK.md

11. Informative References from Source Draft

- **NIST SP 800-161 Rev. 1 Update 1** — Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations. https://csrc.nist.gov/pubs/sp/800/161/r1/upd1/final
- **NIST SP 800-218 v1.1** — Secure Software Development Framework (SSDF). https://csrc.nist.gov/pubs/sp/800/218/final
- **SLSA 1.2** — Supply-chain Levels for Software Artifacts. https://slsa.dev/spec/v1.2/
- **SPDX 3.0** — Software Package Data Exchange specification. https://spdx.github.io/spdx-spec/v3.0/
- **CycloneDX 1.7** — OWASP software bill of materials standard. https://cyclonedx.org/specification/overview/
- **Sigstore** — Keyless signing and transparency-log ecosystem. https://docs.sigstore.dev/
- **NIST SP 800-53 Rev. 5, Release 5.2.0** — Security and Privacy Controls for Information Systems and Organizations. https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final

External mappings are informative unless explicitly incorporated into a contract or regulatory obligation. Adopted organizations remain responsible for validating current source versions and legal applicability.

12. Terms and Definitions

Term	Definition
Accountable owner	The person or formally delegated role that accepts responsibility for an outcome, decision, control, or risk.
Assessment object	The system, process, component, artifact, team, service, or organizational scope being evaluated.
Compensating control	An alternative safeguard that provides comparable risk reduction when the specified control cannot be implemented as written.
Conformance claim	A bounded statement that an identified scope satisfies the applicable requirements of a named standard version and assurance profile.
Evidence	Reviewable information that supports a conclusion about design, implementation, operation, or control effectiveness.
High Assurance	The cumulative profile requiring stronger independence, adversarial testing, continuous verification, or formal evidence where risk warrants it.
Residual risk	Risk remaining after controls, mitigations, and compensating measures are applied.
System	A product, service, application, platform, workflow, integration, operational capability, or combined socio-technical environment.
Tailoring	A documented decision to include, strengthen, parameterize, or mark a control not applicable based on scope and risk.
Extension	An independently developed artifact or service that augments a host system through a defined contract.
Capability grant	A scoped, explicit authorization allowing an extension to perform named operations on named resources.
Publisher identity	The verified human or organizational identity accountable for an extension release.
Revocation	The process of invalidating trust, distribution, execution, credentials, or permissions for an extension or publisher.

13. Applicability and Tailoring

The organization MUST determine applicability at the control level. A not-applicable decision MUST identify the assessed scope, factual basis, approver, review date, and any assumptions that would invalidate the decision. Tailoring may strengthen or parameterize a control; it MUST NOT silently weaken a MUST requirement. Compensating controls require documented equivalence of risk reduction.

FOUNDATION STANDARD / STRUCTURAL PART

Part III – Risk and Architecture

14. Enterprise Problem and Risk Landscape

The principal enterprise risks addressed by this standard include inconsistent ownership, undocumented authority, uncontrolled change, local optimization, evidence gaps, stale assumptions, supplier dependence, false assurance, and the inability to determine whether the operating system still matches its approved intent.

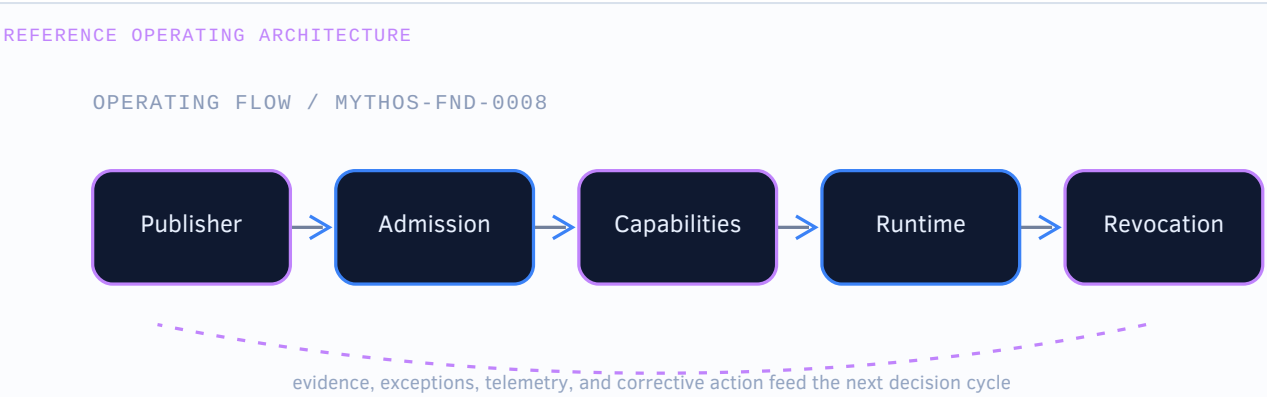
Adopting organizations SHOULD maintain a domain-specific risk register that identifies cause, affected asset or stakeholder, credible scenario, impact, existing controls, residual risk, owner, review trigger, and evidence. Risks that cross standards MUST be linked rather than copied into disconnected registers.

15. Governing Principles

- Extension code is untrusted until policy and evidence establish otherwise.
- Installation does not imply unrestricted authority.
- Capabilities are explicit, narrow, reviewable, and revocable.
- Provenance and update integrity are first-class requirements.
- The host enforces boundaries; extension self-restraint is not a control.
- Failure or removal of an extension must not strand the host in an unsafe state.

16. Reference Operating Architecture

REFERENCE OPERATING ARCHITECTURE



```
Enterprise obligations and risk appetite
    ↓
Accountable ownership and governance
    ↓
Versioned policies, contracts, and authoritative records
    ↓
Engineering implementation and automated enforcement
    ↓
Operational telemetry, evidence, and exception handling
    ↓
Independent assessment and leadership review
    ↓
Corrective action, controlled change, and continuous improvement
```

16.1 Control Plane

The control plane contains accountable ownership, policy, standards, risk decisions, approvals, exception governance, and authoritative state. It MUST be distinguishable from implementation and reporting systems.

16.2 Delivery and Enforcement Plane

The delivery plane contains engineering workflows, automation, validation, configuration, runtime enforcement, and lifecycle processes. Automated enforcement SHOULD be preferred where requirements can be expressed and tested safely.

16.3 Evidence and Assurance Plane

The assurance plane collects evidence, observations, test results, decisions, exceptions, and historical state. Evidence systems MUST protect integrity, scope, provenance, retention, and authorized access.

16.4 Feedback Plane

Metrics, incidents, assessments, user outcomes, exceptions, and changing authorities feed corrective action and controlled revision. Feedback MUST not silently alter normative requirements or accepted risk.

17. Roles and Accountability

Role	Accountability
Platform owner	Owns extension trust model and enforcement boundary.
Ecosystem governance lead	Owns admission, listing, ranking, incident, and publisher policy.
Extension publisher	Owns code, dependencies, disclosures, support, and security response.
Security reviewer	Reviews threat model, permissions, isolation, and supply chain.
Runtime engineering	Implements sandbox, broker, quotas, events, and revocation.
Marketplace operations	Maintains listing integrity, complaints, and emergency communications.
User or enterprise administrator	Approves installation and scoped grants.
Independent assessor	Tests conformance and adversarial resistance.

18. State, Evidence, and Decision Model

The adopting organization MUST distinguish:

- approved intent;
- current implemented state;
- observed operational state;
- generated or inferred recommendations;
- accepted exceptions;
- historical state;
- independently verified results.

A generated report, model conclusion, roadmap, or design proposal MUST NOT be represented as implemented or verified state without supporting evidence.

19. Security and Trust Considerations

Every implementation of this standard MUST apply identity, authorization, classification, least privilege, evidence integrity, sensitive-data handling, and supplier-risk controls appropriate to impact. Machine-generated guidance, automation, extensions, and delegated agents MUST remain subject to external policy and independent verification.

20. Failure Modes

Failure or Anti-Pattern	Enterprise Consequence
Loading third-party code directly into privileged host process	Failure can create hidden risk, misleading assurance, uncontrolled cost, or unsafe operation.
Granting all permissions at install time	Failure can create hidden risk, misleading assurance, uncontrolled cost, or unsafe operation.
Passing raw credentials to extensions	Failure can create hidden risk, misleading assurance, uncontrolled cost, or unsafe operation.
Allowing undeclared network egress	Failure can create hidden risk, misleading assurance, uncontrolled cost, or unsafe operation.
Ranking extensions through opaque paid influence	Failure can create hidden risk, misleading assurance, uncontrolled cost, or unsafe operation.
Updating without signature and rollback	Failure can create hidden risk, misleading assurance, uncontrolled cost, or unsafe operation.
Disabling UI while leaving background authority active	Failure can create hidden risk, misleading assurance, uncontrolled cost, or unsafe operation.

21. Cross-Functional Dependencies

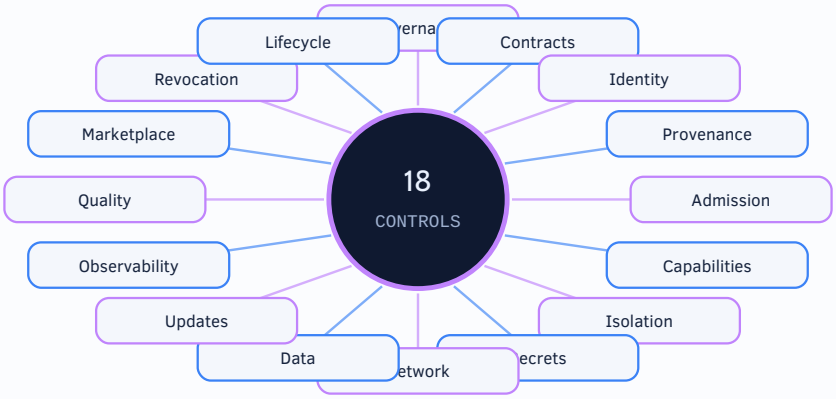
This Foundation standard depends on the remaining MYTHOS-FND standards for documentation, security and trust, quality, operations, data and integration, interfaces, extensions, AI-first behavior, and agentic orchestration. An adopting organization MUST resolve overlapping requirements through the stricter applicable control or a documented authority decision.

FOUNDATION STANDARD / STRUCTURAL PART

Part IV – Normative Control System

22. Control-Family Overview

CONTROL-FAMILY CONSTELLATION



This standard contains **18 controls** across the following families:

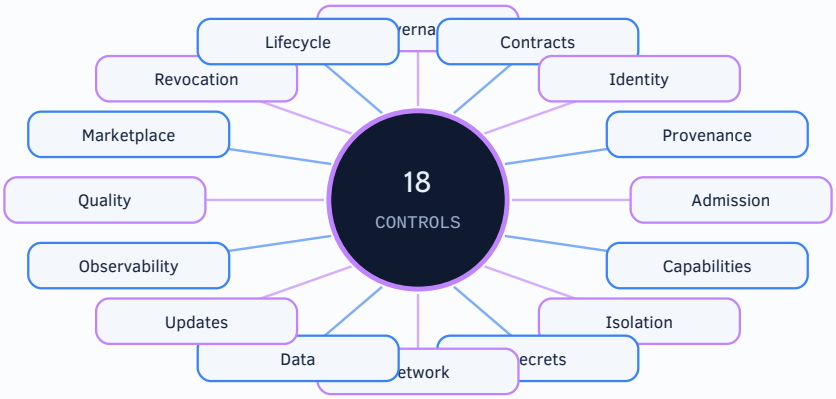
- Governance
- Contracts
- Identity
- Provenance
- Admission
- Capabilities
- Isolation
- Secrets
- Network
- Data
- Updates
- Observability
- Quality
- Marketplace
- Revocation
- Lifecycle
- Incident response
- Portability

23. Normative Controls

CONTROL SET	PROFILES	ASSESSMENT
18	3	4
atomic requirements	cumulative assurance levels	Examine / Interview / Test / Measure

Each control is independently addressable, evidence-bound, and assessable. The following control records preserve the source requirements while presenting implementation guidance, required evidence, assessment procedures, exceptions, compensating controls, and external mappings as a consistent engineering system.

NORMATIVE CONTROL CONSTELLATION



NORMATIVE CONTROL

MYTHOS-FND-EXT-01 – Extension classification and ownership

FAMILY	PROFILES	FAILURE IMPACT	AUTOMATION POTENTIAL
Governance	Foundational, Advanced, High Assurance	Critical	High

Requirement

The host organization MUST inventory extensions and classify them by execution location, publisher, data access, network access, privilege, persistence, update mechanism, tenant reach, and failure consequence.

Purpose

Provides the basis for risk-proportionate admission and monitoring.

Applicability

Applicable to all in-scope systems and organizational processes unless a documented tailoring decision states otherwise.

Implementation guidance

- Include remote SaaS connectors and non-code skills.
- Assign host and publisher owners.

Required evidence

- Extension inventory
- Risk classification
- Ownership records

Assessment procedure

- **Examine:** Compare runtime discoveries to inventory.
- **Interview:** Inspect unowned artifacts.
- **Test:** Exercise the requirement.

Exceptions and compensating controls

Any exception must be approved by an accountable owner, time-bounded, risk-assessed, monitored, and supported by compensating controls.

External mappings

- NIST SP 800-161 Rev. 1

NORMATIVE CONTROL

MYTHOS-FND-EXT-02 – Versioned extension contract

FAMILY	PROFILES	FAILURE IMPACT	AUTOMATION POTENTIAL
Contracts	Foundational, Advanced, High Assurance	Critical	High

Requirement

Extensions MUST use a versioned contract that defines lifecycle hooks, requested capabilities, data schemas, errors, resource limits, compatibility, update behavior, and termination semantics.

Purpose

Prevents undocumented coupling and unsafe behavior.

Applicability

Applicable to all in-scope systems and organizational processes unless a documented tailoring decision states otherwise.

Implementation guidance

- Use machine-readable manifests.
- Reject unknown mandatory fields or unsupported contract versions.

Required evidence

- Manifest schema
- Compatibility tests
- Contract registry

Assessment procedure

- **Examine:** Install incompatible and malformed manifests.
- **Interview:** Confirm ownership and practice.
- **Test:** Exercise the requirement.

Exceptions and compensating controls

Any exception must be approved by an accountable owner, time-bounded, risk-assessed, monitored, and supported by compensating controls.

External mappings

- JSON Schema 2020-12

NORMATIVE CONTROL

MYTHOS-FND-EXT-03 – Verified publisher and artifact identity

FAMILY	PROFILES	FAILURE IMPACT	AUTOMATION POTENTIAL
Identity	Advanced, High Assurance	Critical	High

Requirement

Executable extensions MUST be bound to a verified publisher identity and cryptographically identifiable release artifact before trusted distribution or execution.

Purpose

Creates accountability and resists substitution.

Applicability

Applicable to all in-scope systems and organizational processes unless a documented tailoring decision states otherwise.

Implementation guidance

- Separate publisher identity from signing keys.
- Support key rotation and recovery.

Required evidence

- Publisher records
- Signatures
- Transparency or release log

Assessment procedure

- **Examine:** Verify signature failure and key rotation.
- **Interview:** Confirm ownership and practice.
- **Test:** Exercise the requirement.

Exceptions and compensating controls

Any exception must be approved by an accountable owner, time-bounded, risk-assessed, monitored, and supported by compensating controls.

External mappings

- Sigstore
- SLSA 1.2

NORMATIVE CONTROL

MYTHOS-FND-EXT-04 – Build and dependency provenance

FAMILY	PROFILES	FAILURE IMPACT	AUTOMATION POTENTIAL
Provenance	Advanced, High Assurance	Critical	Partial

Requirement

Material extension releases MUST provide verifiable source, build, dependency, toolchain, and release provenance sufficient to evaluate origin and reproduce or independently validate the artifact where required by profile.

Purpose

Reduces supply-chain ambiguity.

Applicability

Applicable to all in-scope systems and organizational processes unless a documented tailoring decision states otherwise.

Implementation guidance

- Generate SBOMs.
- Pin dependencies and builders.

Required evidence

- Provenance attestations
- SBOM
- Build records

Assessment procedure

- **Examine:** Trace a binary to source and builder.
- **Interview:** Detect undeclared dependency.
- **Test:** Exercise the requirement.

Exceptions and compensating controls

Any exception must be approved by an accountable owner, time-bounded, risk-assessed, monitored, and supported by compensating controls.

External mappings

- SLSA 1.2
- SPDX 3.0
- CycloneDX 1.7

NORMATIVE CONTROL

MYTHOS-FND-EXT-05 – Risk-based admission and review

FAMILY	PROFILES	FAILURE IMPACT	AUTOMATION POTENTIAL
Admission	Foundational, Advanced, High Assurance	Critical	Partial

Requirement

The host MUST evaluate requested capabilities, code and dependency risk, data handling, publisher history, operational impact, legal obligations, and test evidence before admitting an extension to a trust tier.

Purpose

Prevents installation from becoming implicit approval.

Applicability

Applicable to all in-scope systems and organizational processes unless a documented tailoring decision states otherwise.

Implementation guidance

- Use automated analysis plus human review for material risk.
- Record reviewer conflicts.

Required evidence

- Review record
- Analysis results
- Admission decision

Assessment procedure

- **Examine:** Submit an overprivileged extension.
- **Interview:** Verify decision traceability.
- **Test:** Exercise the requirement.

Exceptions and compensating controls

Any exception must be approved by an accountable owner, time-bounded, risk-assessed, monitored, and supported by compensating controls.

External mappings

- NIST SP 800-161 Rev. 1

NORMATIVE CONTROL

MYTHOS-FND-EXT-06 – Explicit least-privilege grants

FAMILY	PROFILES	FAILURE IMPACT	AUTOMATION POTENTIAL
Capabilities	Foundational, Advanced, High Assurance	Critical	High

Requirement

Extensions MUST receive only explicit, resource-scoped, time- or context-bounded capabilities necessary for approved functions, and the host MUST deny undeclared operations by default.

Purpose

Limits blast radius.

Applicability

Applicable to all in-scope systems and organizational processes unless a documented tailoring decision states otherwise.

Implementation guidance

- Separate read, write, execute, administer, and delegate.
- Avoid ambient credentials.

Required evidence

- Capability manifest
- Grant records
- Negative tests

Assessment procedure

- **Examine:** Attempt undeclared filesystem, API, tenant, and network access.
- **Interview:** Confirm ownership and practice.
- **Test:** Exercise the requirement.

Exceptions and compensating controls

Any exception must be approved by an accountable owner, time-bounded, risk-assessed, monitored, and supported by compensating controls.

External mappings

- NIST SP 800-53 — AC-6

NORMATIVE CONTROL

MYTHOS-FND-EXT-07 – Runtime isolation and resource control

FAMILY	PROFILES	FAILURE IMPACT	AUTOMATION POTENTIAL
Isolation	Advanced, High Assurance	Critical	High

Requirement

Executable extensions MUST run within host-enforced isolation appropriate to risk, including process, memory, filesystem, network, tenant, secret, device, compute, and time limits.

Purpose

Contains malicious and defective behavior.

Applicability

Applicable to all in-scope systems and organizational processes unless a documented tailoring decision states otherwise.

Implementation guidance

- Use sandboxing or separate services.
- Terminate runaway work.

Required evidence

- Isolation architecture
- Resource policy
- Escape and exhaustion tests

Assessment procedure

- **Examine:** Attempt boundary escape and resource exhaustion.
- **Interview:** Confirm ownership and practice.
- **Test:** Exercise the requirement.

Exceptions and compensating controls

Any exception must be approved by an accountable owner, time-bounded, risk-assessed, monitored, and supported by compensating controls.

External mappings

- NIST SP 800-53 — SC-39

NORMATIVE CONTROL

MYTHOS-FND-EXT-08 – Brokered secret access

FAMILY	PROFILES	FAILURE IMPACT	AUTOMATION POTENTIAL
Secrets	Foundational, Advanced, High Assurance	Critical	High

Requirement

Extensions MUST NOT receive persistent raw secrets when a scoped brokered token, delegated operation, or just-in-time credential can satisfy the approved function.

Purpose

Reduces credential theft and reuse.

Applicability

Applicable to all in-scope systems and organizational processes unless a documented tailoring decision states otherwise.

Implementation guidance

- Bind tokens to audience, operation, tenant, and lifetime.
- Redact secrets from logs.

Required evidence

- Secret-flow design
- Token policy
- Tests

Assessment procedure

- **Examine:** Inspect environment and storage.
- **Interview:** Attempt token reuse out of scope.
- **Test:** Exercise the requirement.

Exceptions and compensating controls

Any exception must be approved by an accountable owner, time-bounded, risk-assessed, monitored, and supported by compensating controls.

External mappings

- NIST SP 800-53 — IA and SC families

NORMATIVE CONTROL

MYTHOS-FND-EXT-09 – Egress and external-service governance

FAMILY	PROFILES	FAILURE IMPACT	AUTOMATION POTENTIAL
Network	Advanced, High Assurance	Critical	High

Requirement

Extension network access MUST be explicitly declared, policy-enforced, observable, and restricted by destination, protocol, purpose, tenant, and data classification.

Purpose

Controls exfiltration and hidden dependencies.

Applicability

Applicable to all in-scope systems and organizational processes unless a documented tailoring decision states otherwise.

Implementation guidance

- Resolve dynamic services through approved brokers.
- Record DNS and destination evidence.

Required evidence

- Egress policy
- Destination inventory
- Network tests

Assessment procedure

- **Examine:** Attempt undeclared destinations and covert fallback.
- **Interview:** Confirm ownership and practice.
- **Test:** Exercise the requirement.

Exceptions and compensating controls

Any exception must be approved by an accountable owner, time-bounded, risk-assessed, monitored, and supported by compensating controls.

External mappings

- NIST SP 800-53 — SC-7

NORMATIVE CONTROL

MYTHOS-FND-EXT-10 – Extension data-use boundaries

FAMILY	PROFILES	FAILURE IMPACT	AUTOMATION POTENTIAL
Data	Foundational, Advanced, High Assurance	Critical	Partial

Requirement

Extensions MUST declare collection, access, transformation, retention, sharing, model use, telemetry, and deletion behavior, and the host MUST enforce applicable data and tenant boundaries.

Purpose

Prevents unauthorized secondary use.

Applicability

Applicable to all in-scope systems and organizational processes unless a documented tailoring decision states otherwise.

Implementation guidance

- Do not permit training on tenant data by default.
- Support deletion propagation.

Required evidence

- Data-use declaration
- Flow map
- Deletion evidence

Assessment procedure

- **Examine:** Trace sampled data.
- **Interview:** Test cross-tenant and post-uninstall access.
- **Test:** Exercise the requirement.

Exceptions and compensating controls

Any exception must be approved by an accountable owner, time-bounded, risk-assessed, monitored, and supported by compensating controls.

External mappings

- NIST Privacy Framework 1.0

NORMATIVE CONTROL

MYTHOS-FND-EXT-11 – Secure update and rollback

FAMILY	PROFILES	FAILURE IMPACT	AUTOMATION POTENTIAL
Updates	Foundational, Advanced, High Assurance	Critical	High

Requirement

Extension updates MUST be authenticated, integrity-verified, compatibility-tested, policy-reassessed when capabilities or behavior change, staged according to risk, and recoverable through rollback or safe disablement.

Purpose

Prevents update channels from bypassing initial trust decisions.

Applicability

Applicable to all in-scope systems and organizational processes unless a documented tailoring decision states otherwise.

Implementation guidance

- Treat new permissions as new consent.
- Block downgrade where unsafe.

Required evidence

- Update policy
- Signatures
- Staged rollout evidence

Assessment procedure

- **Examine:** Tamper with update.
- **Interview:** Change capabilities.
- **Test:** Test rollback.

Exceptions and compensating controls

Any exception must be approved by an accountable owner, time-bounded, risk-assessed, monitored, and supported by compensating controls.

External mappings

- SLSA 1.2

NORMATIVE CONTROL

MYTHOS-FND-EXT-12 – Runtime accountability

FAMILY	PROFILES	FAILURE IMPACT	AUTOMATION POTENTIAL
Observability	Advanced, High Assurance	Critical	High

Requirement

Material extension activity MUST produce attributable telemetry for invocation, actor, tenant, capability use, external calls, resource consumption, errors, policy denials, and consequential effects without unnecessary sensitive payloads.

Purpose

Supports detection and investigation.

Applicability

Applicable to all in-scope systems and organizational processes unless a documented tailoring decision states otherwise.

Implementation guidance

- Correlate host and extension traces.
- Monitor unexpected capability patterns.

Required evidence

- Telemetry schema
- Logs and traces
- Alert tests

Assessment procedure

- **Examine:** Reconstruct a sampled action.
- **Interview:** Trigger denied capability.
- **Test:** Exercise the requirement.

Exceptions and compensating controls

Any exception must be approved by an accountable owner, time-bounded, risk-assessed, monitored, and supported by compensating controls.

External mappings

- NIST SP 800-53 — AU family

NORMATIVE CONTROL

MYTHOS-FND-EXT-13 – Conformance and adversarial testing

FAMILY	PROFILES	FAILURE IMPACT	AUTOMATION POTENTIAL
Quality	Foundational, Advanced, High Assurance	Critical	Partial

Requirement

Extensions MUST pass contract, compatibility, authorization, isolation, malformed-input, resource-exhaustion, failure-recovery, upgrade, uninstall, and abuse tests proportionate to risk before release.

Purpose

Validates both cooperative and hostile behavior.

Applicability

Applicable to all in-scope systems and organizational processes unless a documented tailoring decision states otherwise.

Implementation guidance

- Provide a developer test kit.
- Use representative host versions.

Required evidence

- Test reports
- Fixtures
- Finding closure

Assessment procedure

- **Examine:** Reproduce a high-severity test.
- **Interview:** Submit malformed inputs.
- **Test:** Exercise the requirement.

Exceptions and compensating controls

Any exception must be approved by an accountable owner, time-bounded, risk-assessed, monitored, and supported by compensating controls.

External mappings

- NIST SSDF v1.1

NORMATIVE CONTROL

MYTHOS-FND-EXT-14 – Transparent listing and ranking

FAMILY	PROFILES	FAILURE IMPACT	AUTOMATION POTENTIAL
Marketplace	Foundational, Advanced, High Assurance	Material	Partial

Requirement

Extension catalogs MUST disclose publisher, ownership, permissions, data use, pricing, support, compatibility, security review status, known limitations, update history, and material ranking or sponsorship factors.

Purpose

Supports informed choice and prevents deceptive trust signals.

Applicability

Applicable to all in-scope systems and organizational processes unless a documented tailoring decision states otherwise.

Implementation guidance

- Distinguish verification from endorsement.
- Label sponsored placement.

Required evidence

- Listing schema
- Review records
- Ranking policy

Assessment procedure

- **Examine:** Compare listing to manifest and runtime behavior.
- **Interview:** Confirm ownership and practice.
- **Test:** Exercise the requirement.

Exceptions and compensating controls

Any exception must be approved by an accountable owner, time-bounded, risk-assessed, monitored, and supported by compensating controls.

External mappings

- NIST SP 800-161 Rev. 1

NORMATIVE CONTROL

MYTHOS-FND-EXT-15 – Emergency disablement and revocation

FAMILY	PROFILES	FAILURE IMPACT	AUTOMATION POTENTIAL
Revocation	Advanced, High Assurance	Critical	High

Requirement

The ecosystem MUST support rapid revocation of publisher credentials, releases, capability grants, distribution, and execution, with tested propagation, offline considerations, appeal, and evidence preservation.

Purpose

Contains compromised or harmful extensions.

Applicability

Applicable to all in-scope systems and organizational processes unless a documented tailoring decision states otherwise.

Implementation guidance

- Define severity-based service objectives.
- Support local emergency policy.

Required evidence

- Revocation plan
- Drill results
- Propagation telemetry

Assessment procedure

- **Examine:** Revoke an active test extension.
- **Interview:** Verify blocked execution and preserved evidence.
- **Test:** Exercise the requirement.

Exceptions and compensating controls

Any exception must be approved by an accountable owner, time-bounded, risk-assessed, monitored, and supported by compensating controls.

External mappings

- NIST SP 800-53 — IR and SI families

NORMATIVE CONTROL

MYTHOS-FND-EXT-16 – Disablement, uninstall, and orphan handling

FAMILY	PROFILES	FAILURE IMPACT	AUTOMATION POTENTIAL
Lifecycle	Foundational, Advanced, High Assurance	Critical	Partial

Requirement

Extensions MUST define safe disablement, uninstall, data export or deletion, dependent-resource handling, credential revocation, rollback, and orphan detection.

Purpose

Prevents unsafe residue and abandoned authority.

Applicability

Applicable to all in-scope systems and organizational processes unless a documented tailoring decision states otherwise.

Implementation guidance

- Preview destructive cleanup.
- Preserve shared data only with explicit ownership.

Required evidence

- Lifecycle contract
- Uninstall tests
- Orphan reports

Assessment procedure

- **Examine:** Remove extension during partial operation.
- **Interview:** Verify credentials and scheduled work are gone.
- **Test:** Exercise the requirement.

Exceptions and compensating controls

Any exception must be approved by an accountable owner, time-bounded, risk-assessed, monitored, and supported by compensating controls.

External mappings

- ISO/IEC/IEEE 15288:2023

NORMATIVE CONTROL

MYTHOS-FND-EXT-17 – Ecosystem incident coordination

FAMILY	PROFILES	FAILURE IMPACT	AUTOMATION POTENTIAL
Incident response	Advanced, High Assurance	Critical	Partial

Requirement

Hosts, marketplaces, and publishers MUST maintain coordinated processes for vulnerability intake, triage, notification, containment, evidence sharing, remediation, revocation, and post-incident review.

Purpose

Addresses multi-party incidents.

Applicability

Applicable to all in-scope systems and organizational processes unless a documented tailoring decision states otherwise.

Implementation guidance

- Define contact and disclosure channels.
- Protect reporters.

Required evidence

- Incident plan
- Contact registry
- Exercise results

Assessment procedure

- **Examine:** Run a compromised-release exercise.
- **Interview:** Confirm ownership and practice.
- **Test:** Exercise the requirement.

Exceptions and compensating controls

Any exception must be approved by an accountable owner, time-bounded, risk-assessed, monitored, and supported by compensating controls.

External mappings

- NIST SP 800-61 Rev. 3

NORMATIVE CONTROL

MYTHOS-FND-EXT-18 – Interoperability and exit

FAMILY	PROFILES	FAILURE IMPACT	AUTOMATION POTENTIAL
Portability	Advanced, High Assurance	Material	Partial

Requirement

Material extension contracts SHOULD support documented export, migration, replacement, and compatibility paths sufficient to avoid unsafe lock-in and abandoned data or workflows.

Purpose

Improves resilience and ecosystem competition.

Applicability

Applicable to all in-scope systems and organizational processes unless a documented tailoring decision states otherwise.

Implementation guidance

- Use open formats where practical.
- Document proprietary dependencies.

Required evidence

- Exit plan
- Export test
- Compatibility matrix

Assessment procedure

- **Examine:** Replace or disable a representative extension.
- **Interview:** Confirm ownership and practice.
- **Test:** Exercise the requirement.

Exceptions and compensating controls

Any exception must be approved by an accountable owner, time-bounded, risk-assessed, monitored, and supported by compensating controls.

External mappings

- ISO/IEC/IEEE 15288:2023

FOUNDATION STANDARD / STRUCTURAL PART

Part V – Implementation and Operations

24. Implementation Profiles

Profile	Required Operating State
Baseline	Extension manifest, stable contract, publisher identity, signing, admission, explicit permissions, sandboxing, secret brokerage, egress policy, update integrity, logging, disablement, and uninstall.
Enterprise	Managed allowlists, policy distribution, central review, provenance verification, risk-tiered isolation, tenant controls, automated conformance, incident coordination, and enterprise lifecycle reporting.
High Assurance	Reproducible builds, hardware-backed publisher identity, capability-secure runtime, microVM isolation, continuous behavioral monitoring, independent red teaming, signed transparency logs, and rapid global revocation.

Profiles are cumulative unless a control explicitly states otherwise. A higher profile cannot be claimed solely through additional tooling; governance, evidence, operating effectiveness, and independent challenge must also satisfy the profile.

25. Implementation Lifecycle

25.1 Establish

- appoint accountable ownership;
- determine applicability and profile;
- inventory current processes, systems, records, and known exceptions;
- identify authority sources and legal applicability;
- establish evidence locations and review cadence.

25.2 Baseline

- assess every applicable control;
- distinguish implemented, partially implemented, not implemented, not applicable, and not assessed;
- record evidence quality and confidence;
- identify systemic dependencies and priority risks.

25.3 Implement

- define target architecture and ownership;
- create or revise policies, contracts, workflows, and controls;
- automate enforcement and evidence where safe;
- test failure and recovery paths;
- train accountable roles.

25.4 Assure

- conduct technical and procedural assessment;
- verify evidence over a representative period;
- test sampled controls and critical workflows;
- challenge exceptions, unsupported claims, and optimistic assumptions.

25.5 Operate and Improve

- monitor metrics and exceptions;
- investigate incidents and control failures;
- update for authority, threat, technology, or organizational change;
- preserve superseded decisions and evidence;
- retire obsolete controls and implementations deliberately.

26. Integration Requirements

Implementations SHOULD integrate the standard with product governance, architecture review, secure development, CI/CD, change management, observability, service management, identity, evidence, risk, procurement, and training systems. Integration MUST preserve ownership and source authority rather than copying uncontrolled state between tools.

27. Failure Handling and Recovery

Control failures MUST produce a classified finding, owner, containment or compensating action, due date, evidence requirement, and escalation path. Where failure creates ongoing material risk, the organization MUST consider stopping, restricting, rolling back, isolating, or retiring the affected activity.

28. Exceptions and Compensating Controls

Exceptions MUST identify the exact control, scope, rationale, risk, owner, approval, compensating measures, monitoring, expiration, and closure evidence. Exceptions MUST NOT be used to convert a permanent design weakness into nominal conformance.

29. Prohibited Practices

- Loading third-party code directly into privileged host process
- Granting all permissions at install time
- Passing raw credentials to extensions
- Allowing undeclared network egress
- Ranking extensions through opaque paid influence
- Updating without signature and rollback
- Disabling UI while leaving background authority active

30. Adoption Roadmap from Source Draft

- Create extension inventory, contract schema, capability model, and publisher identity process.
- Require provenance, signing, dependency manifests, and pre-publication validation.
- Add runtime isolation, egress control, secrets brokering, and evidence collection.
- Establish marketplace governance, incident response, revocation, and transparent appeal.
- For High Assurance, add reproducible builds, independent review, deterministic policy evaluation, and continuous behavioral verification.

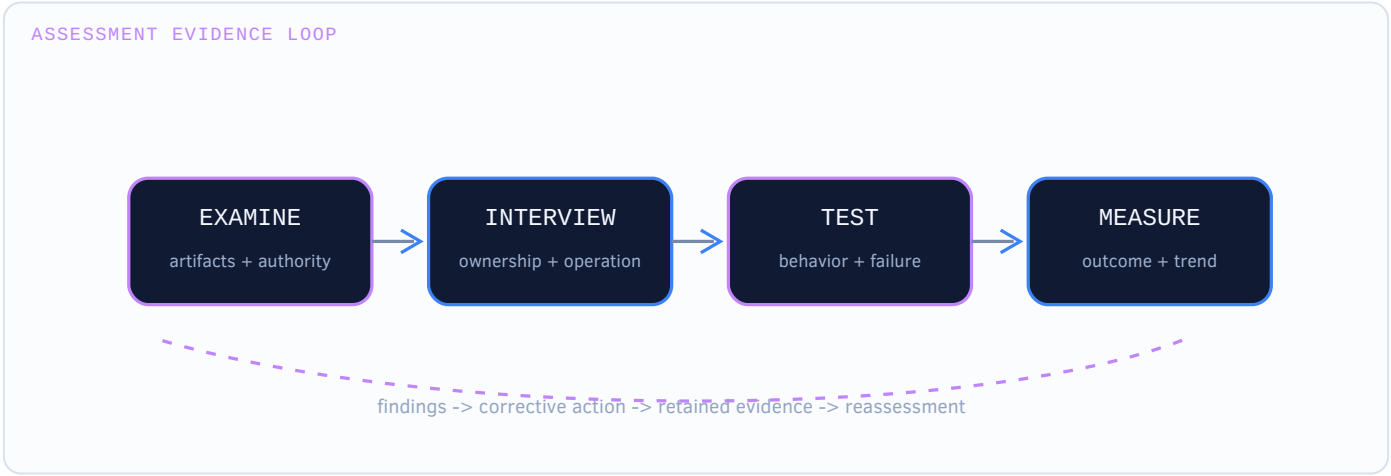
31. Limitations and Residual Risk from Source Draft

Conformance demonstrates that defined requirements were satisfied within a bounded scope and evidence period. It does not guarantee absence of defects, compromise, harm, outage, legal exposure, or future failure. Novel threats, misunderstood dependencies, invalid assumptions, human error, supplier changes, and conditions outside the assessment scope remain possible.

FOUNDATION STANDARD / STRUCTURAL PART

Part VI – Assurance and Assessment

32. Assessment Methodology



Assessors MUST use a combination of examination, interview, and testing appropriate to the selected profile and control risk. Assessment records MUST identify sample size, tools, versions, evidence references, exclusions, limitations, confidence, and residual uncertainty. Automated checks MAY support a finding but MUST NOT be treated as proof of effective governance or operation when the control depends on human accountability or contextual judgment.

12.1 Finding States

- **Satisfied:** requirement implemented and supported by sufficient evidence.
- **Partially satisfied:** some required outcomes or scope are missing.
- **Not satisfied:** requirement absent, ineffective, or contradicted by evidence.
- **Not applicable:** supported by an approved tailoring rationale.
- **Not assessed:** evidence is insufficient.

12.2 Conformance

A scope is **Conformant** only when all applicable MUST controls for the claimed profile are satisfied. A failed critical MUST control cannot be averaged away by stronger performance elsewhere.

33. Metrics and Reporting from Source Draft

Metric	Definition	Expected use or target
Signed release coverage	Installed executable extensions with verified publisher and artifact signatures	100% Advanced and High Assurance
Least-privilege review	Capability grants reviewed and justified	100% of material capabilities

Metric	Definition	Expected use or target
Revocation latency	Time from decision to prevented execution	Risk-based objective tested periodically
Known-vulnerability exposure	Installed artifacts exceeding remediation policy	0 without approved exception
Inventory completeness	Active, disabled, quarantined, and orphaned extensions represented	100%

Metrics MUST be interpreted with scope and uncertainty. Organizations SHOULD report trends, distributions, and exceptions rather than presenting a single composite score as complete assurance.

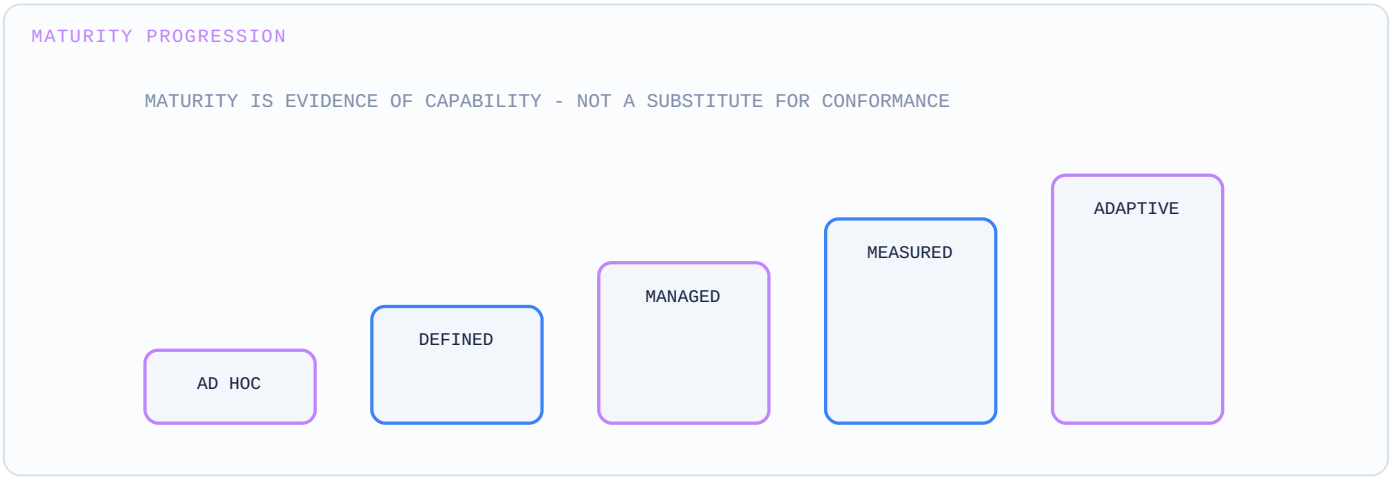
34. Exceptions and Compensating Controls

Every exception MUST identify the affected control and scope, justification, risk, compensating controls, accountable approver, start and expiration dates, monitoring, and remediation or retirement plan. Exceptions MUST be reevaluated after material change or incident and MUST NOT be self-approved by the team or agent requesting the exception where separation of duties is required.

35. Enterprise Metric Set

Metric	Measurement Requirement
extensions without verified publisher	Defined by the adopting organization with owner, source, target, and cadence.
requested versus granted capabilities	Defined by the adopting organization with owner, source, target, and cadence.
extensions with critical dependency findings	Defined by the adopting organization with owner, source, target, and cadence.
unsigned update attempts	Defined by the adopting organization with owner, source, target, and cadence.
sandbox violations	Defined by the adopting organization with owner, source, target, and cadence.
undeclared egress destinations	Defined by the adopting organization with owner, source, target, and cadence.
secrets exposed outside broker	Defined by the adopting organization with owner, source, target, and cadence.
revocation propagation time	Defined by the adopting organization with owner, source, target, and cadence.
orphaned data or permissions after uninstall	Defined by the adopting organization with owner, source, target, and cadence.

36. Maturity Model



Level	Name	Required Characteristics
M0	Unmanaged	Outcome is not intentionally controlled or evidence is unavailable.
M1	Documented	Ownership and procedures exist but implementation is inconsistent or mostly manual.
M2	Implemented	Applicable controls operate in the assessed scope and evidence exists.
M3	Measured	Effectiveness, exceptions, failures, and trends are measured and reviewed.
M4	Assured	Independent testing, representative evidence, and continuous or periodic validation exist.
M5	Adaptive	Controls respond safely to changing risk, authority, technology, and operational evidence.

Maturity does not override conformance. An organization cannot compensate for a failed mandatory requirement by assigning itself a high maturity level.

37. Assessment Confidence

Assessment confidence MUST be recorded as Low, Moderate, High, or Very High. Confidence considers evidence integrity, observation period, sample coverage, source authority, environmental representativeness, test repeatability, reviewer independence, and unresolved gaps.

38. Executive Assurance Dashboard

The executive report SHOULD present:

- applicable controls;
- conformant, partial, nonconformant, exception, not applicable, and not assessed counts;
- high and critical findings;
- evidence freshness;
- exception age;
- maturity distribution;
- assessment confidence;
- top residual risks;

- corrective-action status.

FOUNDATION STANDARD / STRUCTURAL PART

Part VII – Authority and Traceability

39. Cross-Standard Dependencies from Source Draft

This standard is part of an integrated foundation. Product decisions depend on documentation and traceability; implementation depends on security, quality, data, interfaces, and extension controls; release depends on operational readiness; AI and agentic behavior inherit every applicable non-AI requirement. A specialized standard MAY strengthen these requirements but MUST NOT weaken them without an explicit supersession rule.

40. Current External Authority Register

Authority	Relevance	Official Location	Status	Validated
NIST SP 800-218	Secure Software Development Framework 1.1	https://csrc.nist.gov/pubs/sp/800/218/final	Final 1.1; Rev. 1 draft active	2026-09-17
SLSA 1.2	Supply-chain Levels for Software Artifacts	https://slsa.dev/spec/v1.2/	Released	2026-09-17
in-toto Specification	Software supply-chain integrity metadata	https://github.com/in-toto/docs/blob/master/in-toto-spec.md	Published specification	2026-09-17
Sigstore Documentation	Artifact signing and transparency	https://docs.sigstore.dev/	Current	2026-09-17
SPDX 3.0	Software package data exchange	https://spdx.github.io/spdx-spec/v3.0/	Published	2026-09-17
CycloneDX 1.7	SBOM standard	https://cyclonedx.org/specification/overview/	Published	2026-09-17

The authority register is informative unless an adopting organization incorporates a source into a binding obligation. Legal applicability and licensed ISO content must be evaluated by qualified parties. The register records current source identity and relevance without reproducing protected standards text.

41. Control Traceability

Each control MUST remain traceable to:

- the risk or outcome it addresses;
- the applicable profile;
- implementation ownership;
- evidence;
- assessment procedure;
- exceptions;
- external mappings;
- related Foundation controls.

42. Source-Draft Preservation

This enterprise candidate edition preserves every normative control and the substantive source-draft sections. Editorial movement into the enterprise report structure does not remove the original requirement, implementation guidance, evidence, assessment procedure, exception rule, or external mapping.

FOUNDATION STANDARD / STRUCTURAL PART

Part VIII – Appendices

Appendix A – Source-Draft Evolution Notes

- Generalizes the source ecosystem model beyond any Mythos product.
- Separates marketplace policy from host-runtime enforcement.
- Adds explicit revocation, publisher accountability, data-use, and remote-service controls.

Appendix B – Change History

Version	Date	Status	Summary
0.2.0	2026-07-18	Working Draft	First standards-program restructuring of the source draft into atomic controls, assurance profiles, evidence, assessment procedures, and cross-standard dependencies.

Appendix C – Control Summary

Control	Family	Title	Profiles	Automation	Impact
MYTHOS-FND-EXT-01	Governance	Extension classification and ownership	Foundational, Advanced, High Assurance	High	Critical
MYTHOS-FND-EXT-02	Contracts	Versioned extension contract	Foundational, Advanced, High Assurance	High	Critical
MYTHOS-FND-EXT-03	Identity	Verified publisher and artifact identity	Advanced, High Assurance	High	Critical
MYTHOS-FND-EXT-04	Provenance	Build and dependency provenance	Advanced, High Assurance	Partial	Critical
MYTHOS-FND-EXT-05	Admission	Risk-based admission and review	Foundational, Advanced, High Assurance	Partial	Critical
MYTHOS-FND-EXT-06	Capabilities	Explicit least-privilege grants	Foundational, Advanced, High Assurance	High	Critical
MYTHOS-FND-EXT-07	Isolation	Runtime isolation and resource control	Advanced, High Assurance	High	Critical
MYTHOS-FND-EXT-08	Secrets	Brokered secret access	Foundational, Advanced, High Assurance	High	Critical
MYTHOS-FND-EXT-09	Network	Egress and external-service governance	Advanced, High Assurance	High	Critical
MYTHOS-FND-EXT-10	Data	Extension data-use boundaries	Foundational, Advanced, High Assurance	Partial	Critical
MYTHOS-FND-EXT-11	Updates	Secure update and rollback	Foundational, Advanced, High Assurance	High	Critical
	Observability	Runtime accountability	Advanced, High Assurance	High	Critical

Control	Family	Title	Profiles	Automation	Impact
MYTHOS-FND-EXT-12					
MYTHOS-FND-EXT-13	Quality	Conformance and adversarial testing	Foundational, Advanced, High Assurance	Partial	Critical
MYTHOS-FND-EXT-14	Marketplace	Transparent listing and ranking	Foundational, Advanced, High Assurance	Partial	Material
MYTHOS-FND-EXT-15	Revocation	Emergency disablement and revocation	Advanced, High Assurance	High	Critical
MYTHOS-FND-EXT-16	Lifecycle	Disablement, uninstall, and orphan handling	Foundational, Advanced, High Assurance	Partial	Critical
MYTHOS-FND-EXT-17	Incident response	Ecosystem incident coordination	Advanced, High Assurance	Partial	Critical
MYTHOS-FND-EXT-18	Portability	Interoperability and exit	Advanced, High Assurance	Partial	Material

Appendix D – Minimum Conformance Claim Record

```
standard: MYTHOS-FND-0008
version: 0.2.0
profile: foundational | advanced | high_assurance
scope: <bounded systems, teams, environments, and processes>
assessment_period: <start/end>
assessor: <person or independent body>
tailoring_decisions: []
exceptions: []
findings_summary:
  satisfied: 0
  partially_satisfied: 0
  not_satisfied: 0
  not_applicable: 0
  not_assessed: 0
residual_risk_owner: <accountable role>
approval: <record reference>
```

Appendix E – Publication Review Checklist

- [ ] Domain technical review completed
- [ ] Security and privacy review completed
- [ ] Current primary sources validated
- [ ] Exact external mappings reviewed
- [ ] All controls testable
- [ ] Evidence requirements sufficient
- [ ] Assessment procedures repeatable
- [ ] Executive findings supported
- [ ] Legal applicability reviewed where required
- [ ] Accessibility and publication quality verified
- [ ] Machine-readable control catalog validated

- [ ] Change and review record complete
- [ ] Formal approval recorded