CANDIDATE STANDARD

Foundation Standards Executive Synthesis

The institutional operating system for permanent Mythos engineering standards: authority, evidence, assessment, lifecycle, interfaces, AI, and agentic control.

PERMANENT ID
MYTHOS-FND-EXEC-0001

PUBLICATION CLASS
CANDIDATE STANDARD

VERSION / STATUS
1.0.0-candidate / CANDIDATE

EXECUTIVE SYNTHESIS

Foundation Standards

Permanent institutional doctrine inherited by the Mythos Engineering Standards Library.

Permanent ID
MYTHOS-FND-EXEC-0001

Version
1.0.0-candidate

Status
Candidate Executive Synthesis

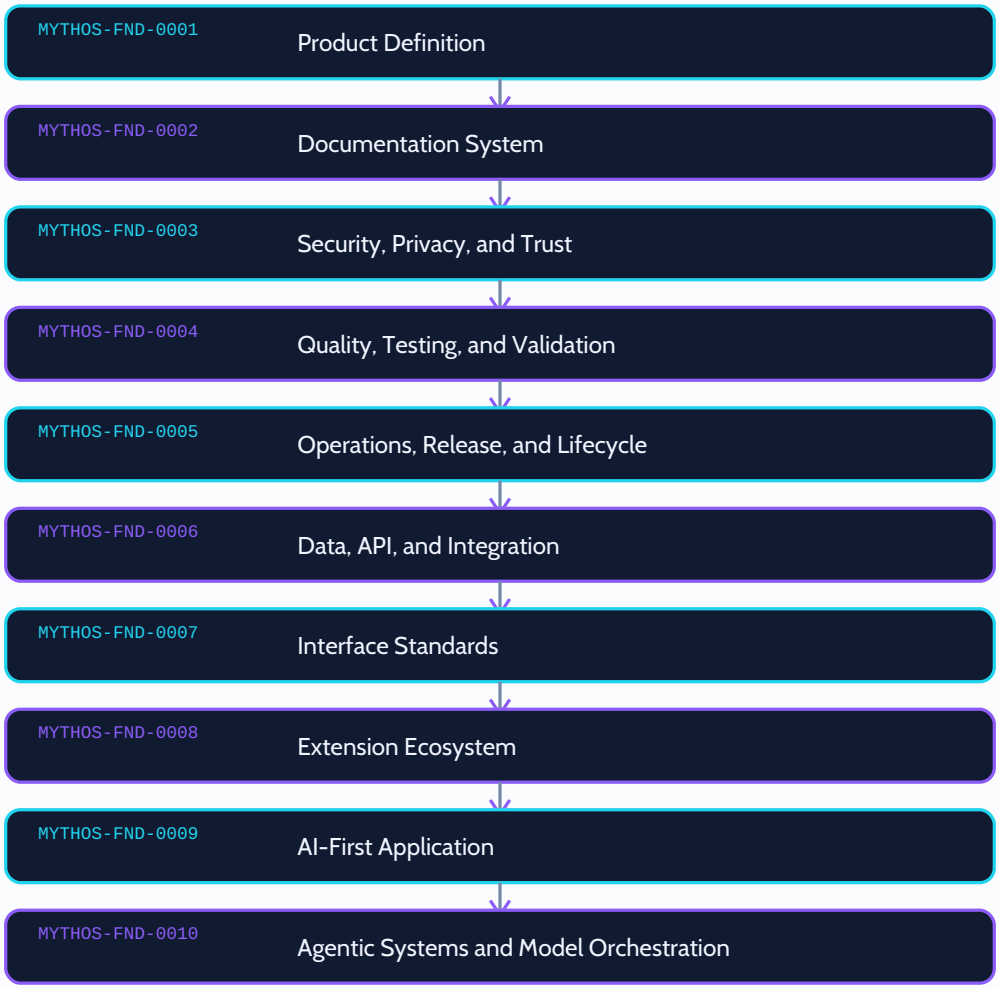
Validated
2026-09-17

STANDARDS	CONTROLS	PROFILES	METHODS
10	187	3	4
Permanent canonical publications	Normative controls	Foundational / Advanced / High Assurance	Examine / Interview / Test / Measure

Institutional purpose

The Foundation series defines how Mythos publications and adopting organizations convert intent into governed requirements, preserve authority and evidence, integrate trust, test outcomes, operate safely, manage data and interfaces, govern extensions, and constrain AI and agentic behavior. The standards are designed to operate as a connected system rather than ten isolated checklists.

FOUNDATION DEPENDENCY MODEL



The ten permanent standards

MYTHOS-FND-0001

Product Definition

Govern product intent before implementation: evidence, scope, requirements, invariants, risk, and objective acceptance.

16 controls / 48 pages

MYTHOS-FND-0002

Documentation System

Treat documentation as an engineered authority, evidence, traceability, and lifecycle system.

18 controls / 50 pages

MYTHOS-FND-0003

Security, Privacy, and Trust

Engineer security, privacy, and trust as system properties with explicit authority, isolation, evidence, and resilience.

19 controls / 58 pages

MYTHOS-FND-0004

Quality, Testing, and Validation

Turn requirements, hazards, and production behavior into reproducible verification and validation evidence.

19 controls / 52 pages

MYTHOS-FND-0005

Operations, Release, and Lifecycle

Govern readiness, release, operation, recovery, maintenance, deprecation, and retirement as one lifecycle.

18 controls / 51 pages

MYTHOS-FND-0006

Data, API, and Integration

Make data meaning, contracts, interfaces, events, lineage, reliability, and compatibility explicit and testable.

19 controls / 51 pages

MYTHOS-FND-0007

Interface Standards

Design human interfaces that preserve understanding, accessibility, authority, safety, feedback, and recovery.

18 controls / 50 pages

MYTHOS-FND-0008

Extension Ecosystem

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

18 controls / 50 pages

MYTHOS-FND-0009

AI-First Application

Govern material AI behavior through justified use, impact analysis, evaluation, grounding, human control, and lifecycle evidence.

19 controls / 51 pages

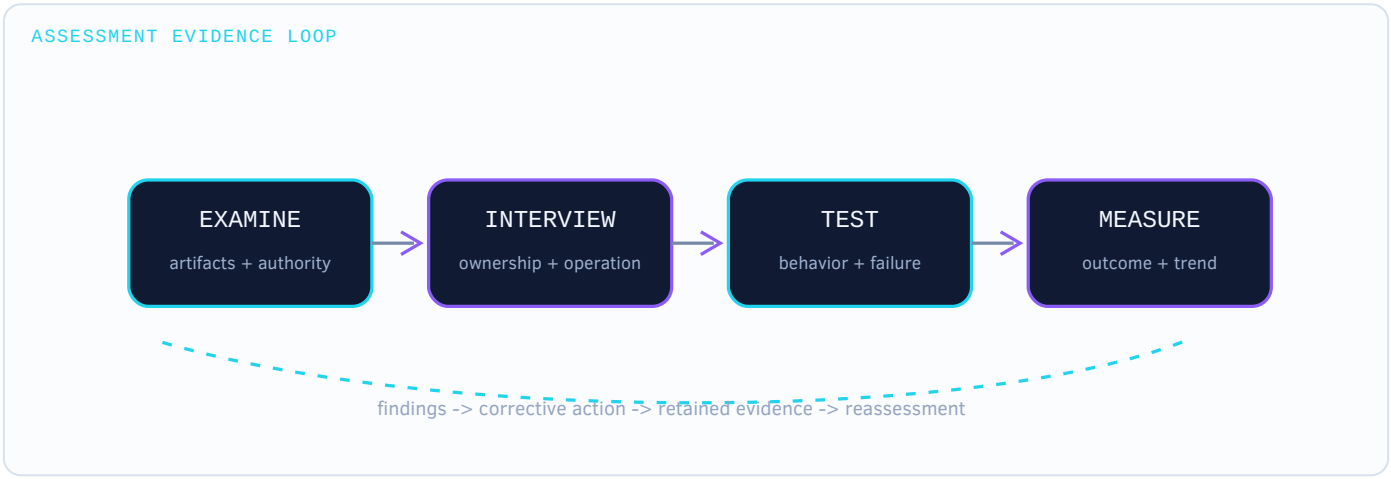
MYTHOS-FND-0010

Agentic Systems and Model Orchestration

Bound delegated action with mission contracts, policy, tool controls, memory governance, budgets, evidence, verification, and containment.

23 controls / 57 pages

Shared assurance doctrine

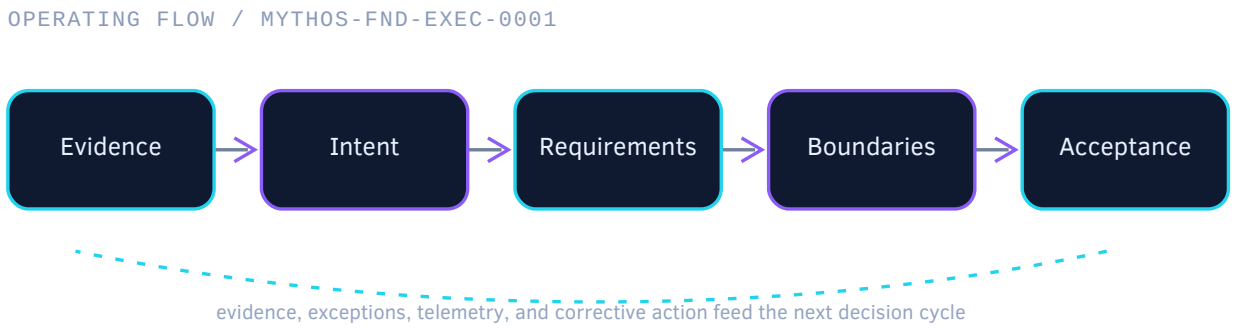


Conformance is bounded by scope, version, profile, tailoring, evidence period, assessor, and unresolved findings. Candidate status does not imply certification or implementation effectiveness. Evidence quality, independence, freshness, and reproducibility determine assessment confidence.

Implementation profiles

Profile	Institutional expectation	Typical evidence posture
Foundational	Broadly applicable minimum governance and engineering controls.	Defined ownership, current records, repeatable tests, retained evidence.
Advanced	Stronger automation, scale, independence, observability, and change discipline.	Automated policy checks, independent challenge, richer operational evidence.
High Assurance	Continuous or independent validation where consequence warrants it.	Adversarial testing, stronger isolation, continuous verification, formal or cryptographic evidence where practical.

Adoption sequence



Adoption begins by establishing accountable ownership and authoritative records, then baselining controls and evidence, implementing the selected profile, independently assuring consequential capabilities, and operating a continuous corrective-action loop. Later Mythos domain standards inherit this grammar rather than redefining it.

Publication integrity and release posture

Candidate publication set

All ten standards use permanent IDs and stable public filenames. External authority registers were revalidated on 2026-09-17; active drafts are identified without silently displacing current final authorities. The release package includes machine-readable publication, control, authority, site-metadata, QA, and SHA-256 manifests.

CANDIDATE STANDARD

Mythos Product Definition Standard

Govern product intent before implementation: evidence, scope, requirements, invariants, risk, and objective acceptance.

PERMANENT ID
MYTHOS-FND-0001

PUBLICATION CLASS
CANDIDATE STANDARD

VERSION / STATUS
1.0.0-candidate / CANDIDATE

PERMANENT PUBLICATION IDENTITY

Mythos Product Definition Standard

Universal Requirements for Product Discovery, Scope, Requirements, Prioritization, Architecture Boundaries, and Delivery Readiness

Document ID
MYTHOS-FND-0001

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	16	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	Product leaders; Engineers and architects; Security, privacy, quality, and operations leaders; Program and delivery managers; Assessors and governance bodies
Publisher / owner	Mythos Systems / Standards Program
Public classification	Public technical standard
Canonical route	/library/standards/foundation/mythos-fnd-0001/

Expected outcomes

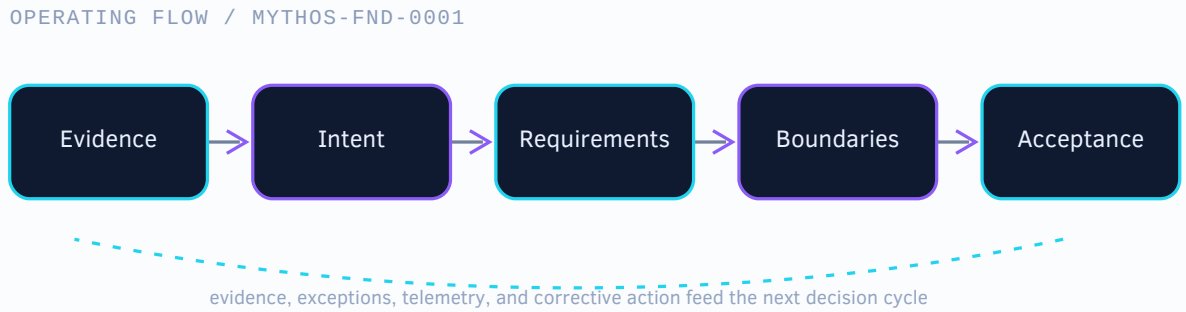
- Create a stable chain from validated problem evidence to released product outcomes.
- Prevent premature implementation, unbounded scope, hidden assumptions, and architecture-by-accident.
- Make product decisions reviewable, reversible where practical, and traceable to evidence.
- Integrate security, privacy, quality, operations, accessibility, data, and AI considerations into product definition rather than treating them as late-stage reviews.

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.

Document Control 8

Revision Record 8

How to Use This Standard 9

Executive Reading Path 9

Engineering Reading Path 9

Assessment Reading Path 9

Normative and Informative Content 9

Part I – Executive Direction 10

1. Executive Overview 10

2. Executive Findings and Required Direction 10

3. Business and Operational Impact 10

4. Target-State Summary 11

5. Leadership Responsibilities 12

Part II – Standard Foundation 13

6. Purpose and Objectives 13

7. Scope 13

8. Intended Audience 13

9. Requirements Language and Conformance 13

10. Normative References from Source Draft 14

11. Informative References from Source Draft 14

12. Terms and Definitions 14

13. Applicability and Tailoring 15

Part III – Risk and Architecture 16

14. Enterprise Problem and Risk Landscape 16

15. Governing Principles 16

16. Reference Operating Architecture 16
17. Roles and Accountability 17
18. State, Evidence, and Decision Model 18
19. Security and Trust Considerations 18
20. Failure Modes 18
21. Cross-Functional Dependencies 18

Part IV – Normative Control System **19**

22. Control-Family Overview 19
23. Normative Controls 20

Part V – Implementation and Operations **38**

24. Implementation Profiles 38
25. Implementation Lifecycle 38
26. Integration Requirements 39
27. Failure Handling and Recovery 39
28. Exceptions and Compensating Controls 39
29. Prohibited Practices 39
30. Adoption Roadmap from Source Draft 39
31. Limitations and Residual Risk from Source Draft 40

Part VI – Assurance and Assessment **41**

32. Assessment Methodology 41
33. Metrics and Reporting from Source Draft 41
34. Exceptions and Compensating Controls 42
35. Enterprise Metric Set 42
36. Maturity Model 43
37. Assessment Confidence 43
38. Executive Assurance Dashboard 43

Part VII – Authority and Traceability **45**

39. Cross-Standard Dependencies from Source Draft 45
40. Current External Authority Register 45

41. Control Traceability 45

42. Source-Draft Preservation 46

Part VIII – Appendices **47**

Appendix A — Source-Draft Evolution Notes 47

Appendix B — Change History 47

Appendix C — Control Summary 47

Appendix D — Minimum Conformance Claim Record 48

Appendix E — Publication Review Checklist 48

NORMATIVE SYSTEM

Control index

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

MYTHOS-FND-PD-01	Accountable product ownership	21
MYTHOS-FND-PD-02	Evidence-based problem definition	22
MYTHOS-FND-PD-03	Measurable product outcomes	23
MYTHOS-FND-PD-04	User, role, and workflow definition	24
MYTHOS-FND-PD-05	Explicit scope and non-goals	25
MYTHOS-FND-PD-06	Assumptions, constraints, and dependencies	26
MYTHOS-FND-PD-07	Atomic and testable requirements	28
MYTHOS-FND-PD-08	Bidirectional requirements traceability	29
MYTHOS-FND-PD-09	Quantified nonfunctional requirements	30
MYTHOS-FND-PD-10	Capability risk and impact classification	31
MYTHOS-FND-PD-11	Architecture boundaries and invariants	32
MYTHOS-FND-PD-12	Build, buy, integrate, or defer decision	33
MYTHOS-FND-PD-13	First vertical slice	34
MYTHOS-FND-PD-14	Evidence-based prioritization	35
MYTHOS-FND-PD-15	Release definition and acceptance evidence	36
MYTHOS-FND-PD-16	Current-state reconciliation and product change control	37

Document Control

Field	Value
Document ID	MYTHOS-FND-0001
Standard	Product Definition
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

Organizations lose capital, time, and trust when implementation begins before the problem, users, outcomes, boundaries, dependencies, and acceptance evidence are sufficiently defined. This standard establishes the minimum institutional system for deciding what should be built, why it should be built, what must remain true, what is deliberately excluded, and how leaders will know that the result created value without introducing unacceptable risk.

The institutional objective is to establish a disciplined product-definition system that converts evidence, stakeholder needs, constraints, risk, and intended outcomes into traceable requirements and release acceptance. 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
Unowned product authority	Product, architecture, risk, and delivery decisions fragment when accountable decision rights are not explicit.	Assign one accountable product owner and publish delegated decision rights.
Solution-first commitment	Teams commit features or technologies before validating the problem and current alternatives.	Require evidence-based discovery and a documented threshold for proceeding.
Untestable requirements	Ambiguous requirements create false completion and late disagreement.	Use atomic, owned, measurable requirements with acceptance criteria.
Hidden scope expansion	Unstated non-goals and dependencies allow uncontrolled growth.	Maintain explicit scope, exclusions, assumptions, dependencies, and deferral conditions.
Aspirational state presented as reality	Roadmaps and prototypes are confused with delivered capability.	Maintain current-state reconciliation and evidence-backed release claims.

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.

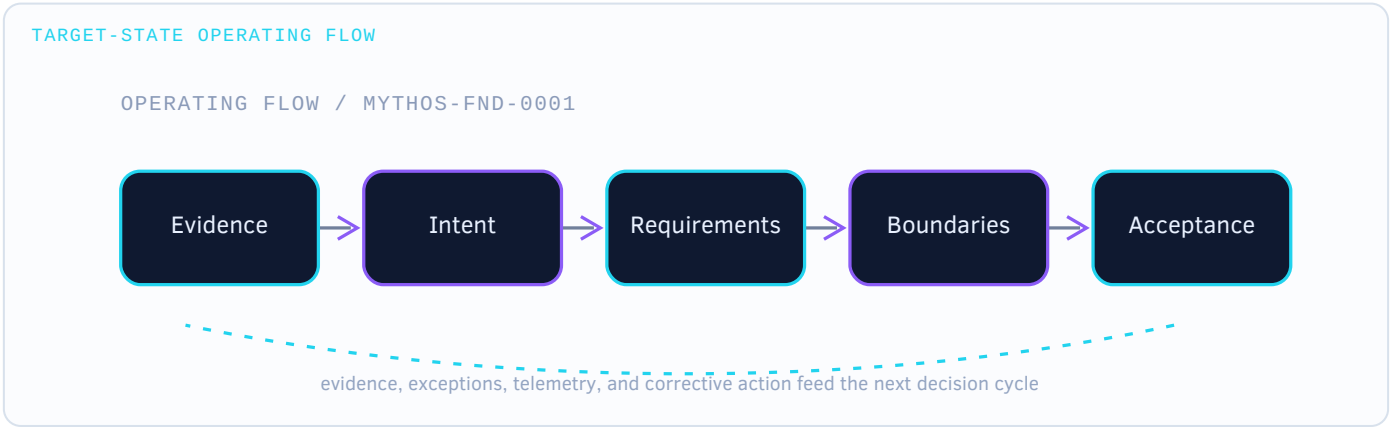
3.3 Security, Privacy, and Trust Impact

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	Product authority and decision-rights model
2	Discovery evidence and problem dossier
3	Outcome and measurement register
4	User, role, and workflow model
5	Scope, non-goal, assumption, and dependency register
6	Atomic requirements and traceability graph
7	Risk and impact classification
8	Architecture boundaries and invariants
9	Build-buy-integrate-defer decision record
10	Vertical-slice and release acceptance package

```
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
Executive sponsor	Funds the product, resolves enterprise priority conflicts, and accepts material business risk.
Accountable product owner	Owns product intent, scope, outcomes, priority, and release acceptance.
Chief or domain architect	Defines architecture boundaries, invariants, integration constraints, and technical tradeoffs.
Security, privacy, and trust lead	Challenges impact, misuse, data, and authority assumptions.
Quality and validation lead	Ensures requirements and outcomes are measurable and independently testable.
Operations owner	Confirms operability, support, recovery, telemetry, and lifecycle readiness.
Delivery lead	Maintains implementation sequence, dependencies, and evidence-based progress.
Independent assessor	Tests conformance claims and evidence sufficiency.

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

- Create a stable chain from validated problem evidence to released product outcomes.
- Prevent premature implementation, unbounded scope, hidden assumptions, and architecture-by-accident.
- Make product decisions reviewable, reversible where practical, and traceable to evidence.
- Integrate security, privacy, quality, operations, accessibility, data, and AI considerations into product definition rather than treating them as late-stage reviews.

7. Scope

Applies to new products, major capabilities, material redesigns, internal platforms, commercial services, automation systems, infrastructure products, AI-enabled applications, and significant lifecycle changes. Minor defect corrections may use a tailored profile when they do not alter behavior, risk, interfaces, or operating assumptions.

8. Intended Audience

- Product leaders
- Engineers and architects
- Security, privacy, quality, and operations leaders
- Program and delivery managers
- Assessors and governance bodies

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

- **ISO/IEC/IEEE 15288:2023** — Systems and software engineering — System life cycle processes. https://www.iso.org/standard/81702.html
- **ISO/IEC/IEEE 29148:2018** — Systems and software engineering — Life cycle processes — Requirements engineering. https://www.iso.org/standard/72089.html
- **ISO/IEC 25010:2023** — Systems and software Quality Requirements and Evaluation — Product quality model. https://www.iso.org/standard/78176.html
- **NIST CSWP 29** — The NIST Cybersecurity Framework (CSF) 2.0. https://doi.org/10.6028/NIST.CSWP.29
- **NIST AI 100-1** — Artificial Intelligence Risk Management Framework (AI RMF 1.0). https://doi.org/10.6028/NIST.AI.100-1
- **ISO/IEC 42005:2025** — Artificial intelligence — AI system impact assessment. https://www.iso.org/standard/44545.html

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.
Product definition system	The controlled set of discovery evidence, product intent, requirements, scope decisions, risk decisions, acceptance criteria, and current-state records that govern delivery.

Term	Definition
First vertical slice	The smallest end-to-end workflow that exercises meaningful user value across relevant interface, domain, data, integration, security, and operational boundaries.
Non-goal	A capability or outcome deliberately excluded from the current scope to preserve focus or manage risk.
Product invariant	A condition that must remain true across design and implementation choices.
Acceptance evidence	Objective artifacts demonstrating that a requirement or release condition has been satisfied.

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

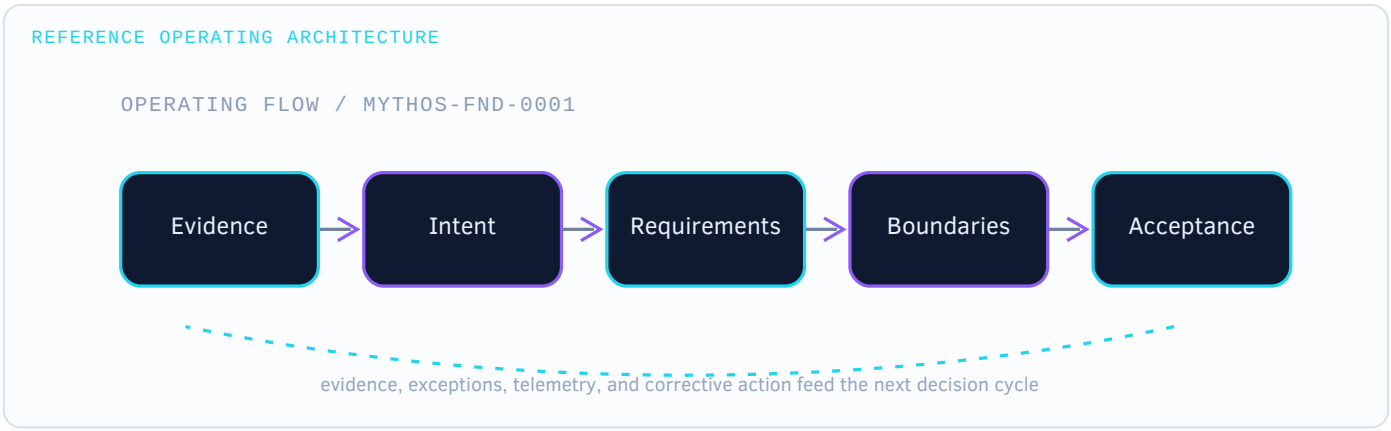
The principal enterprise risks addressed by this standard include inconsistent ownership, undocumented authority, uncontrolled change, local optimization, evidence gaps, stale assumptions, supplier dependence, false assurance, and the inability to determine whether the operating system still matches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

- Problem evidence precedes feature commitment.
- Outcomes and constraints precede implementation detail.
- Scope includes explicit non-goals and deferral conditions.
- Every requirement must be understandable, testable, owned, and traceable.
- Risk and operability are product concerns, not downstream specialties.
- The current product state must be distinguishable from aspiration and historical plans.

16. 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
Executive sponsor	Funds the product, resolves enterprise priority conflicts, and accepts material business risk.
Accountable product owner	Owns product intent, scope, outcomes, priority, and release acceptance.
Chief or domain architect	Defines architecture boundaries, invariants, integration constraints, and technical tradeoffs.
Security, privacy, and trust lead	Challenges impact, misuse, data, and authority assumptions.
Quality and validation lead	Ensures requirements and outcomes are measurable and independently testable.
Operations owner	Confirms operability, support, recovery, telemetry, and lifecycle readiness.
Delivery lead	Maintains implementation sequence, dependencies, and evidence-based progress.
Independent assessor	Tests conformance claims and evidence sufficiency.

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
Feature commitment without problem evidence	Failure can create hidden risk, misleading assurance, uncontrolled cost, or unsafe operation.
Backlogs treated as the product definition	Failure can create hidden risk, misleading assurance, uncontrolled cost, or unsafe operation.
Requirements that combine multiple behaviors or cannot be tested	Failure can create hidden risk, misleading assurance, uncontrolled cost, or unsafe operation.
Architecture decisions hidden inside implementation tickets	Failure can create hidden risk, misleading assurance, uncontrolled cost, or unsafe operation.
Roadmaps presented as current capability	Failure can create hidden risk, misleading assurance, uncontrolled cost, or unsafe operation.
Release approval based only on schedule or stakeholder sentiment	Failure can create hidden risk, misleading assurance, uncontrolled cost, or unsafe operation.

21. Cross-Functional Dependencies

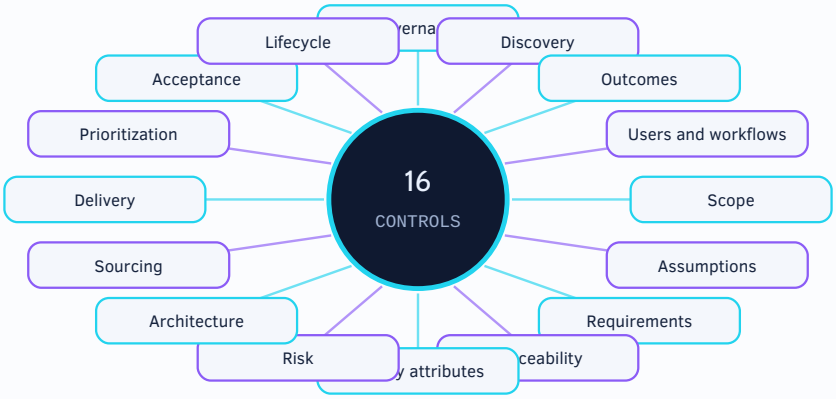
This Foundation standard depends on the remaining MYTHOS-FND standards for documentation, security and trust, quality, operations, data and integration, interfaces, extensions, AI-first behavior, and agentic orchestration. An adopting organization MUST resolve overlapping requirements through the stricter 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 **16 controls** across the following families:

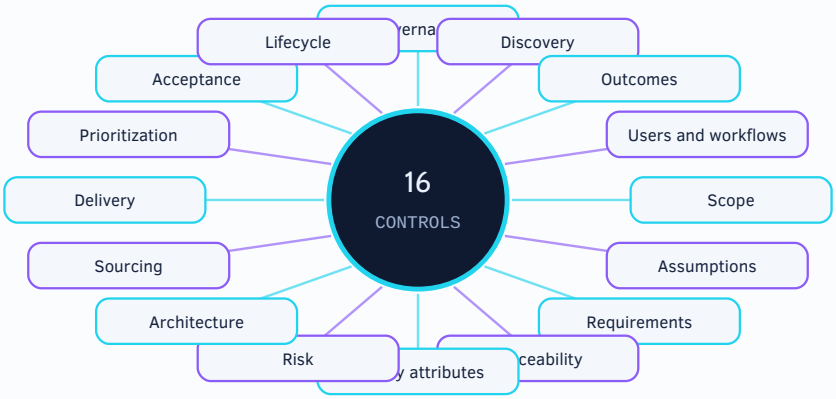
- Governance
- Discovery
- Outcomes
- Users and workflows
- Scope
- Assumptions
- Requirements
- Traceability
- Quality attributes
- Risk
- Architecture
- Sourcing
- Delivery
- Prioritization
- Acceptance
- Lifecycle

23. Normative Controls

CONTROL SET	PROFILES	ASSESSMENT
16	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-PD-01 – Accountable product ownership

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

Requirement

Each in-scope product or material capability MUST have an identified accountable owner with authority to approve product intent, scope boundaries, priority decisions, release criteria, and accepted residual risk.

Purpose

Prevents fragmented accountability and unresolved conflicts among delivery, architecture, risk, and operational stakeholders.

Applicability

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

Implementation guidance

- Record the owner and delegated decision rights in the product brief.
- Define escalation paths for cross-functional disputes.
- Separate recommendation, approval, implementation, and independent review roles where impact warrants.

Required evidence

- Approved product brief
- Responsibility and decision-rights matrix
- Sample decision records

Assessment procedure

- **Examine:** Examine whether ownership and authority are explicit.
- **Interview:** Interview stakeholders to verify that escalation and approval rights are understood.
- **Test:** Sample material decisions and confirm accountable approval.

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 — technical management processes
- NIST CSF 2.0 — GV.RR

NORMATIVE CONTROL

MYTHOS-FND-PD-02 – Evidence-based problem definition

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

Requirement

The organization MUST define the problem, affected users or stakeholders, current alternatives, observable consequences, and supporting evidence before committing a material product capability to implementation.

Purpose

Reduces solution bias, speculative scope, and investment in capabilities that do not address a validated need.

Applicability

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

Implementation guidance

- Use interviews, workflow observation, support data, incident history, market evidence, or operational measurements appropriate to the context.
- Distinguish verified facts, informed hypotheses, and unknowns.
- Define a stopping rule for discovery and the evidence threshold for proceeding.

Required evidence

- Problem statement
- Discovery log and evidence references
- Hypothesis and uncertainty register

Assessment procedure

- **Examine:** Examine evidence quality and provenance.
- **Interview:** Interview representative users and product decision makers.
- **Test:** Trace sampled features back to a validated problem or obligation.

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 29148:2018 — stakeholder needs definition

NORMATIVE CONTROL

MYTHOS-FND-PD-03 – Measurable product outcomes

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

Requirement

The product definition MUST state intended user, operational, business, safety, security, or public-interest outcomes using measures that can be evaluated after release.

Purpose

Ensures delivery is judged by achieved outcomes rather than output volume or feature completion alone.

Applicability

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

Implementation guidance

- Define leading and lagging indicators.
- Specify baseline, target, measurement owner, data source, review interval, and known confounders.
- Avoid metrics that reward harmful shortcuts or conceal distributional effects.

Required evidence

- Outcome register
- Measurement definitions
- Post-release review records

Assessment procedure

- **Examine:** Examine whether indicators are measurable and decision-relevant.
- **Interview:** Test calculation of selected measures from source data.
- **Test:** Verify that outcome reviews influence backlog or lifecycle decisions.

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 25010:2023 — quality model
- NIST AI RMF 1.0 — Measure

NORMATIVE CONTROL

MYTHOS-FND-PD-04 – User, role, and workflow definition

FAMILY	PROFILES	FAILURE IMPACT	AUTOMATION POTENTIAL
Users and workflows	Foundational, Advanced, High Assurance	Material	Manual

Requirement

The organization MUST identify primary users, affected non-users, roles, permissions, critical workflows, failure scenarios, and accessibility or environmental constraints relevant to the product scope.

Purpose

Prevents designs based on generic personas, happy paths, or assumptions that overlook operators, administrators, support teams, and impacted parties.

Applicability

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

Implementation guidance

- Model roles separately from demographic personas.
- Capture trigger, preconditions, decisions, handoffs, data, exceptional paths, and completion evidence for critical workflows.
- Include abuse, misuse, denial, degradation, and recovery scenarios.

Required evidence

- User and role catalog
- Workflow models
- Accessibility and environment constraints

Assessment procedure

- **Examine:** Examine coverage of critical and exceptional paths.
- **Interview:** Interview representative users and operators.
- **Test:** Walk through a sampled workflow against the product definition.

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 29148:2018 — operational concepts

NORMATIVE CONTROL

MYTHOS-FND-PD-05 – Explicit scope and non-goals

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

Requirement

The product definition MUST distinguish capabilities to build now, capabilities intentionally designed for later, explicit non-goals, and conditions that would trigger reconsideration.

Purpose

Constrains scope, preserves architectural options, and prevents implicit commitments from accumulating without evaluation.

Applicability

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

Implementation guidance

- Use decision criteria rather than aspirational wish lists.
- Identify interfaces or data models that require forward compatibility without prematurely implementing deferred features.
- Review non-goals whenever assumptions, risk, or market obligations materially change.

Required evidence

- Scope register
- Non-goal records
- Deferral and reconsideration criteria

Assessment procedure

- **Examine:** Examine consistency among product brief, roadmap, architecture, and backlog.
- **Interview:** Sample deferred items and confirm they are not being implemented indirectly.
- **Test:** Verify material scope changes have approval and impact analysis.

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 — decision management

NORMATIVE CONTROL

MYTHOS-FND-PD-06 – Assumptions, constraints, and dependencies

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

Requirement

Material assumptions, constraints, and dependencies MUST be recorded with an owner, confidence, impact if false or unavailable, validation method, and review trigger.

Purpose

Makes hidden premises visible before they become architectural lock-in, schedule failure, security exposure, or operational fragility.

Applicability

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

Implementation guidance

- Classify assumptions by uncertainty and impact.
- Include legal, regulatory, provider, staffing, data, performance, deployment, and interoperability dependencies.
- Convert validated assumptions into requirements or constraints and close invalid assumptions with decision records.

Required evidence

- Assumption and dependency register
- Validation results
- Linked decision records

Assessment procedure

- **Examine:** Examine aging and unresolved high-risk assumptions.
- **Interview:** Interview owners about validation plans.
- **Test:** Test whether dependency failure scenarios are represented in architecture and acceptance criteria.

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 CSF 2.0 — GV.SC
- ISO/IEC/IEEE 15288:2023 — risk management

NORMATIVE CONTROL

MYTHOS-FND-PD-07 – Atomic and testable requirements

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

Requirement

Product and system requirements MUST use stable identifiers and state an unambiguous outcome, responsible subject, applicability, trigger or conditions, acceptance criteria, and priority or obligation level.

Purpose

Enables consistent implementation, testing, change control, and conformance assessment.

Applicability

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

Implementation guidance

- Separate requirements that contain independent obligations.
- Avoid undefined terms such as intuitive, seamless, robust, secure, fast, or enterprise-grade.
- Keep implementation choices out of requirements unless they are true constraints.

Required evidence

- Requirements register
- Requirement lint results
- Review findings

Assessment procedure

- **Examine:** Examine sampled requirements for atomicity and testability.
- **Interview:** Trace requirements to evidence and acceptance tests.
- **Test:** Attempt independent interpretation and record ambiguities.

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 29148:2018 — requirements characteristics

NORMATIVE CONTROL

MYTHOS-FND-PD-08 – Bidirectional requirements traceability

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

Requirement

Applicable requirements MUST be traceable backward to their source and risk or outcome, and forward to architecture, implementation, verification, release evidence, and lifecycle status.

Purpose

Prevents orphan work, unverified obligations, undocumented behavior, and release claims unsupported by evidence.

Applicability

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

Implementation guidance

- Maintain relationships in a structured register or graph.
- Treat derived requirements as first-class records with rationale.
- Detect broken links and conflicting status automatically where practical.

Required evidence

- Traceability matrix or graph
- Automated coverage report
- Sample end-to-end traces

Assessment procedure

- **Examine:** Examine completeness and stale links.
- **Interview:** Trace a risk-to-control-to-test chain and a feature-to-source chain.
- **Test:** Test whether a changed requirement identifies affected downstream artifacts.

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 29148:2018 — traceability

NORMATIVE CONTROL

MYTHOS-FND-PD-09 – Quantified nonfunctional requirements

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

Requirement

The product definition MUST establish measurable quality-attribute requirements for applicable domains including security, privacy, reliability, performance, resilience, maintainability, usability, accessibility, interoperability, supportability, and cost or resource consumption.

Purpose

Prevents quality attributes from remaining implicit until late-stage testing or production failure.

Applicability

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

Implementation guidance

- Define workload, environment, percentile, duration, error budget, recovery objective, and measurement method where relevant.
- State tradeoffs and priority among competing attributes.
- Link quality requirements to architecture tactics and validation plans.

Required evidence

- Quality attribute scenarios
- Service and performance objectives
- Validation plans

Assessment procedure

- **Examine:** Examine coverage based on product risk.
- **Interview:** Test a sample metric definition for reproducibility.
- **Test:** Verify tradeoff decisions are documented.

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 25010:2023 — product quality model

NORMATIVE CONTROL

MYTHOS-FND-PD-10 – Capability risk and impact classification

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

Requirement

Material capabilities MUST be classified by potential impact to safety, rights, security, privacy, finances, operations, environment, mission, and affected populations before autonomy, data access, release rigor, or approval pathways are selected.

Purpose

Aligns design and assurance effort with consequence rather than novelty or schedule pressure.

Applicability

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

Implementation guidance

- Use both severity and reversibility.
- Consider misuse, foreseeable abuse, correlated failure, dependency concentration, and scale.
- Reassess classification when scope, data, autonomy, or deployment context changes.

Required evidence

- Capability risk register
- Impact assessment
- Approval and reassessment records

Assessment procedure

- **Examine:** Examine classification criteria and sampled outcomes.
- **Interview:** Interview risk owners.
- **Test:** Challenge the classification using plausible worst-case scenarios.

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 CSF 2.0 — GV.RM
- ISO/IEC 42005:2025 — AI impact assessment

NORMATIVE CONTROL

MYTHOS-FND-PD-11 – Architecture boundaries and invariants

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

Requirement

The product definition MUST identify authoritative system boundaries, trust boundaries, data ownership, external dependencies, execution authority, prohibited coupling, and invariants that implementation may not violate without approval.

Purpose

Prevents feature work from silently redefining the system architecture or expanding authority and blast radius.

Applicability

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

Implementation guidance

- Describe what the product owns, integrates, delegates, or explicitly does not control.
- State which components are authoritative for identity, policy, state, secrets, evidence, and execution.
- Link boundary changes to architecture decision records and risk review.

Required evidence

- Context and boundary diagrams
- Invariant register
- Architecture decisions

Assessment procedure

- **Examine:** Examine alignment among boundaries, contracts, and deployment.
- **Interview:** Trace a high-risk workflow across trust and execution boundaries.
- **Test:** Test whether unauthorized coupling would be detected in review or CI.

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 — architecture definition
- NIST SP 800-207 — resource and trust boundaries

NORMATIVE CONTROL

MYTHOS-FND-PD-12 – Build, buy, integrate, or defer decision

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

Requirement

Material sourcing decisions MUST evaluate strategic differentiation, total lifecycle cost, security and privacy exposure, interoperability, portability, operational burden, supplier viability, exit strategy, and evidence quality.

Purpose

Reduces avoidable reinvention, unsafe dependency adoption, and lock-in that cannot be reversed at acceptable cost.

Applicability

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

Implementation guidance

- Compare the no-action and defer options, not only competing products.
- Separate pilot evidence from marketing claims.
- Define contractual, technical, and data exit conditions before adopting critical dependencies.

Required evidence

- Sourcing decision record
- Evaluation evidence
- Exit and contingency plan

Assessment procedure

- **Examine:** Examine decision completeness and conflicts of interest.
- **Interview:** Verify critical assumptions against primary evidence.
- **Test:** Test portability or replacement for high-impact dependencies where feasible.

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 — supply-chain risk management

NORMATIVE CONTROL

MYTHOS-FND-PD-13 – First vertical slice

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

Requirement

Before broad feature expansion, the team SHOULD implement and validate a first vertical slice that delivers meaningful end-to-end value and exercises the most consequential architecture, integration, security, data, and operational assumptions.

Purpose

Creates early evidence about feasibility and system behavior while change remains comparatively inexpensive.

Applicability

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

Implementation guidance

- Choose a real workflow rather than a disconnected technical demo.
- Include observable failures, authorization, persistence, telemetry, and recovery relevant to the slice.
- Record exclusions so the slice is not misrepresented as production readiness.

Required evidence

- Vertical-slice definition
- Demonstration and test evidence
- Learning and decision record

Assessment procedure

- **Examine:** Examine whether the slice tests the highest-uncertainty boundaries.
- **Interview:** Observe execution of the workflow.
- **Test:** Verify findings changed requirements, architecture, or plans where appropriate.

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 — implementation and integration

NORMATIVE CONTROL

MYTHOS-FND-PD-14 – Evidence-based prioritization

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

Requirement

Prioritization MUST account for user or mission value, obligation, risk reduction, dependency order, uncertainty reduction, effort, opportunity cost, operational burden, and confidence; a composite score MUST NOT conceal mandatory or safety-critical work.

Purpose

Avoids false precision and prevents attractive feature work from displacing obligations, foundational work, or risk controls.

Applicability

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

Implementation guidance

- Show underlying dimensions and confidence.
- Identify dependency enablers separately from direct user value.
- Revisit rankings when evidence or constraints change.

Required evidence

- Prioritization model
- Decision log
- Backlog history

Assessment procedure

- **Examine:** Examine whether mandatory work can be overridden by scoring.
- **Interview:** Recalculate sampled priorities from source data.
- **Test:** Interview decision makers about overrides and confidence.

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 CSF 2.0 — GV.OV and GV.RM

NORMATIVE CONTROL

MYTHOS-FND-PD-15 – Release definition and acceptance evidence

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

Requirement

Each release stage MUST have explicit entry, exit, rollback, support, security, quality, documentation, operational, and acceptance-evidence criteria appropriate to its audience and risk.

Purpose

Prevents labels such as alpha, preview, production, or generally available from becoming ungoverned marketing terms.

Applicability

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

Implementation guidance

- Define permissible users, data, environments, guarantees, and support expectations for each stage.
- Require failed mandatory criteria to block release unless an authorized exception process explicitly permits otherwise.
- Preserve immutable release evidence.

Required evidence

- Release criteria
- Signed or approved evidence bundle
- Exception and rollback records

Assessment procedure

- **Examine:** Examine a sampled release against its declared stage.
- **Interview:** Test whether failed mandatory criteria block promotion.
- **Test:** Verify evidence integrity and traceability.

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 — verification, validation, transition

NORMATIVE CONTROL

MYTHOS-FND-PD-16 – Current-state reconciliation and product change control

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

Requirement

The organization MUST maintain an authoritative current-state record and reconcile material changes in product intent, implemented capability, known limitations, risk, dependencies, and release status within a defined interval.

Purpose

Prevents roadmaps, plans, documentation, and stakeholder expectations from diverging from the deployed system.

Applicability

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

Implementation guidance

- Separate current, planned, deprecated, and historical states.
- Define triggers for product redefinition, including incidents, regulation, dependency changes, new data uses, and autonomy changes.
- Retire or supersede conflicting documents rather than leaving ambiguity.

Required evidence

- Current-state record
- Change and reconciliation log
- Supersession notices

Assessment procedure

- **Examine:** Compare current-state claims with production evidence and release records.
- **Interview:** Sample a material change and trace updates.
- **Test:** Test automated drift detection where implemented.

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 — configuration and information management

FOUNDATION STANDARD / STRUCTURAL PART

Part V – Implementation and Operations

24. Implementation Profiles

Profile	Required Operating State
Baseline	Named ownership, validated problem, explicit scope, atomic requirements, risk classification, first vertical slice, and release acceptance evidence.
Enterprise	Portfolio governance, automated traceability, quantitative outcomes, architecture review, dependency governance, and independent release challenge.
High Assurance	Formal invariants, independent validation, adversarial requirements review, continuous traceability, cryptographically protected evidence, and documented residual-risk acceptance.

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

- Feature commitment without problem evidence
- Backlogs treated as the product definition
- Requirements that combine multiple behaviors or cannot be tested
- Architecture decisions hidden inside implementation tickets
- Roadmaps presented as current capability
- Release approval based only on schedule or stakeholder sentiment

30. Adoption Roadmap from Source Draft

- Establish accountable product ownership, a product brief, and a current-state record.

- Create a requirements register with stable identifiers, acceptance criteria, and traceability.
- Classify risk, define the first vertical slice, and document architecture boundaries and non-goals.
- Implement evidence-backed prioritization, release readiness, and post-release outcome review.
- For Advanced and High Assurance adoption, add independent challenge, scenario analysis, automated traceability checks, and continuous current-state reconciliation.

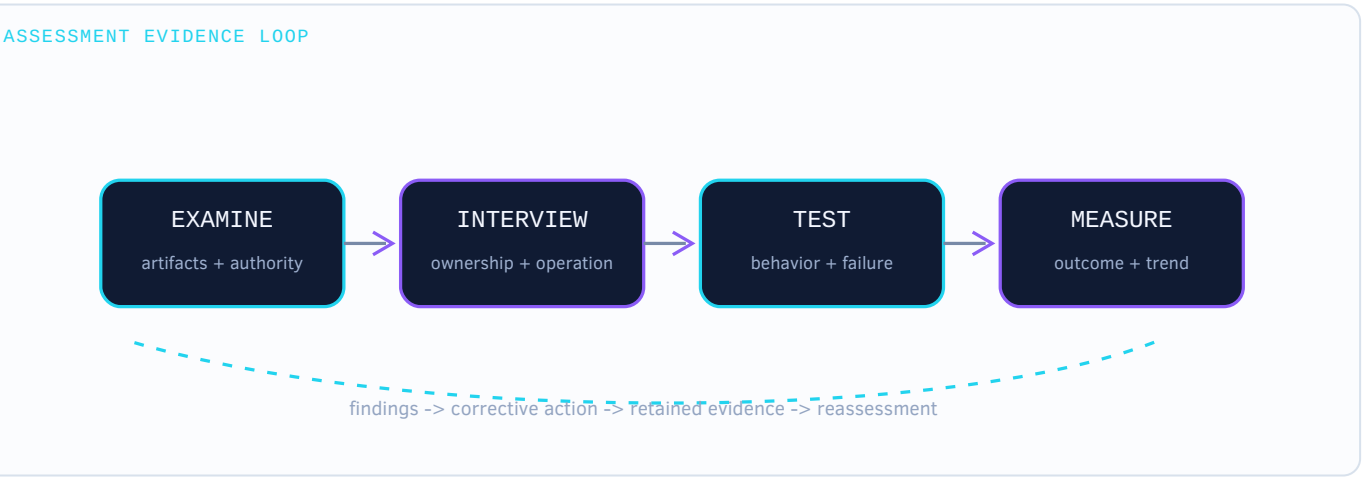
31. Limitations and Residual Risk from Source Draft

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
Requirement traceability coverage	Applicable requirements linked to source evidence, implementation, and acceptance evidence	>= 95% Advanced; 100% High Assurance
	Open assumptions rated high impact or high uncertainty	

Metric	Definition	Expected use or target
Unresolved material assumptions		0 at release authorization unless formally accepted
Scope volatility	Material scope additions after implementation commitment	Tracked by cause and decision latency; declining trend
Acceptance evidence completeness	Release requirements with objective pass/fail evidence	100% of MUST requirements
Outcome realization	Released outcomes meeting the defined success indicators	Measured at the review interval defined in the product brief

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.

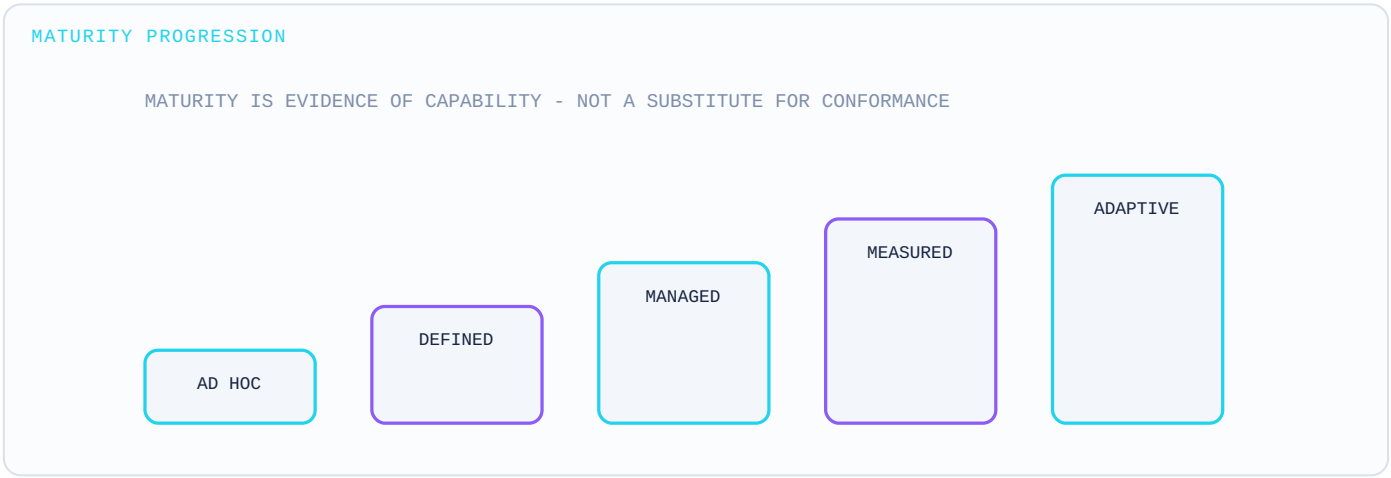
34. Exceptions and Compensating Controls

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
requirements with accountable owner	Defined by the adopting organization with owner, source, target, and cadence.
requirements with verified acceptance evidence	Defined by the adopting organization with owner, source, target, and cadence.
features traceable to validated problem or obligation	Defined by the adopting organization with owner, source, target, and cadence.
open assumptions past review date	Defined by the adopting organization with owner, source, target, and cadence.
scope changes without decision record	Defined by the adopting organization with owner, source, target, and cadence.
release claims unsupported by evidence	Defined by the adopting organization with owner, source, target, and cadence.
outcome measures reviewed after release	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
ISO/IEC/IEEE 15288:2023	System life cycle processes	https://www.iso.org/standard/81702.html	Published	2026-09-17
ISO/IEC/IEEE 29148:2018	Requirements engineering	https://www.iso.org/standard/72089.html	Published	2026-09-17
ISO/IEC 25010:2023	Product quality model	https://www.iso.org/standard/78176.html	Published	2026-09-17
ISO/IEC/IEEE 16085:2021	Life-cycle risk management	https://www.iso.org/standard/74371.html	Published	2026-09-17
NIST CSF 2.0	Cybersecurity risk governance	https://www.nist.gov/cyberframework	Current	2026-09-17
NIST AI RMF 1.0	AI risk management	https://www.nist.gov/itl/ai-risk-management-framework	Current; revision program active	2026-09-17
ISO/IEC 42005:2025	AI system impact assessment	https://www.iso.org/standard/42005	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

- Preserves the source draft's strong treatment of product briefs, first vertical slices, non-goals, requirement quality, and current-state discipline.
- Reframes AI-specific delivery instructions as universally applicable governance controls.
- Replaces product-type labels with risk-based assurance profiles shared across the Mythos standards series.
- Separates normative controls from informative templates and implementation examples.

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-PD-01	Governance	Accountable product ownership	Foundational, Advanced, High Assurance	Partial	Critical
MYTHOS-FND-PD-02	Discovery	Evidence-based problem definition	Foundational, Advanced, High Assurance	Partial	Material
MYTHOS-FND-PD-03	Outcomes	Measurable product outcomes	Foundational, Advanced, High Assurance	Partial	Material
MYTHOS-FND-PD-04	Users and workflows	User, role, and workflow definition	Foundational, Advanced, High Assurance	Manual	Material
MYTHOS-FND-PD-05	Scope	Explicit scope and non-goals	Foundational, Advanced, High Assurance	Partial	Material
MYTHOS-FND-PD-06	Assumptions	Assumptions, constraints, and dependencies	Foundational, Advanced, High Assurance	Partial	Critical
MYTHOS-FND-PD-07	Requirements	Atomic and testable requirements	Foundational, Advanced, High Assurance	High	Critical
MYTHOS-FND-PD-08	Traceability	Bidirectional requirements traceability	Advanced, High Assurance	High	Critical
MYTHOS-FND-PD-09	Quality attributes	Quantified nonfunctional requirements	Foundational, Advanced, High Assurance	Partial	Critical
MYTHOS-FND-PD-10	Risk	Capability risk and impact classification	Foundational, Advanced, High Assurance	Partial	Critical
	Architecture	Architecture boundaries and invariants		Partial	Critical

Control	Family	Title	Profiles	Automation	Impact
MYTHOS-FND-PD-11			Foundational, Advanced, High Assurance		
MYTHOS-FND-PD-12	Sourcing	Build, buy, integrate, or defer decision	Foundational, Advanced, High Assurance	Partial	Material
MYTHOS-FND-PD-13	Delivery	First vertical slice	Foundational, Advanced, High Assurance	Partial	Material
MYTHOS-FND-PD-14	Prioritization	Evidence-based prioritization	Foundational, Advanced, High Assurance	High	Material
MYTHOS-FND-PD-15	Acceptance	Release definition and acceptance evidence	Foundational, Advanced, High Assurance	High	Critical
MYTHOS-FND-PD-16	Lifecycle	Current-state reconciliation and product change control	Foundational, Advanced, High Assurance	High	Critical

Appendix D – Minimum Conformance Claim Record

```
standard: MYTHOS-FND-0001
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

CANDIDATE STANDARD

Mythos Documentation System Standard

Treat documentation as an engineered authority, evidence, traceability, and lifecycle system.

PERMANENT ID
MYTHOS-FND-0002

PUBLICATION CLASS
CANDIDATE STANDARD

VERSION / STATUS
1.0.0-candidate / CANDIDATE

PERMANENT PUBLICATION IDENTITY

Mythos Documentation System Standard

Universal Requirements for Documentation Authority, Architecture, Traceability, Evidence, Documentation-as-Code, and Lifecycle Governance

Document ID
MYTHOS-FND-0002

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	Technical writers and documentation engineers; Engineers and architects; Product, security, quality, and operations teams; AI and automation system designers; Auditors, assessors, and reviewers
Publisher / owner	Mythos Systems / Standards Program
Public classification	Public technical standard
Canonical route	/library/standards/foundation/mythos-fnd-0002/

Expected outcomes

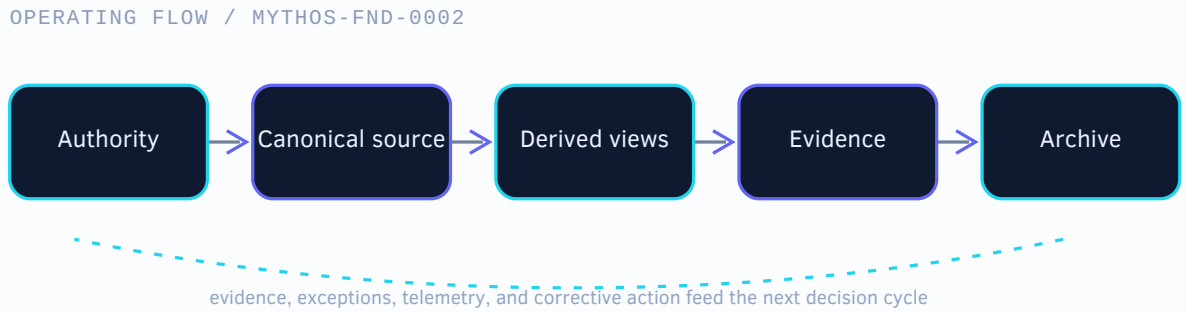
- Ensure every material claim has an identifiable authority, owner, status, and source.
- Make documentation discoverable and usable by engineers, operators, users, assessors, and authorized automation.
- Prevent stale plans, generated artifacts, and informal notes from silently overriding authoritative records.
- Integrate documentation quality and traceability into delivery and operations workflows.

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.

Document Control 8

Revision Record 8

How to Use This Standard 9

Executive Reading Path 9

Engineering Reading Path 9

Assessment Reading Path 9

Normative and Informative Content 9

Part I – Executive Direction 10

1. Executive Overview 10

2. Executive Findings and Required Direction 10

3. Business and Operational Impact 10

4. Target-State Summary 11

5. Leadership Responsibilities 12

Part II – Standard Foundation 13

6. Purpose and Objectives 13

7. Scope 13

8. Intended Audience 13

9. Requirements Language and Conformance 13

10. Normative References from Source Draft 13

11. Informative References from Source Draft 14

12. Terms and Definitions 14

13. Applicability and Tailoring 15

Part III – Risk and Architecture 16

14. Enterprise Problem and Risk Landscape 16

15. Governing Principles 16

16. Reference Operating Architecture 16

17. Roles and Accountability 17

18. State, Evidence, and Decision Model 18

19. Security and Trust Considerations 18

20. Failure Modes 18

21. Cross-Functional Dependencies 18

Part IV – Normative Control System 19

22. Control-Family Overview 19

23. Normative Controls 20

Part V – Implementation and Operations 39

24. Implementation Profiles 39

25. Implementation Lifecycle 39

26. Integration Requirements 40

27. Failure Handling and Recovery 40

28. Exceptions and Compensating Controls 40

29. Prohibited Practices 40

30. Adoption Roadmap from Source Draft 40

31. Limitations and Residual Risk from Source Draft 41

Part VI – Assurance and Assessment 42

32. Assessment Methodology 42

33. Metrics and Reporting from Source Draft 42

34. Exceptions and Compensating Controls 43

35. Enterprise Metric Set 43

36. Maturity Model 44

37. Assessment Confidence 44

38. Executive Assurance Dashboard 44

Part VII – Authority and Traceability 46

39. Cross-Standard Dependencies from Source Draft 46

40. Current External Authority Register 46

41. Control Traceability 46

42. Source-Draft Preservation 47

Part VIII – Appendices **48**

Appendix A — Source-Draft Evolution Notes 48

Appendix B — Change History 48

Appendix C — Control Summary 48

Appendix D — Minimum Conformance Claim Record 49

Appendix E — Publication Review Checklist 49

NORMATIVE SYSTEM

Control index

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

MYTHOS-FND-DOC-01	Documentation authority model	21
MYTHOS-FND-DOC-02	Canonical metadata and identity	22
MYTHOS-FND-DOC-03	Authoritative documentation map	23
MYTHOS-FND-DOC-04	Risk-based documentation profile	24
MYTHOS-FND-DOC-05	Status, review, and supersession lifecycle	25
MYTHOS-FND-DOC-06	Architecture documentation and invariants	26
MYTHOS-FND-DOC-07	Architecture and product decision records	27
MYTHOS-FND-DOC-08	Contract and interface documentation	28
MYTHOS-FND-DOC-09	Documentation traceability graph	29
MYTHOS-FND-DOC-10	Security, privacy, and risk documentation	30
MYTHOS-FND-DOC-11	Test strategy and evidence documentation	31
MYTHOS-FND-DOC-12	Actionable runbooks and operational documentation	32
MYTHOS-FND-DOC-13	Release documentation and evidence manifest	33
MYTHOS-FND-DOC-14	Audience-appropriate user information	34
MYTHOS-FND-DOC-15	Documentation-as-code controls	35
MYTHOS-FND-DOC-16	Generated-documentation boundaries	36
MYTHOS-FND-DOC-17	Safe machine and AI consumption	37
MYTHOS-FND-DOC-18	Documentation quality and drift management	38

Document Control

Field	Value
Document ID	MYTHOS-FND-0002
Standard	Documentation System
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

Documentation is operational infrastructure. When teams cannot identify which document is authoritative, current, reviewed, applicable, and connected to implementation, engineering decisions become unrepeatable and operational risk rises. This standard defines documentation as a governed system of records, decisions, contracts, runbooks, evidence, and audience-specific guidance rather than a loose collection of files.

The institutional objective is to establish an authoritative, lifecycle-managed documentation system that makes products, systems, decisions, interfaces, operations, risks, tests, and user obligations understandable and traceable. 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
Multiple competing truths	Wikis, tickets, repositories, and generated drafts often disagree without an authority model.	Publish a documentation map and canonical authority for every information class.
Stale but plausible guidance	Old documents remain discoverable and are mistaken for current direction.	Require status, supersession, review triggers, and drift detection.
Untraceable decisions	Architecture and product decisions are lost inside chats and meetings.	Capture decisions with rationale, alternatives, consequences, and supersession.
Generated-documentation risk	AI-generated text can create convincing but unsupported system descriptions.	Label generated content, require source pointers, and validate against observed implementation.
Unsafe machine consumption	Agents may ingest obsolete, malicious, or out-of-scope documents as instructions.	Separate source content from instructions and publish safe machine-consumption boundaries.

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.

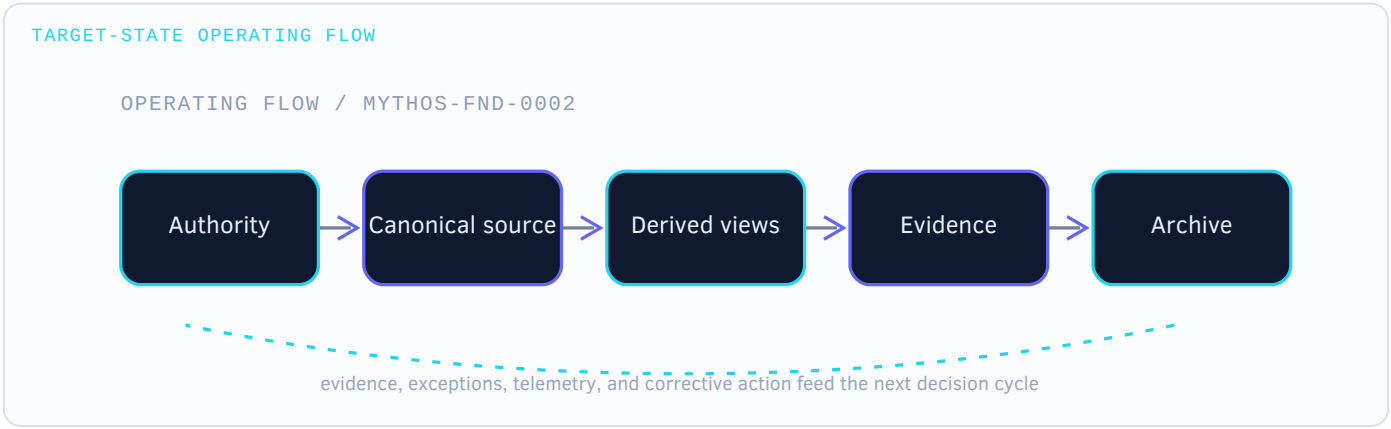
3.3 Security, Privacy, and Trust Impact

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	Documentation authority and ownership model
2	Canonical metadata and document identity
3	Authoritative documentation map
4	Risk-based documentation profiles
5	Status, review, supersession, and retirement lifecycle
6	Architecture and decision records
7	Contract and interface documentation
8	Traceability graph
9	Security, privacy, test, operations, release, and user information
10	Documentation-as-code pipeline
11	Generated-content governance
12	Machine and agent consumption boundary
13	Quality and drift management

```
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
Executive sponsor	Requires documentation accountability for material systems.
Documentation owner	Owns the documentation system and publication policy.
Domain author	Maintains technically accurate content.
Architecture authority	Approves architecture and decision records.
Operations owner	Owns runbooks and operational procedures.
Security and privacy reviewer	Reviews sensitive and risk-bearing content.
Release manager	Ensures release documentation and evidence are complete.
Information architect	Maintains taxonomy, discoverability, templates, and audience paths.
Independent reviewer	Tests accuracy, completeness, currency, and traceability.

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

- Ensure every material claim has an identifiable authority, owner, status, and source.
- Make documentation discoverable and usable by engineers, operators, users, assessors, and authorized automation.
- Prevent stale plans, generated artifacts, and informal notes from silently overriding authoritative records.
- Integrate documentation quality and traceability into delivery and operations workflows.

7. Scope

Applies to product, architecture, security, privacy, data, interface, contract, test, release, operations, user, governance, decision, and evidence documentation for systems of any implementation technology.

8. Intended Audience

- Technical writers and documentation engineers
- Engineers and architects
- Product, security, quality, and operations teams
- AI and automation system designers
- Auditors, assessors, and reviewers

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

- **ISO/IEC/IEEE 26514:2022** — Design and development of information for users. https://www.iso.org/standard/77451.html
- **ISO/IEC/IEEE 15288:2023** — Systems and software engineering — System life cycle processes. https://www.iso.org/standard/81702.html
- **ISO/IEC/IEEE 29148:2018** — Systems and software engineering — Life cycle processes — Requirements engineering. https://www.iso.org/standard/72089.html
- **NIST SP 800-218 v1.1** — Secure Software Development Framework (SSDF). https://csrc.nist.gov/pubs/sp/800/218/final
- **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.
Authority class	A declared category indicating whether a document is policy, product authority, architecture authority, contract authority, decision authority, operational authority, evidence, or informational material.
Documentation map	The authoritative index describing what documents exist, their purpose, authority, status, owner, and recommended reading order.
Generated documentation	Documentation produced from code, schemas, configuration, telemetry, or another authoritative source through a reproducible process.
Documentation drift	A material divergence between documentation and the system, process, contract, or decision it claims to represent.

Term	Definition
Supersession	A controlled transition in which a document is replaced while historical identity and traceability are preserved.

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.

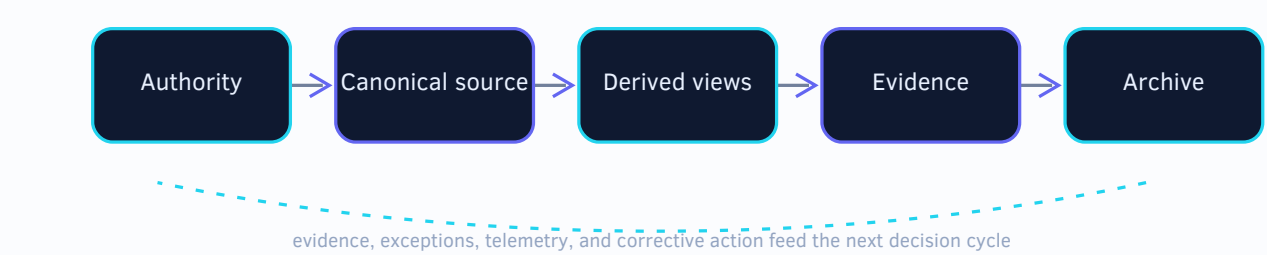
Adopting organizations SHOULD maintain a domain-specific risk register that identifies cause, affected asset or stakeholder, credible scenario, impact, existing controls, residual risk, owner, review trigger, and evidence. Risks that cross standards MUST be linked rather than copied into disconnected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

15. Governing Principles

- Documentation has explicit authority and conflict-resolution rules.
- The source of truth is named; generated views do not silently become authorities.
- Documentation is versioned, reviewable, testable, and maintained with the system.
- Current state, future intent, evidence, and historical record remain distinguishable.
- Documentation must support both human judgment and safe machine retrieval.
- Operational documents are validated through use, not merely publication.

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
Executive sponsor	Requires documentation accountability for material systems.
Documentation owner	Owns the documentation system and publication policy.
Domain author	Maintains technically accurate content.
Architecture authority	Approves architecture and decision records.
Operations owner	Owns runbooks and operational procedures.
Security and privacy reviewer	Reviews sensitive and risk-bearing content.
Release manager	Ensures release documentation and evidence are complete.
Information architect	Maintains taxonomy, discoverability, templates, and audience paths.
Independent reviewer	Tests accuracy, completeness, currency, and traceability.

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
Treating chat transcripts as authoritative documentation	Failure can create hidden risk, misleading assurance, uncontrolled cost, or unsafe operation.
Maintaining duplicate current documents without precedence	Failure can create hidden risk, misleading assurance, uncontrolled cost, or unsafe operation.
Publishing generated text without provenance or review	Failure can create hidden risk, misleading assurance, uncontrolled cost, or unsafe operation.
Runbooks that describe goals but not executable steps	Failure can create hidden risk, misleading assurance, uncontrolled cost, or unsafe operation.
Architecture diagrams without version or scope	Failure can create hidden risk, misleading assurance, uncontrolled cost, or unsafe operation.
Deleting superseded decisions instead of preserving history	Failure can create hidden risk, misleading assurance, uncontrolled cost, or unsafe operation.

21. Cross-Functional Dependencies

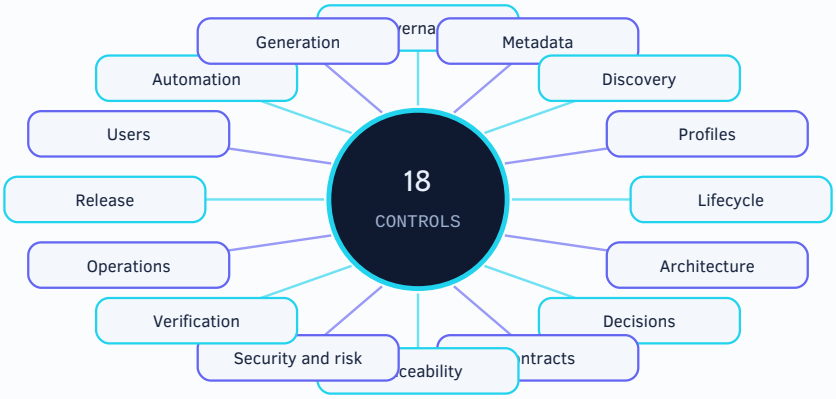
This Foundation standard depends on the remaining MYTHOS-FND standards for documentation, security and trust, quality, operations, data and integration, interfaces, extensions, AI-first behavior, and agentic orchestration. An adopting organization MUST resolve overlapping requirements through the stricter 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
- Metadata
- Discovery
- Profiles
- Lifecycle
- Architecture
- Decisions
- Contracts
- Traceability
- Security and risk
- Verification
- Operations
- Release
- Users
- Automation
- Generation
- Machine consumption
- Quality

23. Normative Controls

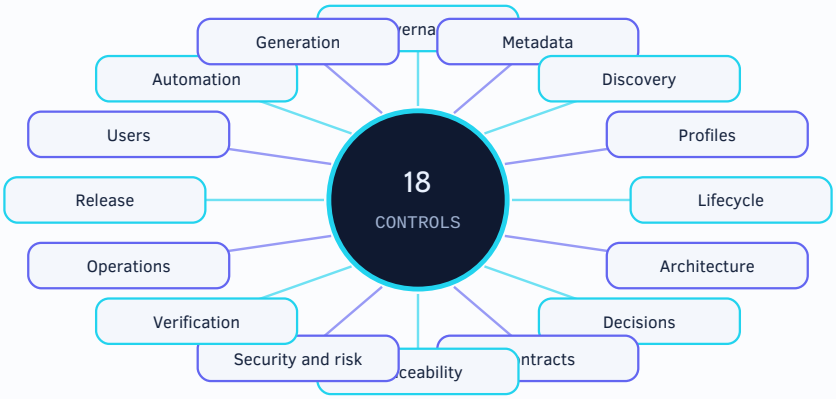
CONTROL SET
18
atomic requirements

PROFILES
3
cumulative assurance levels

ASSESSMENT
4
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-DOC-01 – Documentation authority model

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

Requirement

The organization MUST define documentation authority classes and an explicit conflict-resolution order that identifies which artifact governs when statements disagree.

Purpose

Prevents informal notes, stale plans, generated files, or presentation material from overriding policy, contracts, decisions, or current-state authority.

Applicability

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

Implementation guidance

- Define at minimum policy, product, architecture, contract, decision, operational, evidence, and informational classes.
- Declare the authority class in metadata.
- Require conflicts to be resolved rather than silently interpreted.

Required evidence

- Authority policy
- Sample metadata
- Conflict resolution records

Assessment procedure

- **Examine:** Examine whether authority classes are consistently used.
- **Interview:** Present a conflict scenario and verify the resolution path.
- **Test:** Sample resolved conflicts for traceability.

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 — information management

NORMATIVE CONTROL

MYTHOS-FND-DOC-02 – Canonical metadata and identity

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

Requirement

Authoritative documents MUST have a stable identifier, title, version, status, owner, approver or approval authority, classification, effective date, review trigger or interval, and supersession relationship where applicable.

Purpose

Enables reliable discovery, governance, lifecycle management, citation, and machine processing.

Applicability

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

Implementation guidance

- Use repository-independent IDs.
- Separate content version from file path or storage revision.
- Validate required metadata automatically.

Required evidence

- Metadata schema
- Validation results
- Sample document headers

Assessment procedure

- **Examine:** Examine metadata completeness and uniqueness.
- **Interview:** Test automated rejection of missing required fields.
- **Test:** Verify moved or renamed documents retain stable identity.

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 26514:2022 — information management

NORMATIVE CONTROL

MYTHOS-FND-DOC-03 – Authoritative documentation map

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

Requirement

Each product, service, or governed program MUST maintain a documentation map that identifies authoritative documents, owners, statuses, audiences, known gaps, historical material, and recommended reading paths.

Purpose

Reduces search cost and prevents users or automated systems from relying on the first discoverable but non-authoritative artifact.

Applicability

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

Implementation guidance

- Provide role-based reading paths for new engineers, operators, security reviewers, product owners, and machine consumers.
- Link superseded content through history rather than mixing it with active guidance.
- Treat missing required documents as visible gaps.

Required evidence

- Documentation map
- User retrieval test results
- Gap register

Assessment procedure

- **Examine:** Ask representative users to locate authoritative answers.
- **Interview:** Verify every listed artifact exists and metadata agrees.
- **Test:** Sample repository documents not in the map and determine disposition.

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 26514:2022 — information architecture

NORMATIVE CONTROL

MYTHOS-FND-DOC-04 – Risk-based documentation profile

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

Requirement

The organization MUST select and document a documentation profile proportionate to system complexity, lifecycle, user impact, regulatory exposure, operational criticality, data sensitivity, and extension or AI capabilities.

Purpose

Avoids both under-documentation of high-risk systems and wasteful documentation requirements for low-risk utilities.

Applicability

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

Implementation guidance

- Define minimum required artifact classes per profile.
- Allow lean documents to combine concerns when authority and ownership remain clear.
- Strengthen documentation following incidents, scale increases, new integrations, or material autonomy.

Required evidence

- Selected profile
- Tailoring rationale
- Required-document checklist

Assessment procedure

- **Examine:** Examine whether the profile matches risk.
- **Interview:** Verify required classes are present or explicitly tailored.
- **Test:** Review profile changes after material triggers.

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 Rev. 5 — PL family

NORMATIVE CONTROL

MYTHOS-FND-DOC-05 – Status, review, and supersession lifecycle

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

Requirement

Authoritative documents MUST use a controlled lifecycle with defined status meanings, promotion criteria, review triggers, deprecation rules, supersession links, and historical retention.

Purpose

Prevents draft or obsolete material from being treated as approved and preserves decision history without creating ambiguity.

Applicability

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

Implementation guidance

- Use statuses such as working draft, reviewed draft, approved, deprecated, superseded, and withdrawn.
- Display prominent notices on non-current documents.
- Trigger review after relevant incidents, architecture changes, interface changes, or source-standard updates.

Required evidence

- Lifecycle policy
- Review and approval records
- Supersession graph

Assessment procedure

- **Examine:** Examine status consistency.
- **Interview:** Test links from superseded to successor documents.
- **Test:** Sample overdue reviews and verify escalation.

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 — configuration management

NORMATIVE CONTROL

MYTHOS-FND-DOC-06 – Architecture documentation and invariants

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

Requirement

Architecture documentation MUST describe system context, components, responsibilities, data and control flows, trust boundaries, deployment variants, dependencies, failure domains, and invariants at a level sufficient for implementation and independent review.

Purpose

Makes architecture decisions and risk-bearing boundaries visible rather than implicit in code or tribal knowledge.

Applicability

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

Implementation guidance

- Use multiple views when one diagram cannot represent logical, deployment, data, security, and operational concerns.
- Record assumptions and known omissions.
- Keep diagrams as text or reproducible source where practical.

Required evidence

- Architecture description
- Diagrams and source
- Invariant register

Assessment procedure

- **Examine:** Trace a critical workflow through documented components.
- **Interview:** Compare deployed topology with architecture claims.
- **Test:** Interview maintainers about undocumented boundaries.

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 — architecture definition

NORMATIVE CONTROL

MYTHOS-FND-DOC-07 – Architecture and product decision records

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

Requirement

Material decisions MUST be recorded with context, decision, alternatives, consequences, risks, validation, owner, date, and revisit triggers; accepted decision records MUST remain immutable except for metadata and supersession links.

Purpose

Preserves rationale, supports future reversal, and prevents recurring debates or undocumented architecture drift.

Applicability

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

Implementation guidance

- Define triggers such as new dependencies, irreversible data models, trust-boundary changes, public contracts, and significant cost commitments.
- Create a new superseding record rather than rewriting history.
- Link decisions to requirements and implementation.

Required evidence

- Decision records
- Supersession links
- Validation evidence

Assessment procedure

- **Examine:** Sample changes and determine whether decisions were recorded.
- **Interview:** Verify alternatives and negative consequences are substantive.
- **Test:** Trace a superseded decision to current authority.

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 — decision management

NORMATIVE CONTROL

MYTHOS-FND-DOC-08 – Contract and interface documentation

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

Requirement

Externally or internally consumed interfaces, schemas, events, configuration formats, extension contracts, and command behaviors MUST have versioned, machine-readable contracts or precise normative documentation with compatibility rules.

Purpose

Reduces integration ambiguity and enables automated validation of compatibility and behavior.

Applicability

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

Implementation guidance

- Name the authoritative source for each contract.
- Generate human-readable views from machine-readable contracts where feasible.
- Document errors, limits, authorization, deprecation, and examples.

Required evidence

- API or schema specifications
- Compatibility policy
- Contract test results

Assessment procedure

- **Examine:** Validate examples against the contract.
- **Interview:** Test backward-compatibility claims.
- **Test:** Verify documentation and implementation derive from the same authority.

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

- OpenAPI Specification 3.2.0
- JSON Schema 2020-12

NORMATIVE CONTROL

MYTHOS-FND-DOC-09 – Documentation traceability graph

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

Requirement

The documentation system MUST support bidirectional traceability among source obligations, requirements, risks, decisions, architecture, contracts, implementation, tests, evidence, releases, incidents, and lifecycle status for material items.

Purpose

Allows impact analysis, completeness assessment, and reliable explanation of why the system exists and how it is verified.

Applicability

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

Implementation guidance

- Use stable identifiers rather than fragile heading links.
- Record relationship type and rationale.
- Detect orphaned and stale relationships automatically where practical.

Required evidence

- Traceability graph or matrix
- Coverage report
- Sample traces

Assessment procedure

- **Examine:** Trace selected obligations end to end.
- **Interview:** Modify a requirement in a test environment and verify affected artifacts are identified.
- **Test:** Review unexplained orphan nodes.

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 29148:2018 — traceability

NORMATIVE CONTROL

MYTHOS-FND-DOC-10 – Security, privacy, and risk documentation

FAMILY	PROFILES	FAILURE IMPACT	AUTOMATION POTENTIAL
Security and risk	Foundational, Advanced, High Assurance	Critical	Partial

Requirement

Systems handling material risk MUST maintain current security architecture, threat and abuse models, data classifications, authorization rules, privacy assessments, exception records, incident procedures, and risk ownership appropriate to scope.

Purpose

Ensures security and privacy decisions are reviewable, operationally usable, and connected to implementation.

Applicability

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

Implementation guidance

- Avoid duplicating secrets or sensitive exploitation details in broadly accessible documentation.
- Classify and access-control sensitive artifacts.
- Link mitigations to controls and tests.

Required evidence

- Security and privacy document set
- Access controls
- Threat-to-test traceability

Assessment procedure

- **Examine:** Examine completeness against risk.
- **Interview:** Verify sensitive documentation access.
- **Test:** Trace sampled threats to implementation and validation.

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 Rev. 5 — PL, RA, CA families

NORMATIVE CONTROL

MYTHOS-FND-DOC-11 – Test strategy and evidence documentation

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

Requirement

The organization MUST document verification and validation strategy, test scope, environments, data, expected results, limitations, evidence provenance, and disposition of failures for release-relevant requirements.

Purpose

Prevents pass claims without reproducible context and distinguishes planned testing from executed evidence.

Applicability

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

Implementation guidance

- Separate test design from execution evidence.
- Preserve tool versions, configuration, timestamps, and artifact hashes for high-impact evidence.
- Document known blind spots and nondeterminism.

Required evidence

- Test strategy
- Test catalog
- Evidence bundles and failure records

Assessment procedure

- **Examine:** Reproduce a sampled test from documentation.
- **Interview:** Verify failed results cannot be overwritten without history.
- **Test:** Compare release claims with evidence.

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 800-53A Rev. 5 — assessment evidence

NORMATIVE CONTROL

MYTHOS-FND-DOC-12 – Actionable runbooks and operational documentation

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

Requirement

Critical operational procedures MUST document trigger, preconditions, safety warnings, detection, diagnosis, action, verification, rollback or recovery, escalation, evidence preservation, and last exercise date.

Purpose

Makes operations repeatable under stress and reduces dependence on individual memory.

Applicability

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

Implementation guidance

- Write steps around observable conditions rather than assumed causes.
- Include permissions and blast-radius warnings.
- Exercise high-impact runbooks through simulation, game day, or live use at defined intervals.

Required evidence

- Runbooks
- Exercise records
- Post-use improvements

Assessment procedure

- **Examine:** Observe an operator use a sampled runbook.
- **Interview:** Verify rollback and escalation paths.
- **Test:** Review stale or never-exercised procedures.

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 — incident response documentation

NORMATIVE CONTROL

MYTHOS-FND-DOC-13 – Release documentation and evidence manifest

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

Requirement

Each governed release MUST include release notes, known limitations, compatibility and migration information, security and quality status, deployment and rollback instructions, evidence references, and an immutable manifest of released artifacts.

Purpose

Supports safe adoption, reproducibility, support, audit, and rollback.

Applicability

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

Implementation guidance

- Distinguish user-visible changes from internal changes.
- Identify deprecated and removed behavior.
- Hash or sign evidence and artifacts for higher-assurance releases.

Required evidence

- Release notes
- Release manifest
- Artifact and evidence hashes

Assessment procedure

- **Examine:** Verify a deployed artifact matches the manifest.
- **Interview:** Trace a release statement to evidence.
- **Test:** Test rollback instructions in a representative environment.

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 — produce well-secured releases

NORMATIVE CONTROL

MYTHOS-FND-DOC-14 – Audience-appropriate user information

FAMILY	PROFILES	FAILURE IMPACT	AUTOMATION POTENTIAL
Users	Foundational, Advanced, High Assurance	Material	Manual

Requirement

User, administrator, operator, developer, and support documentation MUST address the tasks, permissions, risks, failure modes, and recovery needs of each applicable audience without assuming internal implementation knowledge.

Purpose

Reduces misuse, unsafe operation, support burden, and exclusion caused by documentation written only for builders.

Applicability

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

Implementation guidance

- Use task-oriented structure.
- Clearly distinguish warnings, prerequisites, expected results, and troubleshooting.
- Evaluate accessibility, localization, and reading context.

Required evidence

- Audience map
- Published user information
- Usability and retrieval test results

Assessment procedure

- **Examine:** Ask representative users to complete tasks using documentation.
- **Interview:** Review support cases for documentation gaps.
- **Test:** Verify inaccessible or privileged steps are labeled.

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 26514:2022 — information for users

NORMATIVE CONTROL

MYTHOS-FND-DOC-15 – Documentation-as-code controls

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

Requirement

Documentation stored with or governing software and infrastructure SHOULD be version-controlled, reviewed, linted, link-checked, rendered reproducibly, and validated in delivery workflows before merge or release.

Purpose

Applies engineering controls to documentation and catches structural defects before publication.

Applicability

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

Implementation guidance

- Validate metadata, identifiers, terminology, references, links, schemas, and generated outputs.
- Use protected branches or equivalent review controls for authoritative documents.
- Keep build tooling and dependencies pinned where reproducibility matters.

Required evidence

- Repository history
- CI results
- Publication build manifest

Assessment procedure

- **Examine:** Introduce a controlled documentation error and verify detection.
- **Interview:** Review bypass privileges.
- **Test:** Reproduce a published artifact from source.

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 — protect software and development artifacts

NORMATIVE CONTROL

MYTHOS-FND-DOC-16 – Generated-documentation boundaries

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

Requirement

Generated documentation MUST identify its authoritative source, generation method, timestamp or version, and overwrite policy; generated output MUST NOT be manually edited when regeneration would discard or conceal the change.

Purpose

Prevents divergence between code or schema authority and human-modified generated copies.

Applicability

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

Implementation guidance

- Mark generated files prominently.
- Fail generation when source and output are inconsistent if output is committed.
- Place authored commentary in supported extension points.

Required evidence

- Generator configuration
- Generated-file headers
- Drift check results

Assessment procedure

- **Examine:** Modify generated output and verify drift detection.
- **Interview:** Trace a generated claim to source.
- **Test:** Confirm manual extension points survive regeneration.

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 26514:2022 — information development

NORMATIVE CONTROL

MYTHOS-FND-DOC-17 – Safe machine and AI consumption

FAMILY	PROFILES	FAILURE IMPACT	AUTOMATION POTENTIAL
Machine consumption	Advanced, High Assurance	Critical	High

Requirement

Documentation supplied to search, retrieval, automation, or AI systems MUST preserve authority, status, provenance, access controls, supersession, and citation metadata, and MUST prevent unauthorized material from being promoted as trusted context.

Purpose

Reduces hallucination, stale guidance, data leakage, and automation based on non-authoritative content.

Applicability

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

Implementation guidance

- Index document sections with stable IDs and source metadata.
- Apply access control before retrieval, not only after generation.
- Prefer authoritative current material and expose uncertainty or conflicts.
- Evaluate retrieval and citation quality with representative tasks.

Required evidence

- Ingestion policy
- Retrieval test corpus
- Access-control and citation results

Assessment procedure

- **Examine:** Query known conflicting or superseded material.
- **Interview:** Test unauthorized retrieval attempts.
- **Test:** Measure whether generated answers cite the correct current authority.

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 AI RMF 1.0 — Map and Measure
- NIST AI 600-1 — content provenance and information integrity

NORMATIVE CONTROL

MYTHOS-FND-DOC-18 – Documentation quality and drift management

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

Requirement

The organization MUST monitor material documentation defects, unresolved gaps, broken references, stale ownership, retrieval failures, and documented-versus-actual drift, with severity, ownership, remediation targets, and escalation.

Purpose

Turns documentation quality into an observable operational concern rather than an occasional cleanup activity.

Applicability

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

Implementation guidance

- Prioritize defects that could cause unsafe actions, invalid compliance claims, or failed recovery.
- Use production incidents and support trends as documentation signals.
- Publish known gaps rather than concealing them.

Required evidence

- Documentation quality dashboard
- Defect and gap register
- Drift remediation records

Assessment procedure

- **Examine:** Review aging and severity trends.
- **Interview:** Sample closed defects for verified correction.
- **Test:** Compare selected documentation claims to live system evidence.

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 26514:2022 — quality management

FOUNDATION STANDARD / STRUCTURAL PART

Part V – Implementation and Operations

24. Implementation Profiles

Profile	Required Operating State
Baseline	Canonical metadata, owner, status, authoritative map, essential architecture, interface, runbook, release, and user documentation.
Enterprise	Documentation-as-code, automated link and freshness checks, traceability graph, generated-content controls, audience portals, and review dashboards.
High Assurance	Independent source validation, signed release documentation, protected evidence, controlled machine corpus, formal document baselines, and continuous drift detection.

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

- Treating chat transcripts as authoritative documentation
- Maintaining duplicate current documents without precedence
- Publishing generated text without provenance or review
- Runbooks that describe goals but not executable steps
- Architecture diagrams without version or scope
- Deleting superseded decisions instead of preserving history

30. Adoption Roadmap from Source Draft

- Define the authority model, metadata schema, repository structure, and documentation map.

- Establish required documentation profiles and stable identifiers for requirements, decisions, contracts, tests, and runbooks.
- Add documentation-as-code checks, link validation, ownership enforcement, and lifecycle statuses.
- Implement traceability, generated-document boundaries, release evidence, and runbook exercises.
- For Advanced and High Assurance adoption, add structured schemas, signed evidence, retrieval evaluation, and continuous drift detection.

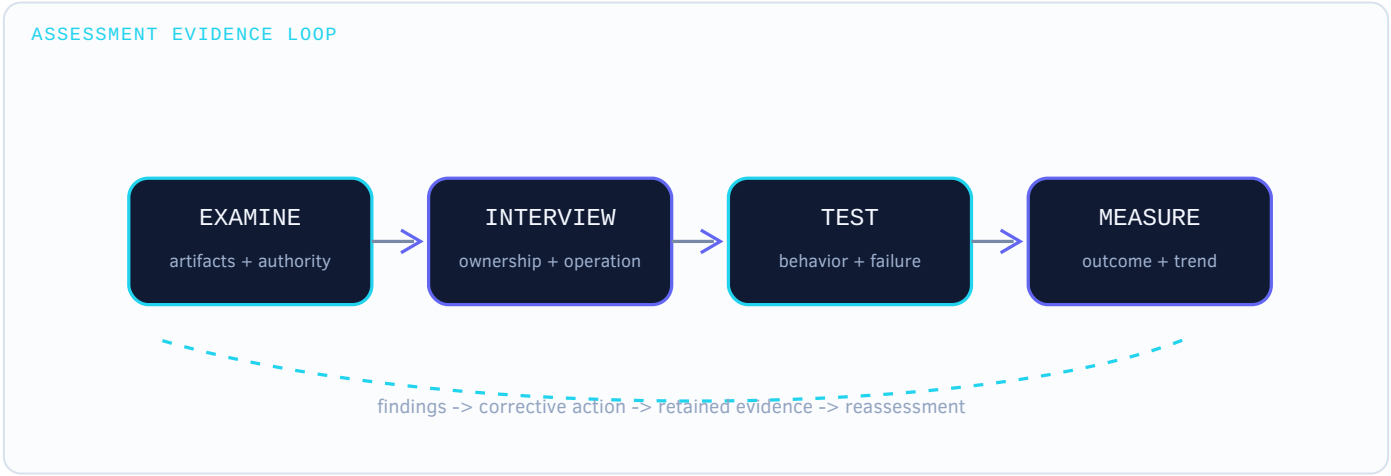
31. Limitations and Residual Risk from Source Draft

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
Authoritative-document coverage	Required document classes with current approved owners and status	100% for selected profile
Broken trace links		0 critical; declining total

Metric	Definition	Expected use or target
	Invalid or unresolved references among requirements, decisions, contracts, tests, and releases	
Documentation drift age	Time between material system change and authoritative documentation reconciliation	Defined per risk; continuous or release-bound for High Assurance
Runbook exercise rate	Critical runbooks exercised within their required interval	100%
Retrieval success	Representative users able to locate the authoritative answer without escalation	>= 90% in sampled tasks

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.

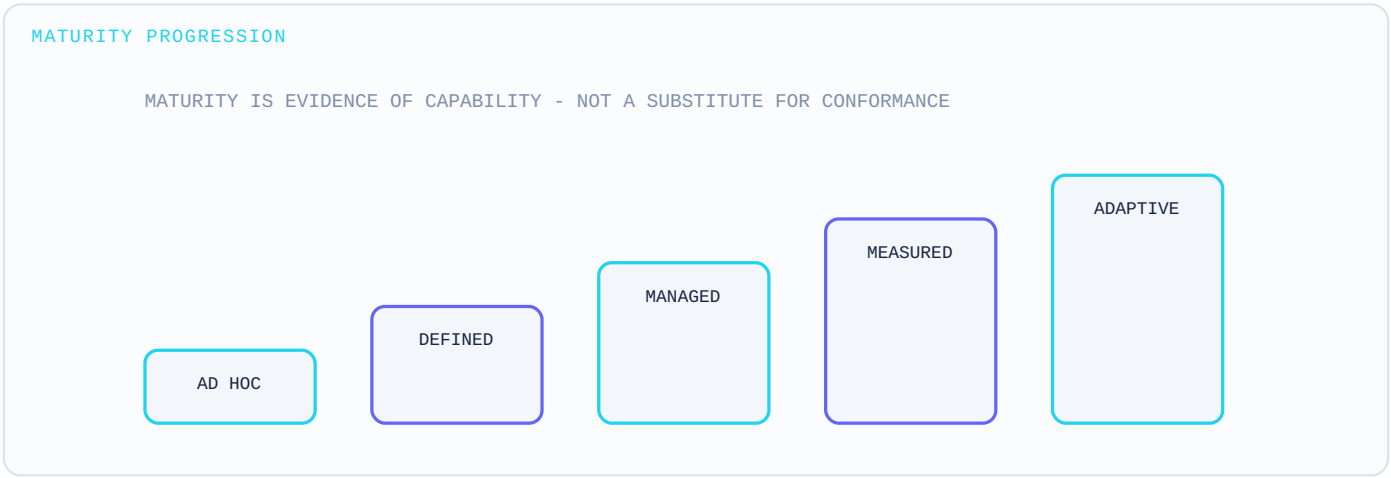
34. Exceptions and Compensating Controls

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
documents with current owner and review date	Defined by the adopting organization with owner, source, target, and cadence.
authoritative information classes with one designated source	Defined by the adopting organization with owner, source, target, and cadence.
broken references	Defined by the adopting organization with owner, source, target, and cadence.
superseded documents still presented as current	Defined by the adopting organization with owner, source, target, and cadence.
documented decisions linked to implementation	Defined by the adopting organization with owner, source, target, and cadence.
runbooks validated through exercise	Defined by the adopting organization with owner, source, target, and cadence.
generated claims without source pointers	Defined by the adopting organization with owner, source, target, and cadence.
documentation drift findings unresolved beyond target	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
ISO/IEC/IEEE 15288:2023	System life cycle information and processes	https://www.iso.org/standard/81702.html	Published	2026-09-17
ISO/IEC/IEEE 29148:2018	Requirements information items	https://www.iso.org/standard/72089.html	Published	2026-09-17
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
RFC 2119	Requirements language	https://www.rfc-editor.org/rfc/rfc2119	BCP 14	2026-09-17
RFC 8174	Uppercase requirements language clarification	https://www.rfc-editor.org/rfc/rfc8174	BCP 14	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

- Preserves the source draft's authority classes, documentation map, ADR discipline, runbook structure, traceability, and documentation-as-code requirements.
- Replaces mandatory AI-assistant scripts with a general machine-consumption protocol and explicit trust boundaries.
- Consolidates overlapping repository-layout advice into profile-based requirements.
- Adds assessment procedures, evidence quality, retrieval evaluation, and measurable drift 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-DOC-01	Governance	Documentation authority model	Foundational, Advanced, High Assurance	Partial	Critical
MYTHOS-FND-DOC-02	Metadata	Canonical metadata and identity	Foundational, Advanced, High Assurance	High	Material
MYTHOS-FND-DOC-03	Discovery	Authoritative documentation map	Foundational, Advanced, High Assurance	High	Material
MYTHOS-FND-DOC-04	Profiles	Risk-based documentation profile	Foundational, Advanced, High Assurance	Partial	Material
MYTHOS-FND-DOC-05	Lifecycle	Status, review, and supersession lifecycle	Foundational, Advanced, High Assurance	High	Critical
MYTHOS-FND-DOC-06	Architecture	Architecture documentation and invariants	Foundational, Advanced, High Assurance	Partial	Critical
MYTHOS-FND-DOC-07	Decisions	Architecture and product decision records	Foundational, Advanced, High Assurance	Partial	Material
MYTHOS-FND-DOC-08	Contracts	Contract and interface documentation	Foundational, Advanced, High Assurance	High	Critical
MYTHOS-FND-DOC-09	Traceability	Documentation traceability graph	Advanced, High Assurance	High	Critical
MYTHOS-FND-DOC-10	Security and risk	Security, privacy, and risk documentation	Foundational, Advanced, High Assurance	Partial	Critical

Control	Family	Title	Profiles	Automation	Impact
MYTHOS-FND-DOC-11	Verification	Test strategy and evidence documentation	Foundational, Advanced, High Assurance	High	Critical
MYTHOS-FND-DOC-12	Operations	Actionable runbooks and operational documentation	Foundational, Advanced, High Assurance	Partial	Critical
MYTHOS-FND-DOC-13	Release	Release documentation and evidence manifest	Foundational, Advanced, High Assurance	High	Critical
MYTHOS-FND-DOC-14	Users	Audience-appropriate user information	Foundational, Advanced, High Assurance	Manual	Material
MYTHOS-FND-DOC-15	Automation	Documentation-as-code controls	Foundational, Advanced, High Assurance	High	Material
MYTHOS-FND-DOC-16	Generation	Generated-documentation boundaries	Foundational, Advanced, High Assurance	High	Material
MYTHOS-FND-DOC-17	Machine consumption	Safe machine and AI consumption	Advanced, High Assurance	High	Critical
MYTHOS-FND-DOC-18	Quality	Documentation quality and drift management	Foundational, Advanced, High Assurance	High	Critical

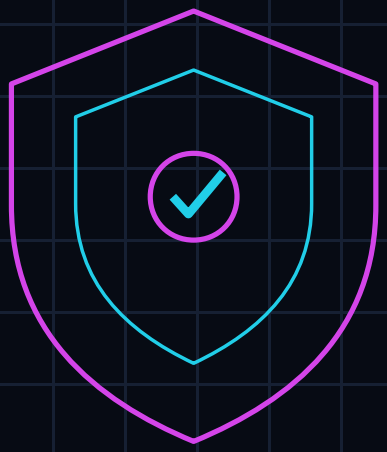
Appendix D – Minimum Conformance Claim Record

```
standard: MYTHOS-FND-0002
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



CANDIDATE STANDARD

Mythos Security, Privacy, and Trust Standard

Engineer security, privacy, and trust as system properties with explicit authority, isolation, evidence, and resilience.

PERMANENT ID
MYTHOS-FND-0003

PUBLICATION CLASS
CANDIDATE STANDARD

VERSION / STATUS
1.0.0-candidate / CANDIDATE

PERMANENT PUBLICATION IDENTITY

Mythos Security, Privacy, and Trust Standard

Universal Requirements for Risk Governance, Secure Architecture, Identity, Data Protection, Privacy, Resilience, Supply Chain, and Continuous Assurance

Document ID
MYTHOS-FND-0003

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	19	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	Security and privacy leaders; Engineers and architects; Product and data owners; Operations and incident response teams; Risk managers, assessors, and auditors
Publisher / owner	Mythos Systems / Standards Program
Public classification	Public technical standard
Canonical route	/library/standards/foundation/mythos-fnd-0003/

Expected outcomes

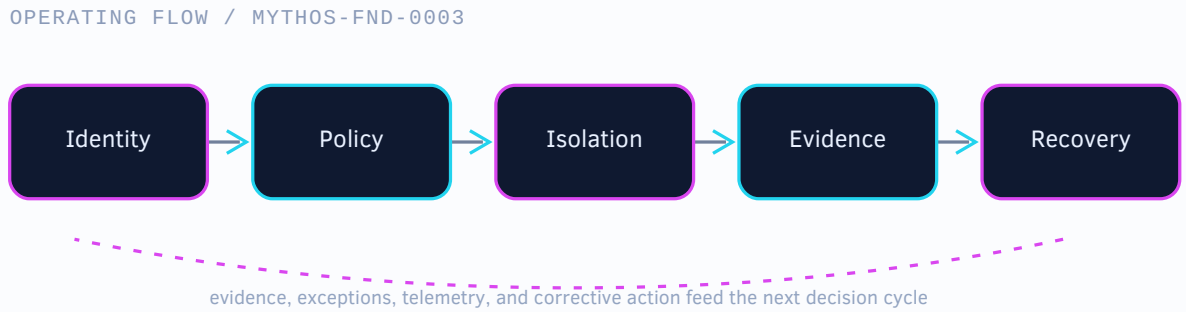
- Embed security, privacy, and trust outcomes throughout system and organizational lifecycles.
- Constrain authority, exposure, data use, and blast radius through explicit boundaries and least privilege.
- Protect software and dependency supply chains and preserve evidence needed for assurance and incident response.
- Make controls testable, continuously observable where practical, and proportionate to consequence.

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.

Document Control 8

Revision Record 8

How to Use This Standard 9

Executive Reading Path 9

Engineering Reading Path 9

Assessment Reading Path 9

Normative and Informative Content 9

Part I – Executive Direction 10

1. Executive Overview 10

2. Executive Findings and Required Direction 10

3. Business and Operational Impact 10

4. Target-State Summary 11

5. Leadership Responsibilities 12

Part II – Standard Foundation 13

6. Purpose and Objectives 13

7. Scope 13

8. Intended Audience 13

9. Requirements Language and Conformance 13

10. Normative References from Source Draft 13

11. Informative References from Source Draft 14

12. Terms and Definitions 14

13. Applicability and Tailoring 15

Part III – Risk and Architecture 16

14. Enterprise Problem and Risk Landscape 16

15. Governing Principles 16

16. Reference Operating Architecture 16

17. Roles and Accountability 17

18. State, Evidence, and Decision Model 18

19. Security and Trust Considerations 18

20. Failure Modes 18

21. Cross-Functional Dependencies 18

Part IV – Normative Control System **19**

22. Control-Family Overview 19

23. Normative Controls 20

Part V – Implementation and Operations **47**

24. Implementation Profiles 47

25. Implementation Lifecycle 47

26. Integration Requirements 48

27. Failure Handling and Recovery 48

28. Exceptions and Compensating Controls 48

29. Prohibited Practices 48

30. Adoption Roadmap from Source Draft 48

31. Limitations and Residual Risk from Source Draft 49

Part VI – Assurance and Assessment **50**

32. Assessment Methodology 50

33. Metrics and Reporting from Source Draft 50

34. Exceptions and Compensating Controls 51

35. Enterprise Metric Set 51

36. Maturity Model 52

37. Assessment Confidence 52

38. Executive Assurance Dashboard 52

Part VII – Authority and Traceability **54**

39. Cross-Standard Dependencies from Source Draft 54

40. Current External Authority Register 54

41. Control Traceability 54

42. Source-Draft Preservation 55

Part VIII – Appendices **56**

Appendix A — Source-Draft Evolution Notes 56

Appendix B — Change History 56

Appendix C — Control Summary 56

Appendix D — Minimum Conformance Claim Record 57

Appendix E — Publication Review Checklist 57

NORMATIVE SYSTEM

Control index

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

MYTHOS-FND-SPT-01	Integrated security, privacy, and trust governance	21
MYTHOS-FND-SPT-02	Security architecture and invariants	22
MYTHOS-FND-SPT-03	Threat, abuse, and misuse modeling	23
MYTHOS-FND-SPT-04	Asset, data, and capability classification	24
MYTHOS-FND-SPT-05	Strong identity and authentication	25
MYTHOS-FND-SPT-06	Least privilege and explicit delegation	26
MYTHOS-FND-SPT-07	Secrets, certificates, and key lifecycle	27
MYTHOS-FND-SPT-08	Approved cryptography and crypto-agility	28
MYTHOS-FND-SPT-09	Purpose limitation, minimization, and consent	29
MYTHOS-FND-SPT-10	Retention, deletion, and export protection	30
MYTHOS-FND-SPT-11	Tenant, workload, and execution isolation	31
MYTHOS-FND-SPT-12	Secure design and implementation lifecycle	32
MYTHOS-FND-SPT-13	Software and service supply-chain integrity	34
MYTHOS-FND-SPT-14	Security logging, audit, and evidence integrity	36
MYTHOS-FND-SPT-15	Vulnerability and exposure management	38
MYTHOS-FND-SPT-16	Incident response and emergency authority	39
MYTHOS-FND-SPT-17	Backup, recovery, and continuity assurance	41
MYTHOS-FND-SPT-18	Third-party, AI, and delegated-action trust	43
MYTHOS-FND-SPT-19	Continuous control assurance and trust claims	45

Document Control

Field	Value
Document ID	MYTHOS-FND-0003
Standard	Security, Privacy, and Trust
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

Security, privacy, and trust cannot be added after architecture decisions have already established identity, data, execution, and dependency boundaries. This standard defines a unified governance and engineering system for protecting organizational operations, users, data, software, infrastructure, and delegated machine action while avoiding unsupported claims of security, privacy, sovereignty, or compliance.

The institutional objective is to integrate security, privacy, resilience, cryptography, identity, supply-chain integrity, evidence, and trust claims across the full system lifecycle. 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
Fragmented governance	Security, privacy, resilience, and AI trust are often managed as disconnected reviews.	Use one integrated risk and control model with accountable ownership.
Ambient authority	Users, workloads, agents, and integrations often inherit broader access than necessary.	Use explicit identity, least privilege, constrained delegation, and expiring grants.
Secrets and cryptography debt	Long-lived credentials and algorithm lock-in create systemic exposure.	Broker secrets, rotate credentials, maintain cryptographic inventory, and design for agility.
Supply-chain opacity	Organizations cannot reliably prove what entered a release.	Require provenance, SBOMs, signing, dependency policy, and verified build controls.
Trust claims without evidence	Products claim privacy, locality, security, or compliance without bounded proof.	Define claim scope, evidence, limitations, and review triggers.

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.

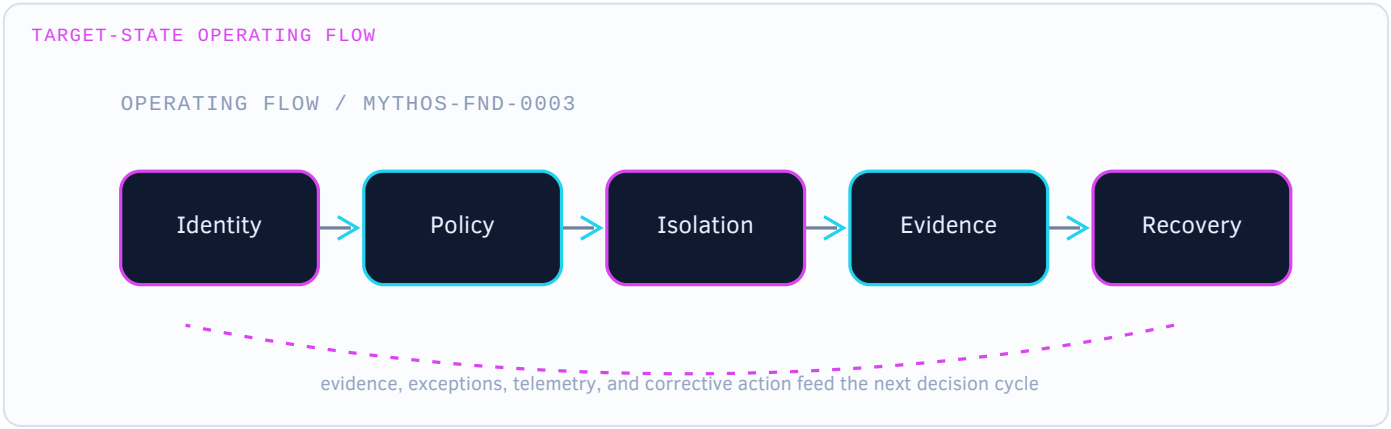
3.3 Security, Privacy, and Trust Impact

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	Integrated governance and risk model
2	Security architecture and invariants
3	Threat, abuse, and misuse modeling
4	Asset, data, and capability classification
5	Human and workload identity
6	Authorization and delegation
7	Secrets, certificates, keys, and cryptographic agility
8	Privacy purpose, minimization, consent, retention, deletion, and export
9	Isolation and sandboxing
10	Secure development and supply chain
11	Logging, audit, and evidence integrity
12	Vulnerability and exposure management
13	Incident and emergency authority
14	Backup, recovery, and continuity

#	Target-State Component
15	Third-party and AI trust
16	Continuous assurance and trust-claim registry

```
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
Board or executive risk owner	Sets risk appetite and receives material trust reporting.
Chief information security officer	Owns security governance and enterprise control outcomes.
Privacy officer	Owns privacy risk, lawful use, rights, retention, and disclosure.
Security architect	Defines trust boundaries, identity, cryptography, isolation, and invariants.
Product and service owners	Implement controls and accept residual risk within delegated authority.
Incident commander	Coordinates containment, communication, recovery, and evidence.
Supply-chain owner	Maintains provenance, dependency, and supplier assurance.
Independent assessor	Tests design and operating effectiveness.

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

- Embed security, privacy, and trust outcomes throughout system and organizational lifecycles.
- Constrain authority, exposure, data use, and blast radius through explicit boundaries and least privilege.
- Protect software and dependency supply chains and preserve evidence needed for assurance and incident response.
- Make controls testable, continuously observable where practical, and proportionate to consequence.

7. Scope

Applies to all systems that process organizational or user data, connect to networks, execute code, expose interfaces, delegate authority, integrate third parties, or affect operational, financial, safety, privacy, legal, or mission outcomes.

8. Intended Audience

- Security and privacy leaders
- Engineers and architects
- Product and data owners
- Operations and incident response teams
- Risk managers, assessors, and auditors

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 CSWP 29** — The NIST Cybersecurity Framework (CSF) 2.0. https://doi.org/10.6028/NIST.CSWP.29
- **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
- **NIST SP 800-53A Rev. 5, Release 5.2.0** — Assessing Security and Privacy Controls in Information Systems and Organizations. https://csrc.nist.gov/pubs/sp/800/53/a/r5/final
- **NIST SP 800-218 v1.1** — Secure Software Development Framework (SSDF). https://csrc.nist.gov/pubs/sp/800/218/final
- **NIST SP 800-207** — Zero Trust Architecture. https://doi.org/10.6028/NIST.SP.800-207
- **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 800-61 Rev. 3** — Incident Response Recommendations and Considerations for Cybersecurity Risk Management. https://csrc.nist.gov/pubs/sp/800/61/r3/final
- **NIST Privacy Framework 1.0** — A Tool for Improving Privacy through Enterprise Risk Management. https://www.nist.gov/privacy-framework/privacy-framework
- **CISA CPG 2.0** — Cross-Sector Cybersecurity Performance Goals 2.0. https://www.cisa.gov/cybersecurity-performance-goals-2-0-cpg-2-0
- **CIS Controls v8.1** — CIS Critical Security Controls. https://www.cisecurity.org/controls/v8-1
- **OWASP ASVS** — Application Security Verification Standard. https://owasp.org/www-project-application-security-verification-standard/
- **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/

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.

Term	Definition
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.
Ambient authority	Permission available to code or a principal without an explicit, scoped delegation for the current action.
Trust boundary	A transition where identity, authority, data sensitivity, integrity, execution context, or control ownership changes.
Security invariant	A condition that must remain true to maintain the intended security or privacy posture.
Cryptographic agility	The ability to inventory, replace, configure, and retire cryptographic mechanisms without uncontrolled system redesign.
Trust claim	A statement about identity, integrity, provenance, authorization, safety, privacy, or control effectiveness that requires evidence.

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.

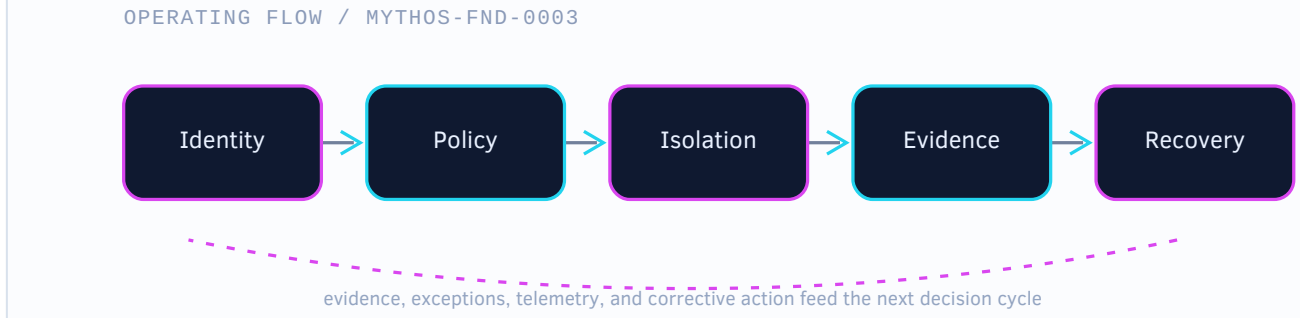
Adopting organizations SHOULD maintain a domain-specific risk register that identifies cause, affected asset or stakeholder, credible scenario, impact, existing controls, residual risk, owner, review trigger, and evidence. Risks that cross standards MUST be linked rather than copied into disconnected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

15. Governing Principles

- Deny by default and grant the minimum authority for the minimum time.
- Local, internal, signed, or vendor-provided does not automatically mean trusted.
- Trust boundaries and security invariants must be explicit and testable.
- Sensitive data collection and processing must be minimized and purpose-bound.
- Security controls must fail safely and remain operable during degradation.
- All material authority must be revocable, observable, and attributable.
- Claims of security or privacy require bounded evidence, not confidence language.

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
Board or executive risk owner	Sets risk appetite and receives material trust reporting.
Chief information security officer	Owns security governance and enterprise control outcomes.
Privacy officer	Owns privacy risk, lawful use, rights, retention, and disclosure.
Security architect	Defines trust boundaries, identity, cryptography, isolation, and invariants.
Product and service owners	Implement controls and accept residual risk within delegated authority.
Incident commander	Coordinates containment, communication, recovery, and evidence.
Supply-chain owner	Maintains provenance, dependency, and supplier assurance.
Independent assessor	Tests design and operating effectiveness.

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
Security approval based only on a checklist	Failure can create hidden risk, misleading assurance, uncontrolled cost, or unsafe operation.
Storing credentials in model or agent context	Failure can create hidden risk, misleading assurance, uncontrolled cost, or unsafe operation.
Calling a system zero trust, private, sovereign, or post-quantum without bounded evidence	Failure can create hidden risk, misleading assurance, uncontrolled cost, or unsafe operation.
Relying on network location as identity	Failure can create hidden risk, misleading assurance, uncontrolled cost, or unsafe operation.
Treating successful backup jobs as proof of recoverability	Failure can create hidden risk, misleading assurance, uncontrolled cost, or unsafe operation.
Allowing extensions or agents ambient access	Failure can create hidden risk, misleading assurance, uncontrolled cost, or unsafe operation.

21. Cross-Functional Dependencies

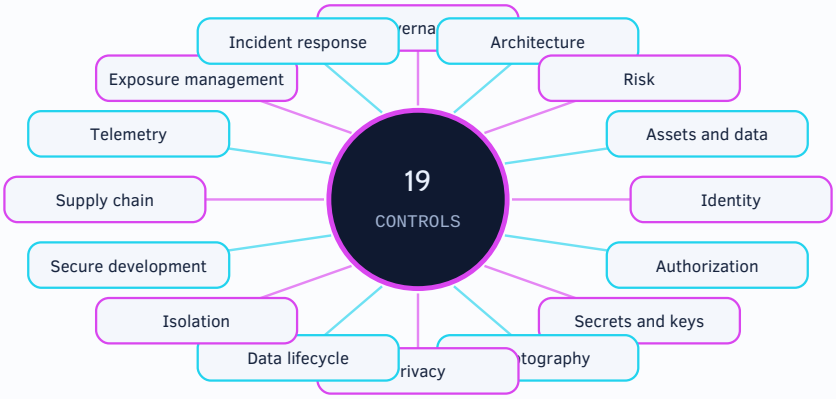
This Foundation standard depends on the remaining MYTHOS-FND standards for documentation, security and trust, quality, operations, data and integration, interfaces, extensions, AI-first behavior, and agentic orchestration. An adopting organization MUST resolve overlapping requirements through the stricter 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 **19 controls** across the following families:

- Governance
- Architecture
- Risk
- Assets and data
- Identity
- Authorization
- Secrets and keys
- Cryptography
- Privacy
- Data lifecycle
- Isolation
- Secure development
- Supply chain
- Telemetry
- Exposure management
- Incident response
- Resilience
- Third parties and automation

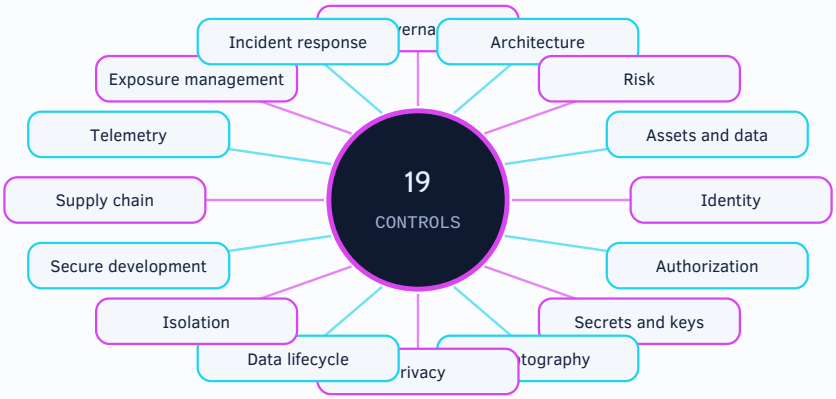
- Assurance

23. Normative Controls

CONTROL SET	PROFILES	ASSESSMENT
19	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-SPT-01 – Integrated security, privacy, and trust governance

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

Requirement

The organization MUST assign accountable ownership for security, privacy, and trust outcomes; define risk appetite and escalation; and integrate these concerns into product, architecture, procurement, release, operations, and retirement decisions.

Purpose

Prevents fragmented control ownership and late-stage risk discovery.

Applicability

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

Implementation guidance

- Define decision rights and separation of duties.
- Maintain an integrated risk register linked to systems, data, suppliers, and controls.
- Require material residual risk to be accepted by an authority with appropriate business accountability.

Required evidence

- Governance charter
- Risk appetite and escalation criteria
- Sample risk decisions

Assessment procedure

- **Examine:** Examine ownership and decision records.
- **Interview:** Interview accountable leaders and implementers.
- **Test:** Trace material risk from discovery through disposition.

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 CSF 2.0 — Govern
- NIST SP 800-53 — PM and RA families

NORMATIVE CONTROL

MYTHOS-FND-SPT-02 – Security architecture and invariants

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

Requirement

Each in-scope system MUST document and enforce security and privacy architecture, including assets, principal types, data flows, trust boundaries, control planes, privileged paths, failure domains, dependencies, and security invariants.

Purpose

Makes consequential boundaries and assumptions reviewable and testable.

Applicability

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

Implementation guidance

- Model normal, degraded, administrative, recovery, support, and update paths.
- Identify authoritative policy and identity decision points.
- Link invariants to automated tests or monitoring where feasible.

Required evidence

- Security architecture
- Trust-boundary diagrams
- Invariant tests

Assessment procedure

- **Examine:** Trace privileged and sensitive workflows.
- **Interview:** Compare documented controls with deployment.
- **Test:** Attempt to violate selected invariants in a controlled environment.

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 800-160 Vol. 1 Rev. 1
- NIST SP 800-207

NORMATIVE CONTROL

MYTHOS-FND-SPT-03 – Threat, abuse, and misuse modeling

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

Requirement

The organization MUST identify credible threats, abuse cases, misuse, privacy harms, dependency failures, insider scenarios, and recovery risks before release and after material change.

Purpose

Expands analysis beyond accidental defects and externally initiated attacks.

Applicability

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

Implementation guidance

- Record actor or cause, preconditions, affected assets, attack or failure path, impact, detection, mitigations, validation, and residual risk.
- Include supply-chain, administrative, cross-tenant, automation, AI, and support-channel scenarios where applicable.
- Prioritize by consequence and plausibility without treating low probability as zero risk.

Required evidence

- Threat and abuse model
- Risk treatment links
- Validation records

Assessment procedure

- **Examine:** Review scenario completeness against architecture.
- **Interview:** Conduct structured challenge or threat-model workshop.
- **Test:** Test one high-impact scenario end to end.

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 — RA-3
- NIST AI RMF — Map

NORMATIVE CONTROL

MYTHOS-FND-SPT-04 – Asset, data, and capability classification

FAMILY	PROFILES	FAILURE IMPACT	AUTOMATION POTENTIAL
Assets and data	Foundational, Advanced, High Assurance	Critical	High

Requirement

Assets, data, credentials, models, tools, interfaces, and executable capabilities MUST be classified by sensitivity, criticality, integrity, availability, privacy, provenance, retention, and authority requirements.

Purpose

Enables controls to follow the actual value and consequence of resources.

Applicability

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

Implementation guidance

- Classify unknown data conservatively until resolved.
- Propagate classification through derived data, backups, caches, logs, exports, and model context.
- Associate handling rules and owners with each class.

Required evidence

- Classification policy
- Inventories and data maps
- Handling-rule tests

Assessment procedure

- **Examine:** Sample assets and trace classification through processing.
- **Interview:** Test enforcement of handling rules.
- **Test:** Review unclassified or ownerless resources.

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 — RA-2, MP family
- NIST Privacy Framework — Data Processing Management

NORMATIVE CONTROL

MYTHOS-FND-SPT-05 – Strong identity and authentication

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

Requirement

Every human, workload, device, service, agent, extension, and administrative process exercising material authority MUST have a distinct, verifiable identity and authentication strength proportionate to risk.

Purpose

Prevents shared, ambiguous, or weakly authenticated authority and supports attribution and revocation.

Applicability

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

Implementation guidance

- Prefer phishing-resistant authentication for privileged and high-impact access.
- Use short-lived workload credentials and avoid embedded static secrets.
- Define session binding, reauthentication, device posture, and recovery requirements.

Required evidence

- Identity inventory
- Authentication configuration
- Credential and session test results

Assessment procedure

- **Examine:** Attempt shared or anonymous privileged access.
- **Interview:** Verify credential lifetime and revocation.
- **Test:** Review authentication recovery for bypass risk.

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 family
- CISA CPG 2.0 — account security

NORMATIVE CONTROL

MYTHOS-FND-SPT-06 – Least privilege and explicit delegation

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

Requirement

Authorization decisions MUST be deny-by-default, evaluated at authoritative enforcement points, scoped to the requested action and resource, and based on explicit policy, current identity, context, and delegated authority.

Purpose

Constrains blast radius and prevents frontend-only, ambient, stale, or transitive privilege.

Applicability

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

Implementation guidance

- Separate authentication from authorization.
- Model permissions as narrowly as operationally practical.
- Require step-up or additional approval for high-impact actions.
- Invalidate cached decisions when relevant identity or policy state changes.

Required evidence

- Authorization policy
- Decision logs
- Negative and escalation-path tests

Assessment procedure

- **Examine:** Attempt unauthorized direct calls bypassing the interface.
- **Interview:** Test revocation and policy-change propagation.
- **Test:** Review wildcard and inherited permissions.

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 family
- NIST SP 800-207

NORMATIVE CONTROL

MYTHOS-FND-SPT-07 – Secrets, certificates, and key lifecycle

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

Requirement

Secrets, private keys, certificates, tokens, and recovery material MUST be inventoried, protected outside ordinary source and logs, issued to specific identities and purposes, rotated or renewed, revocable, and monitored for exposure.

Purpose

Reduces credential theft, uncontrolled reuse, and long-lived compromise.

Applicability

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

Implementation guidance

- Broker access rather than distributing raw secrets where feasible.
- Separate secret references from values.
- Define emergency rotation and dependent-system recovery.
- Validate certificate chains, names, purposes, and revocation.

Required evidence

- Secrets inventory
- Issuance and rotation records
- Exposure scanning and revocation tests

Assessment procedure

- **Examine:** Search code, artifacts, logs, and backups for sampled secrets.
- **Interview:** Revoke a test credential and verify denial.
- **Test:** Review ownership and age.

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-5, SC-12, SC-17

NORMATIVE CONTROL

MYTHOS-FND-SPT-08 – Approved cryptography and crypto-agility

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

Requirement

Cryptographic mechanisms MUST be selected from approved, context-appropriate algorithms and protocols; configured securely; inventoried with dependencies; and replaceable through a documented crypto-agility plan.

Purpose

Protects confidentiality and integrity while reducing migration risk from algorithm, library, protocol, or key compromise.

Applicability

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

Implementation guidance

- Inventory algorithm, mode, parameter, key source, library, protocol, data purpose, and owner.
- Prohibit silent downgrade and unauthenticated encryption.
- Plan migration for long-lived sensitive data and cryptographic dependencies, including post-quantum transition where risk warrants.

Required evidence

- Cryptographic inventory
- Configuration policy
- Migration and downgrade tests

Assessment procedure

- **Examine:** Scan deployments and artifacts for prohibited mechanisms.
- **Interview:** Test negotiation and downgrade behavior.
- **Test:** Review replacement feasibility for critical dependencies.

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-12 and SC-13
- NIST post-quantum cryptography program

NORMATIVE CONTROL

MYTHOS-FND-SPT-09 – Purpose limitation, minimization, and consent

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

Requirement

Personal and sensitive data processing MUST have a defined purpose and lawful or authorized basis, collect and retain only what is necessary, communicate material use, and prevent secondary use outside approved bounds.

Purpose

Reduces privacy harm, legal exposure, breach impact, and opaque data practices.

Applicability

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

Implementation guidance

- Perform privacy impact assessment proportionate to data and consequence.
- Avoid dark patterns and bundled consent.
- Minimize telemetry, prompts, model context, and support bundles.
- Provide meaningful controls and alternatives when consent is the basis.

Required evidence

- Data-purpose register
- Privacy assessment
- Consent and preference records

Assessment procedure

- **Examine:** Trace sampled fields to approved purposes.
- **Interview:** Test withdrawal or preference changes.
- **Test:** Review data used for new purposes or AI training.

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
- NIST SP 800-53 — PT and DM families

NORMATIVE CONTROL

MYTHOS-FND-SPT-10 – Retention, deletion, and export protection

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

Requirement

Data retention, archival, backup, export, and deletion MUST be governed by classification, purpose, obligation, recovery needs, and user or organizational commitments, with verifiable deletion semantics and secure export controls.

Purpose

Prevents indefinite accumulation, orphan data, insecure support bundles, and false deletion claims.

Applicability

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

Implementation guidance

- Define behavior across primary stores, replicas, caches, indexes, backups, logs, embeddings, and derived artifacts.
- Encrypt and authorize sensitive exports.
- Record residual retention caused by immutable backups or legal holds.

Required evidence

- Retention schedule
- Deletion and export tests
- Deletion evidence

Assessment procedure

- **Examine:** Delete a test subject or record and inspect downstream stores.
- **Interview:** Attempt unauthorized export.
- **Test:** Review expired data and orphaned storage.

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 — SI-12 and MP family
- NIST Privacy Framework — Disassociated Processing

NORMATIVE CONTROL

MYTHOS-FND-SPT-11 – Tenant, workload, and execution isolation

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

Requirement

Systems serving multiple tenants, trust domains, plugins, users, or workloads MUST enforce isolation across identity, authorization, compute, memory, storage, network, cache, telemetry, and administrative access.

Purpose

Prevents cross-boundary disclosure, influence, resource theft, and privilege escalation.

Applicability

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

Implementation guidance

- Bind tenant or trust-domain context at authoritative entry points.
- Use defense in depth rather than relying on a single query filter or process boundary.
- Test support and break-glass paths.
- Apply resource quotas and side-channel risk analysis where warranted.

Required evidence

- Isolation architecture
- Cross-boundary test results
- Administrative access records

Assessment procedure

- **Examine:** Attempt cross-tenant reads, writes, cache access, log access, and resource exhaustion.
- **Interview:** Review support impersonation controls.
- **Test:** Test context propagation under asynchronous execution.

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-4, SC-2, SC-7, SC-39

NORMATIVE CONTROL

MYTHOS-FND-SPT-12 – Secure design and implementation lifecycle

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

Requirement

Software, infrastructure, models, prompts, policies, and configuration MUST be developed through controlled environments using reviewed changes, secure coding practices, dependency controls, protected build processes, and security verification proportionate to risk.

Purpose

Reduces preventable defects and malicious or accidental compromise during creation and change.

Applicability

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

Implementation guidance

- Define security requirements and misuse cases early.
- Protect branches, build identities, signing keys, and release workflows.
- Use static, dynamic, composition, infrastructure, secret, and policy analysis as applicable.
- Require remediation or accepted exception before release.

Required evidence

- Development policy
- Change and review records
- Security test results

Assessment procedure

- **Examine:** Sample changes from requirement to release.
- **Interview:** Attempt bypass of required review or build controls.
- **Test:** Verify findings are dispositioned.

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
- OWASP ASVS

- OWASP SAMM

NORMATIVE CONTROL

MYTHOS-FND-SPT-13 – Software and service supply-chain integrity

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

Requirement

Critical dependencies, build inputs, artifacts, suppliers, services, models, extensions, and update channels MUST have verified identity, provenance, integrity, risk evaluation, vulnerability monitoring, and supported replacement or containment plans.

Purpose

Reduces compromise through upstream components, opaque services, malicious updates, and abandoned dependencies.

Applicability

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

Implementation guidance

- Generate and preserve SBOM or equivalent inventories.
- Verify signatures and provenance at admission and deployment.
- Assess maintainer health, licensing, concentration, transitive risk, and update practices.
- Define quarantine and revocation.

Required evidence

- SBOM and dependency inventory
- Provenance attestations
- Supplier and update risk records

Assessment procedure

- **Examine:** Verify artifact signatures and provenance.
- **Interview:** Introduce an unapproved dependency in a test pipeline.
- **Test:** Review response to a withdrawn or compromised package.

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
- SLSA 1.2

- SPDX 3.0
- CycloneDX 1.7
- Sigstore

NORMATIVE CONTROL

MYTHOS-FND-SPT-14 – Security logging, audit, and evidence integrity

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

Requirement

Material security, privacy, administrative, policy, data-access, execution, extension, model, and lifecycle events MUST produce attributable, time-synchronized, access-controlled, redacted, and integrity-protected records sufficient for detection, investigation, accountability, and assessment.

Purpose

Creates evidence for operational defense without turning logs into an uncontrolled sensitive-data store.

Applicability

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

Implementation guidance

- Define required events and fields.
- Exclude or tokenize secrets and unnecessary personal data.
- Protect audit configuration and monitor gaps.
- Use tamper-evident storage or signed evidence where consequence warrants.

Required evidence

- Logging specification
- Sample events
- Integrity, retention, and access tests

Assessment procedure

- **Examine:** Perform a privileged action and trace it end to end.
- **Interview:** Test redaction and audit-disable detection.
- **Test:** Verify clock and identity consistency.

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
- CISA CPG 2.0 — logging

NORMATIVE CONTROL

MYTHOS-FND-SPT-15 – Vulnerability and exposure management

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

Requirement

The organization MUST continuously identify, validate, prioritize, remediate, mitigate, or formally accept vulnerabilities and exposures across assets, software, infrastructure, identities, configurations, suppliers, and external attack surfaces.

Purpose

Focuses action on exploitable conditions and business impact rather than scanner volume alone.

Applicability

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

Implementation guidance

- Combine severity with reachability, exposure, exploitability, asset criticality, compensating controls, and threat evidence.
- Define remediation targets and emergency pathways.
- Verify fixes and detect recurrence.

Required evidence

- Asset and exposure inventory
- Findings and service-level records
- Remediation verification

Assessment procedure

- **Examine:** Sample findings across severity and age.
- **Interview:** Reproduce or validate selected exposures.
- **Test:** Test whether recurrence or reopened exposure is detected.

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 CSF 2.0 — ID.RA and PR.PS
- CIS Controls v8.1 — Continuous Vulnerability Management

NORMATIVE CONTROL

MYTHOS-FND-SPT-16 – Incident response and emergency authority

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

Requirement

The organization MUST maintain and exercise incident capabilities for detection, triage, containment, evidence preservation, eradication, recovery, communication, legal or privacy obligations, and post-incident improvement, including narrowly governed emergency authority.

Purpose

Reduces harm and decision paralysis during high-pressure events.

Applicability

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

Implementation guidance

- Define severity, roles, communications, external dependencies, and escalation.
- Pre-authorize reversible containment actions where delay is dangerous.
- Protect evidence chain of custody.
- Review incidents for control and documentation changes.

Required evidence

- Incident plan and playbooks
- Exercise and incident records
- Post-incident actions

Assessment procedure

- **Examine:** Run a scenario exercise.
- **Interview:** Verify emergency access is logged, time-bound, and reviewed.
- **Test:** Trace corrective actions to closure.

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
- NIST CSF 2.0 — Respond

NORMATIVE CONTROL

MYTHOS-FND-SPT-17 – Backup, recovery, and continuity assurance

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

Requirement

Critical services and data MUST have risk-based resilience, backup, recovery, and continuity strategies that protect integrity and confidentiality and are exercised against realistic failure, corruption, compromise, and dependency-loss scenarios.

Purpose

Ensures availability claims survive actual restoration and not merely backup-job success.

Applicability

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

Implementation guidance

- Define recovery time and recovery point objectives.
- Separate or immutably protect recovery assets from common compromise paths.
- Validate restored data and software integrity.
- Include supplier and identity-system failure.

Required evidence

- Continuity and recovery plans
- Restore exercise results
- Integrity validation

Assessment procedure

- **Examine:** Restore a representative system or dataset.
- **Interview:** Test access when primary identity or network services are unavailable.
- **Test:** Review unmet objectives and remediation.

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 CSF 2.0 — Recover
- NIST SP 800-53 — CP family

NORMATIVE CONTROL

MYTHOS-FND-SPT-18 – Third-party, AI, and delegated-action trust

FAMILY	PROFILES	FAILURE IMPACT	AUTOMATION POTENTIAL
Third parties and automation	Advanced, High Assurance	Critical	High

Requirement

External services, AI systems, agents, extensions, integrations, and automated decision or execution components MUST operate within explicit data, capability, identity, approval, observability, and revocation boundaries, and their outputs MUST NOT be treated as inherently trusted.

Purpose

Constrains opaque or probabilistic components and prevents delegated systems from silently expanding authority.

Applicability

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

Implementation guidance

- Validate outputs before consequential use.
- Broker tools and credentials through policy enforcement points.
- Maintain kill switches, provider exit paths, and degraded modes.
- Assess prompt injection, tool abuse, model change, data use, and provider retention where applicable.

Required evidence

- Delegation and capability policy
- Provider and component assessments
- Adversarial and revocation tests

Assessment procedure

- **Examine:** Attempt unauthorized tool use or data disclosure.
- **Interview:** Change or remove a provider and verify controlled degradation.
- **Test:** Review whether human accountability remains explicit.

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 AI RMF 1.0
- OWASP LLM Top 10 2025

- OWASP Agentic Applications Top 10 2026

NORMATIVE CONTROL

MYTHOS-FND-SPT-19 – Continuous control assurance and trust claims

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

Requirement

Material security, privacy, and trust claims MUST identify scope, conditions, evidence, assessment date, confidence, limitations, and residual risk; critical controls SHOULD be continuously or regularly verified for drift and effectiveness.

Purpose

Prevents broad claims such as secure, private, zero trust, compliant, or encrypted from exceeding the evidence.

Applicability

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

Implementation guidance

- Maintain evidence freshness requirements.
- Separate design evidence from operating-effectiveness evidence.
- Use independent assessment for high-impact claims.
- Withdraw or qualify claims when evidence expires or conditions change.

Required evidence

- Control evidence register
- Assessment reports
- Claim and limitation statements

Assessment procedure

- **Examine:** Challenge sampled trust claims.
- **Interview:** Verify evidence freshness and scope.
- **Test:** Induce a safe control drift and confirm detection.

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 800-53A Rev. 5
- NIST CSF 2.0 — Govern and Identify

FOUNDATION STANDARD / STRUCTURAL PART

Part V – Implementation and Operations

24. Implementation Profiles

Profile	Required Operating State
Baseline	Asset and data classification, strong identity, least privilege, secrets lifecycle, approved cryptography, privacy controls, secure development, logging, vulnerability management, incident response, and recovery.
Enterprise	Central policy, workload identity, automated evidence, SBOM and provenance, continuous exposure management, tenant isolation, supplier assurance, and trust-claim governance.
High Assurance	Hardware-backed identity, high-isolation execution, independent red teaming, cryptographic evidence, formal threat analysis, post-quantum migration planning, continuous control validation, and four-eyes emergency governance.

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

- Security approval based only on a checklist
- Storing credentials in model or agent context
- Calling a system zero trust, private, sovereign, or post-quantum without bounded evidence
- Relying on network location as identity
- Treating successful backup jobs as proof of recoverability
- Allowing extensions or agents ambient access

30. Adoption Roadmap from Source Draft

- Establish governance, asset and data classification, threat models, trust boundaries, and accountable risk ownership.

- Implement identity, authorization, secrets, cryptography, privacy, logging, secure development, and vulnerability-management baselines.
- Add supply-chain provenance, isolation, incident response, recovery validation, and third-party controls.
- Automate policy checks, evidence collection, continuous exposure monitoring, and control-drift detection.
- For High Assurance, add independent adversarial testing, stronger isolation, tamper-evident evidence, and tested emergency revocation.

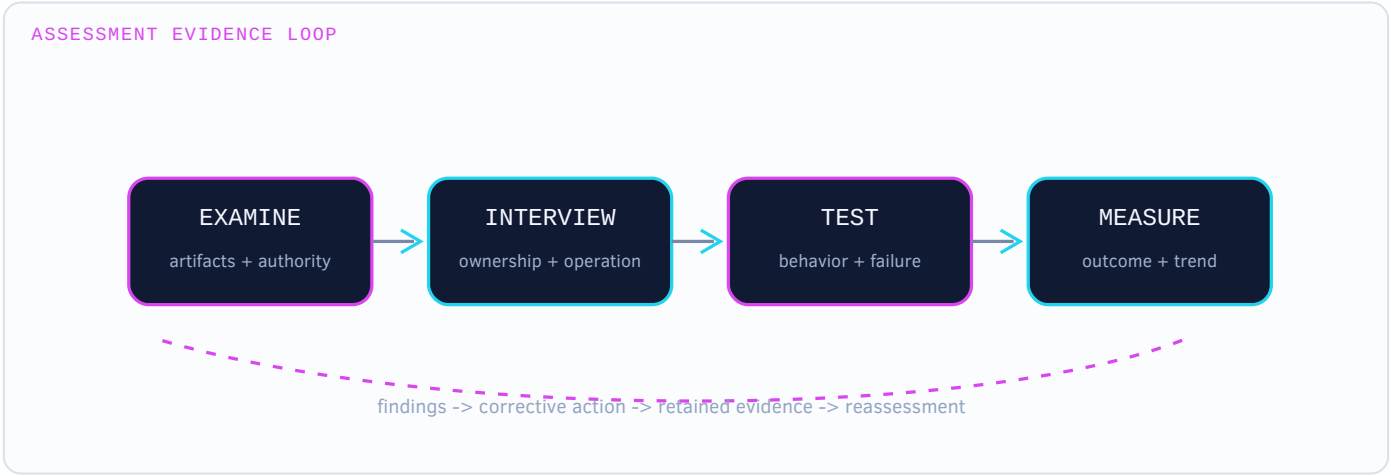
31. Limitations and Residual Risk from Source Draft

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
Critical-control verification	Applicable critical controls with current verified evidence	100%
Mean time to revoke		Risk-defined and tested

Metric	Definition	Expected use or target
	Elapsed time to revoke compromised identity, credential, key, token, extension, or release	
High-risk finding age	Age of unresolved critical and high findings beyond target	0 beyond approved target without active exception
Security telemetry coverage	Material trust boundaries and privileged actions producing usable events	100% High Assurance
Recovery validation	Critical services with exercised recovery and integrity verification	100% within defined interval

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.

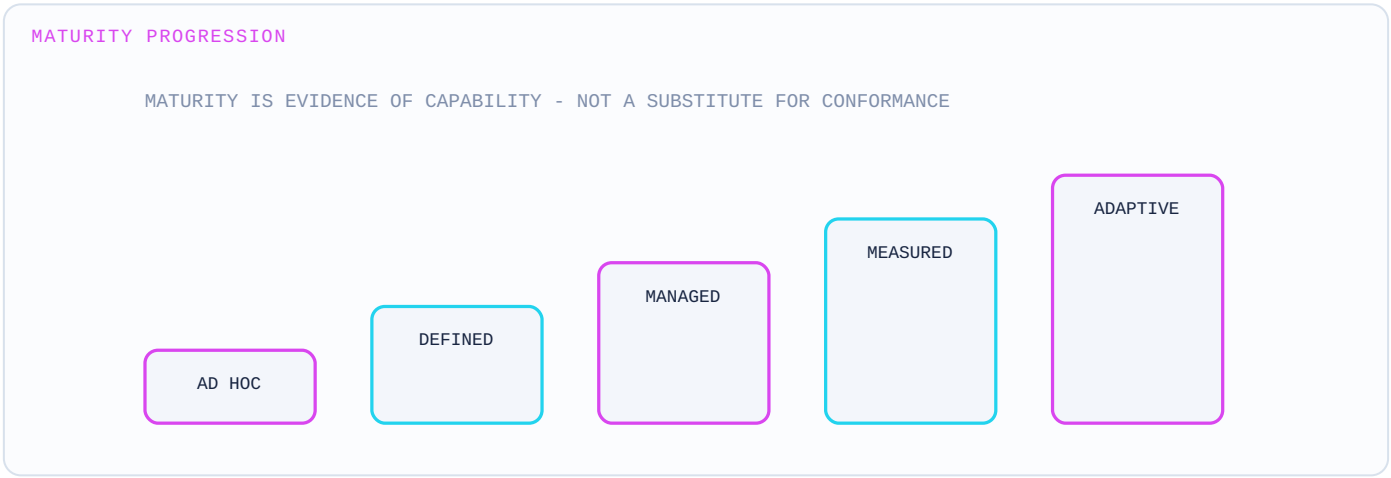
34. Exceptions and Compensating Controls

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
privileged identities without current owner	Defined by the adopting organization with owner, source, target, and cadence.
long-lived secrets beyond policy	Defined by the adopting organization with owner, source, target, and cadence.
critical assets without threat model	Defined by the adopting organization with owner, source, target, and cadence.
data stores without classification or retention rule	Defined by the adopting organization with owner, source, target, and cadence.
unsigned or unprovenanced release artifacts	Defined by the adopting organization with owner, source, target, and cadence.
critical vulnerabilities beyond target	Defined by the adopting organization with owner, source, target, and cadence.
security incidents without completed corrective actions	Defined by the adopting organization with owner, source, target, and cadence.
trust claims without current evidence	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 CSF 2.0	Cybersecurity risk governance	https://www.nist.gov/cyberframework	Current	2026-09-17
NIST SP 800-53 Rev. 5	Security and privacy controls	https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final	Final update 1	2026-09-17
NIST SP 800-207	Zero Trust Architecture	https://csrc.nist.gov/pubs/sp/800/207/final	Final	2026-09-17
NIST SP 800-218	Secure Software Development Framework 1.1	https://csrc.nist.gov/pubs/sp/800/218/final	Final; 1.2 revision is draft	2026-09-17
FIPS 203	ML-KEM	https://csrc.nist.gov/pubs/fips/203/final	Final	2026-09-17
FIPS 204	ML-DSA	https://csrc.nist.gov/pubs/fips/204/final	Final	2026-09-17
FIPS 205	SLH-DSA	https://csrc.nist.gov/pubs/fips/205/final	Final	2026-09-17
NIST SP 800-227	Recommendations for Key-Encapsulation Mechanisms	https://csrc.nist.gov/pubs/sp/800/227/final	Final	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

- Preserves the source draft's emphasis on deny-by-default, no ambient authority, trust boundaries, cryptographic agility, privacy, isolation, secure exports, and lifecycle security.
- Generalizes implementation-specific desktop and framework guidance into technology-neutral control outcomes.
- Adds current supply-chain, incident-response, and continuous-assurance structures.
- Replaces absolute security language with scoped trust claims, evidence, and residual-risk reporting.

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-SPT-01	Governance	Integrated security, privacy, and trust governance	Foundational, Advanced, High Assurance	Partial	Critical
MYTHOS-FND-SPT-02	Architecture	Security architecture and invariants	Foundational, Advanced, High Assurance	Partial	Critical
MYTHOS-FND-SPT-03	Risk	Threat, abuse, and misuse modeling	Foundational, Advanced, High Assurance	Partial	Critical
MYTHOS-FND-SPT-04	Assets and data	Asset, data, and capability classification	Foundational, Advanced, High Assurance	High	Critical
MYTHOS-FND-SPT-05	Identity	Strong identity and authentication	Foundational, Advanced, High Assurance	High	Critical
MYTHOS-FND-SPT-06	Authorization	Least privilege and explicit delegation	Foundational, Advanced, High Assurance	High	Critical
MYTHOS-FND-SPT-07	Secrets and keys	Secrets, certificates, and key lifecycle	Foundational, Advanced, High Assurance	High	Critical
MYTHOS-FND-SPT-08	Cryptography	Approved cryptography and crypto-agility	Foundational, Advanced, High Assurance	High	Critical
MYTHOS-FND-SPT-09	Privacy	Purpose limitation, minimization, and consent	Foundational, Advanced, High Assurance	Partial	Critical
MYTHOS-FND-SPT-10	Data lifecycle	Retention, deletion, and export protection	Foundational, Advanced, High Assurance	High	Critical

Control	Family	Title	Profiles	Automation	Impact
MYTHOS-FND-SPT-11	Isolation	Tenant, workload, and execution isolation	Advanced, High Assurance	High	Critical
MYTHOS-FND-SPT-12	Secure development	Secure design and implementation lifecycle	Foundational, Advanced, High Assurance	High	Critical
MYTHOS-FND-SPT-13	Supply chain	Software and service supply-chain integrity	Foundational, Advanced, High Assurance	High	Critical
MYTHOS-FND-SPT-14	Telemetry	Security logging, audit, and evidence integrity	Foundational, Advanced, High Assurance	High	Critical
MYTHOS-FND-SPT-15	Exposure management	Vulnerability and exposure management	Foundational, Advanced, High Assurance	High	Critical
MYTHOS-FND-SPT-16	Incident response	Incident response and emergency authority	Foundational, Advanced, High Assurance	Partial	Critical
MYTHOS-FND-SPT-17	Resilience	Backup, recovery, and continuity assurance	Foundational, Advanced, High Assurance	Partial	Critical
MYTHOS-FND-SPT-18	Third parties and automation	Third-party, AI, and delegated-action trust	Advanced, High Assurance	High	Critical
MYTHOS-FND-SPT-19	Assurance	Continuous control assurance and trust claims	Foundational, Advanced, High Assurance	High	Critical

Appendix D – Minimum Conformance Claim Record

```
standard: MYTHOS-FND-0003
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

CANDIDATE STANDARD

Mythos Quality, Testing, and Validation Standard

Turn requirements, hazards, and production behavior into reproducible verification and validation evidence.

PERMANENT ID
MYTHOS-FND-0004

PUBLICATION CLASS
CANDIDATE STANDARD

VERSION / STATUS
1.0.0-candidate / CANDIDATE

PERMANENT PUBLICATION IDENTITY

Mythos Quality, Testing, and Validation Standard

Universal Requirements for Quality Engineering, Verification, Validation, Test Evidence, Reliability, Performance, Accessibility, Security, and AI Evaluation

Document ID
MYTHOS-FND-0004

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	19	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	Quality engineers and test architects; Software, infrastructure, and data engineers; Security, privacy, accessibility, and reliability teams; Product and operations leaders; Independent validators and assessors
Publisher / owner	Mythos Systems / Standards Program
Public classification	Public technical standard
Canonical route	/library/standards/foundation/mythos-fnd-0004/

Expected outcomes

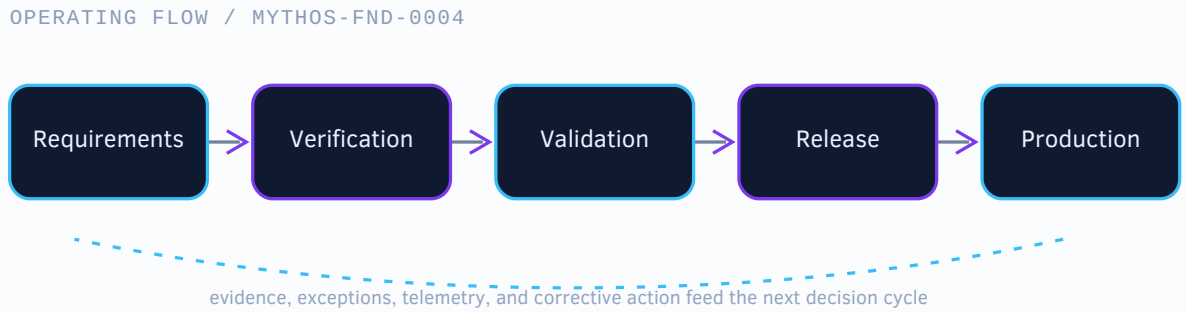
- Establish measurable quality models and risk-based validation depth.
- Create reproducible evidence across static, dynamic, operational, human, security, and AI evaluation methods.
- Prevent test quantity, code coverage, or pipeline success from substituting for meaningful assurance.
- Continuously reconcile pre-release assumptions with production behavior and user outcomes.

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.

Document Control 8

Revision Record 8

How to Use This Standard 9

Executive Reading Path 9

Engineering Reading Path 9

Assessment Reading Path 9

Normative and Informative Content 9

Part I – Executive Direction 10

1. Executive Overview 10

2. Executive Findings and Required Direction 10

3. Business and Operational Impact 10

4. Target-State Summary 11

5. Leadership Responsibilities 12

Part II – Standard Foundation 13

6. Purpose and Objectives 13

7. Scope 13

8. Intended Audience 13

9. Requirements Language and Conformance 13

10. Normative References from Source Draft 13

11. Informative References from Source Draft 14

12. Terms and Definitions 14

13. Applicability and Tailoring 15

Part III – Risk and Architecture 16

14. Enterprise Problem and Risk Landscape 16

15. Governing Principles 16

16. Reference Operating Architecture 16
17. Roles and Accountability 17
18. State, Evidence, and Decision Model 18
19. Security and Trust Considerations 18
20. Failure Modes 18
21. Cross-Functional Dependencies 18

Part IV – Normative Control System 19

22. Control-Family Overview 19
23. Normative Controls 20

Part V – Implementation and Operations 41

24. Implementation Profiles 41
25. Implementation Lifecycle 41
26. Integration Requirements 42
27. Failure Handling and Recovery 42
28. Exceptions and Compensating Controls 42
29. Prohibited Practices 42
30. Adoption Roadmap from Source Draft 42
31. Limitations and Residual Risk from Source Draft 43

Part VI – Assurance and Assessment 44

32. Assessment Methodology 44
33. Metrics and Reporting from Source Draft 44
34. Exceptions and Compensating Controls 45
35. Enterprise Metric Set 45
36. Maturity Model 46
37. Assessment Confidence 46
38. Executive Assurance Dashboard 46

Part VII – Authority and Traceability 48

39. Cross-Standard Dependencies from Source Draft 48
40. Current External Authority Register 48

41. Control Traceability 48

42. Source-Draft Preservation 49

Part VIII – Appendices **50**

Appendix A — Source-Draft Evolution Notes 50

Appendix B — Change History 50

Appendix C — Control Summary 50

Appendix D — Minimum Conformance Claim Record 51

Appendix E — Publication Review Checklist 51

NORMATIVE SYSTEM

Control index

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

MYTHOS-FND-QTV-01	Quality ownership and independent challenge	21
MYTHOS-FND-QTV-02	Measurable quality attributes	22
MYTHOS-FND-QTV-03	Risk-based verification and validation strategy	23
MYTHOS-FND-QTV-04	Requirement and risk traceability	24
MYTHOS-FND-QTV-05	Static analysis and review	25
MYTHOS-FND-QTV-06	Unit and component verification	26
MYTHOS-FND-QTV-07	Contract and integration testing	27
MYTHOS-FND-QTV-08	End-to-end workflow and user validation	28
MYTHOS-FND-QTV-09	Performance, scalability, and resource validation	29
MYTHOS-FND-QTV-10	Resilience and recovery testing	30
MYTHOS-FND-QTV-11	Security and privacy verification	31
MYTHOS-FND-QTV-12	Accessible and usable interaction validation	32
MYTHOS-FND-QTV-13	Data quality, migration, and compatibility validation	33
MYTHOS-FND-QTV-14	AI and probabilistic-system evaluation	34
MYTHOS-FND-QTV-15	Controlled environments and test data	36
MYTHOS-FND-QTV-16	Reproducible and integrity-protected test evidence	37
MYTHOS-FND-QTV-17	Defect, flakiness, and exception governance	38
MYTHOS-FND-QTV-18	Evidence-based quality gates	39
MYTHOS-FND-QTV-19	Production quality monitoring and learning	40

Document Control

Field	Value
Document ID	MYTHOS-FND-0004
Standard	Quality, Testing, and Validation
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

Quality is not the number of tests executed. It is the demonstrated fitness, safety, reliability, accessibility, security, and operability of a defined system in representative conditions. This standard creates a risk-based assurance system that links requirements and hazards to test evidence, prevents self-attested completion, and extends validation into production behavior and probabilistic AI performance.

The institutional objective is to establish risk-based, traceable, reproducible, and independently challengeable verification and validation across deterministic, distributed, interactive, and probabilistic systems. 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
Testing begins too late	Late verification reveals architecture defects when correction is expensive.	Define quality attributes, risks, and verification strategy during product definition.
Passing tests without representative conditions	Synthetic environments can conceal integration, scale, and recovery failures.	Use controlled but production-representative environments and data.
Self-verification	The same component or model that produced an output often declares success.	Require independent test or observation for consequential outcomes.
Flakiness normalized	Repeated reruns turn unstable tests into informal exceptions.	Measure, quarantine, remediate, and govern flakiness explicitly.
Probabilistic systems assessed like deterministic software	Single prompts and anecdotal demos do not establish AI quality.	Use representative datasets, repeated trials, harm metrics, and regression gates.

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.

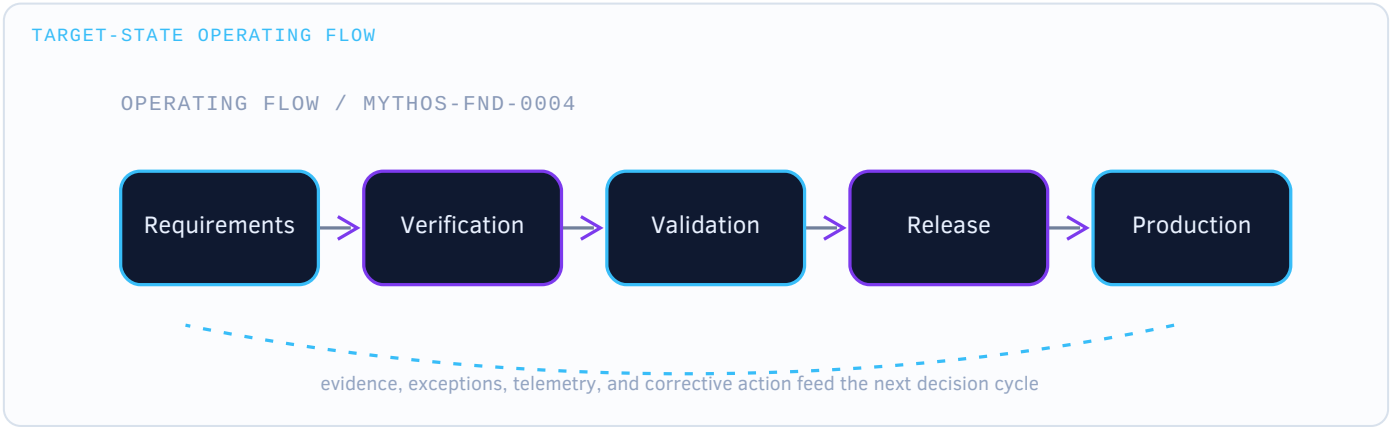
3.3 Security, Privacy, and Trust Impact

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	Quality ownership and challenge model
2	Quality-attribute and risk register
3	Requirements-to-test traceability
4	Static analysis and review
5	Unit, component, contract, integration, end-to-end, performance, resilience, security, privacy, accessibility, and migration testing
6	AI and probabilistic evaluation
7	Controlled environments and test data
8	Reproducible evidence and integrity
9	Defect and flakiness governance
10	Quality gates
11	Production monitoring and learning

```
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
Quality executive or engineering leader	Owns quality policy and systemic risk.
Quality architect	Defines assurance strategy and quality models.
Engineering teams	Implement testable systems and component verification.
Independent validation team	Challenges high-impact claims and release evidence.
Security and privacy testers	Validate abuse, exposure, and privacy controls.
Accessibility specialist	Validates representative user access.
Site reliability or operations team	Validates operational and recovery behavior.
Model evaluation lead	Owns probabilistic and AI evaluation methodology.

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

- Establish measurable quality models and risk-based validation depth.
- Create reproducible evidence across static, dynamic, operational, human, security, and AI evaluation methods.
- Prevent test quantity, code coverage, or pipeline success from substituting for meaningful assurance.
- Continuously reconcile pre-release assumptions with production behavior and user outcomes.

7. Scope

Applies to software, infrastructure, data systems, services, interfaces, integrations, extensions, automation, models, agents, and operational procedures throughout acquisition, development, deployment, change, and retirement.

8. Intended Audience

- Quality engineers and test architects
- Software, infrastructure, and data engineers
- Security, privacy, accessibility, and reliability teams
- Product and operations leaders
- Independent validators 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

- **ISO/IEC 25010:2023** — Systems and software Quality Requirements and Evaluation — Product quality model. https://www.iso.org/standard/78176.html
- **ISO/IEC/IEEE 15288:2023** — Systems and software engineering — System life cycle processes. https://www.iso.org/standard/81702.html
- **ISO/IEC/IEEE 29148:2018** — Systems and software engineering — Life cycle processes — Requirements engineering. https://www.iso.org/standard/72089.html
- **NIST SP 800-53A Rev. 5, Release 5.2.0** — Assessing Security and Privacy Controls in Information Systems and Organizations. https://csrc.nist.gov/pubs/sp/800/53/a/r5/final
- **NIST SP 800-218 v1.1** — Secure Software Development Framework (SSDF). https://csrc.nist.gov/pubs/sp/800/218/final
- **OWASP ASVS** — Application Security Verification Standard. https://owasp.org/www-project-application-security-verification-standard/
- **W3C WCAG 2.2** — Web Content Accessibility Guidelines 2.2. https://www.w3.org/TR/WCAG22/
- **NIST AI 100-1** — Artificial Intelligence Risk Management Framework (AI RMF 1.0). https://doi.org/10.6028/NIST.AI.100-1
- **NIST AI 600-1** — Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile. https://doi.org/10.6028/NIST.AI.600-1

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.

Term	Definition
Verification	Confirmation through objective evidence that specified requirements have been fulfilled.
Validation	Confirmation through objective evidence that the resulting system satisfies intended use and stakeholder needs in its context.
Test oracle	The mechanism or rule used to determine whether observed behavior is acceptable.
Quality gate	A defined decision point that blocks or conditions progression based on evidence and risk.
Flaky test	A test that produces inconsistent results without a relevant change in the assessed object or controlled inputs.

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.

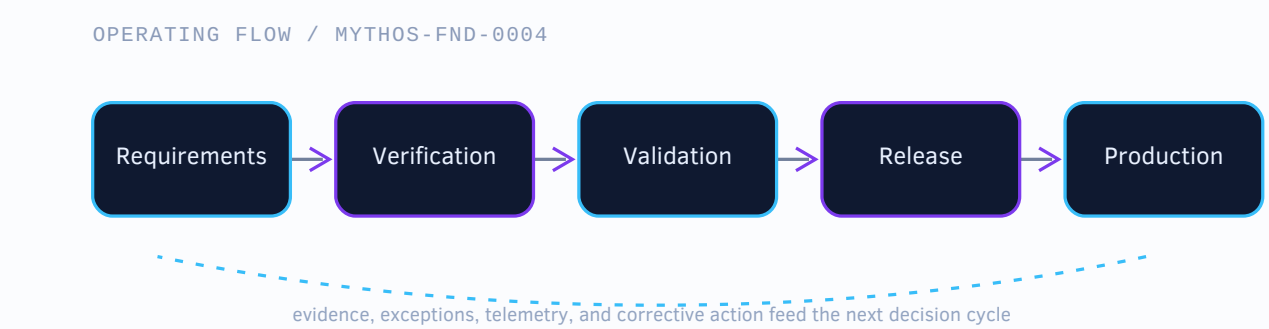
Adopting organizations SHOULD maintain a domain-specific risk register that identifies cause, affected asset or stakeholder, credible scenario, impact, existing controls, residual risk, owner, review trigger, and evidence. Risks that cross standards MUST be linked rather than copied into disconnected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

15. Governing Principles

- Quality requirements must be explicit before their tests are considered complete.
- Testing depth follows consequence, uncertainty, novelty, and change risk.
- Evidence must be reproducible, attributable, and honest about limitations.
- Negative, degraded, adversarial, and recovery behavior are first-class test concerns.
- Production telemetry and incidents are part of validation, not substitutes for pre-release engineering.
- A passed pipeline cannot override a failed mandatory requirement.

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
Quality executive or engineering leader	Owns quality policy and systemic risk.
Quality architect	Defines assurance strategy and quality models.
Engineering teams	Implement testable systems and component verification.
Independent validation team	Challenges high-impact claims and release evidence.
Security and privacy testers	Validate abuse, exposure, and privacy controls.
Accessibility specialist	Validates representative user access.
Site reliability or operations team	Validates operational and recovery behavior.
Model evaluation lead	Owns probabilistic and AI evaluation methodology.

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
Counting tests as a quality measure without coverage or risk context	Failure can create hidden risk, misleading assurance, uncontrolled cost, or unsafe operation.
Rerunning failed tests until they pass	Failure can create hidden risk, misleading assurance, uncontrolled cost, or unsafe operation.
Using production customer data without controlled authorization	Failure can create hidden risk, misleading assurance, uncontrolled cost, or unsafe operation.
Allowing a model to grade its own consequential output	Failure can create hidden risk, misleading assurance, uncontrolled cost, or unsafe operation.
Treating staging success as production verification	Failure can create hidden risk, misleading assurance, uncontrolled cost, or unsafe operation.
Skipping accessibility or recovery because automation is difficult	Failure can create hidden risk, misleading assurance, uncontrolled cost, or unsafe operation.

21. Cross-Functional Dependencies

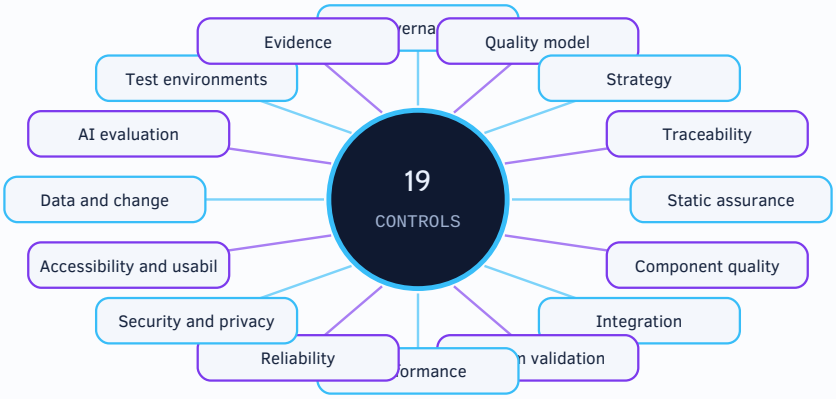
This Foundation standard depends on the remaining MYTHOS-FND standards for documentation, security and trust, quality, operations, data and integration, interfaces, extensions, AI-first behavior, and agentic orchestration. An adopting organization MUST resolve overlapping requirements through the stricter 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 **19 controls** across the following families:

- Governance
- Quality model
- Strategy
- Traceability
- Static assurance
- Component quality
- Integration
- System validation
- Performance
- Reliability
- Security and privacy
- Accessibility and usability
- Data and change
- AI evaluation
- Test environments
- Evidence
- Defects
- Release gates

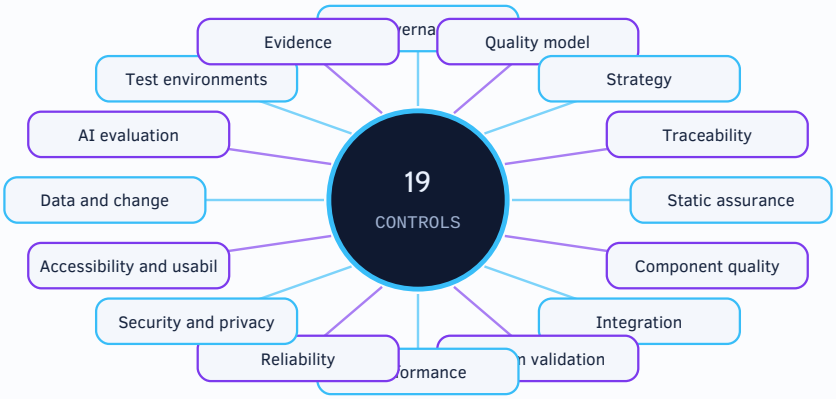
- Production validation

23. Normative Controls

CONTROL SET	PROFILES	ASSESSMENT
19	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-QTV-01 – Quality ownership and independent challenge

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

Requirement

The organization MUST assign accountable ownership for quality outcomes and define when verification or validation requires independence from the implementer.

Purpose

Prevents quality from becoming an unowned team activity and reduces confirmation bias for high-impact capabilities.

Applicability

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

Implementation guidance

- Define decision rights for accepting failed or incomplete evidence.
- Use independent review, test design, or execution for safety-critical, security-critical, irreversible, or high-consequence changes.
- Separate release pressure from evidence interpretation.

Required evidence

- Quality governance plan
- Responsibility matrix
- Independent review records

Assessment procedure

- **Examine:** Examine authority and escalation.
- **Interview:** Interview implementers and validators.
- **Test:** Sample exceptions to determine who accepted residual risk.

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 — verification and validation

NORMATIVE CONTROL

MYTHOS-FND-QTV-02 – Measurable quality attributes

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

Requirement

The system MUST have measurable quality requirements and acceptance thresholds for applicable functional suitability, performance, reliability, security, privacy, usability, accessibility, compatibility, maintainability, portability, safety, and operational characteristics.

Purpose

Creates testable expectations and exposes tradeoffs before implementation and release.

Applicability

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

Implementation guidance

- Use scenario-based measures with workload, environment, percentile, duration, and failure conditions.
- Prioritize conflicting attributes.
- Link each material attribute to owner and validation method.

Required evidence

- Quality model
- Acceptance thresholds
- Quality-attribute scenarios

Assessment procedure

- **Examine:** Examine completeness against system risk.
- **Interview:** Recalculate selected measures.
- **Test:** Verify ambiguous adjectives have been replaced by measurable criteria.

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 25010:2023

NORMATIVE CONTROL

MYTHOS-FND-QTV-03 – Risk-based verification and validation strategy

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

Requirement

The organization MUST maintain a test strategy that maps consequence, uncertainty, change scope, attack surface, user impact, and operational criticality to required methods, environments, independence, depth, and evidence.

Purpose

Directs finite testing effort toward the failures that matter most.

Applicability

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

Implementation guidance

- Include static analysis, review, unit, component, contract, integration, system, performance, security, accessibility, resilience, operational, and user validation as applicable.
- State excluded methods and residual uncertainty.
- Update strategy after incidents and architecture changes.

Required evidence

- Test strategy
- Risk-to-method matrix
- Change records

Assessment procedure

- **Examine:** Trace high-risk scenarios to methods.
- **Interview:** Review exclusions and rationale.
- **Test:** Verify strategy changed after relevant events.

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 800-53A Rev. 5 — assessment planning

NORMATIVE CONTROL

MYTHOS-FND-QTV-04 – Requirement and risk traceability

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

Requirement

Every applicable mandatory requirement, material risk, threat, privacy concern, and critical workflow MUST be linked to one or more verification or validation methods and current evidence or an explicit unresolved finding.

Purpose

Prevents false completeness based on test counts or code coverage.

Applicability

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

Implementation guidance

- Record the relationship and evidence freshness.
- Detect orphan requirements and tests automatically where practical.
- Do not mark a requirement passed solely because adjacent tests passed.

Required evidence

- Traceability matrix
- Coverage report
- Unresolved finding register

Assessment procedure

- **Examine:** Trace sampled requirements to evidence.
- **Interview:** Identify orphan tests and explain purpose.
- **Test:** Modify a requirement and confirm impact analysis.

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 29148:2018 — traceability

NORMATIVE CONTROL

MYTHOS-FND-QTV-05 – Static analysis and review

FAMILY	PROFILES	FAILURE IMPACT	AUTOMATION POTENTIAL
Static assurance	Foundational, Advanced, High Assurance	Material	High

Requirement

Source code, infrastructure, configuration, schemas, policies, documentation, dependencies, and model or prompt assets SHOULD undergo automated analysis and human review appropriate to their risk before integration.

Purpose

Finds defects and unsafe changes before execution while preserving design judgment for issues tools cannot infer.

Applicability

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

Implementation guidance

- Use language- and artifact-specific analysis.
- Define severity thresholds and suppressions with expiration and rationale.
- Review generated code and automated changes under the same risk rules as human changes.

Required evidence

- Review records
- Analysis results
- Suppression register

Assessment procedure

- **Examine:** Introduce representative violations in a test branch.
- **Interview:** Review stale suppressions.
- **Test:** Verify high-risk changes receive qualified review.

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 — PW and RV practices

NORMATIVE CONTROL

MYTHOS-FND-QTV-06 – Unit and component verification

FAMILY	PROFILES	FAILURE IMPACT	AUTOMATION POTENTIAL
Component quality	Foundational, Advanced, High Assurance	Material	High

Requirement

Deterministic business rules, transformations, policy decisions, parsers, calculations, and component contracts MUST have automated tests covering expected, boundary, invalid, and failure behavior proportionate to risk.

Purpose

Creates fast, localized evidence and protects critical logic from regression.

Applicability

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

Implementation guidance

- Prefer behavior assertions over implementation coupling.
- Use property-based, mutation, fuzz, or formal methods where examples provide weak coverage.
- Define deterministic seeds and shrinkable failures for randomized tests.

Required evidence

- Test suites
- Coverage and mutation reports where used
- Failure artifacts

Assessment procedure

- **Examine:** Run representative tests from a clean environment.
- **Interview:** Inspect boundary and negative cases.
- **Test:** Evaluate whether coverage metrics correspond to meaningful assertions.

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 — SA-11

NORMATIVE CONTROL

MYTHOS-FND-QTV-07 – Contract and integration testing

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

Requirement

Interfaces among components, services, data stores, providers, devices, extensions, and external systems MUST be validated against versioned contracts, authorization rules, failure semantics, timeouts, retries, and compatibility expectations.

Purpose

Detects defects that isolated components cannot reveal.

Applicability

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

Implementation guidance

- Use consumer- and provider-side contract tests where ownership is distributed.
- Test malformed, delayed, duplicated, reordered, unavailable, and incompatible interactions.
- Use representative authentication and tenant contexts.

Required evidence

- Contract tests
- Integration environment records
- Compatibility results

Assessment procedure

- **Examine:** Break a contract in a controlled branch and verify detection.
- **Interview:** Exercise provider failure and timeout.
- **Test:** Review test doubles for unrealistic behavior.

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

- OpenAPI 3.2.0
- AsyncAPI 3.1.0

NORMATIVE CONTROL

MYTHOS-FND-QTV-08 – End-to-end workflow and user validation

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

Requirement

Critical workflows MUST be validated end to end in representative environments across success, error, degraded, interruption, recovery, authorization, accessibility, and concurrency scenarios.

Purpose

Confirms that integrated behavior satisfies intended use rather than only component specifications.

Applicability

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

Implementation guidance

- Include operators, administrators, and affected non-users where relevant.
- Validate observable state and evidence at each handoff.
- Avoid relying exclusively on brittle UI automation when lower-level evidence is stronger.

Required evidence

- Scenario catalog
- End-to-end results
- User validation findings

Assessment procedure

- **Examine:** Observe sampled workflows.
- **Interview:** Interrupt or degrade a dependency.
- **Test:** Verify recovery does not produce hidden duplicate or unauthorized actions.

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 — validation

NORMATIVE CONTROL

MYTHOS-FND-QTV-09 – Performance, scalability, and resource validation

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

Requirement

Systems MUST be tested against defined workload models, service-level objectives, capacity limits, saturation behavior, resource budgets, and recovery from overload before claims of scale or performance are made.

Purpose

Prevents averages, synthetic microbenchmarks, and unconstrained test environments from overstating production capability.

Applicability

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

Implementation guidance

- Measure percentiles, throughput, queueing, errors, resource use, and tail behavior.
- Include realistic data size, concurrency, locality, dependency latency, and warm or cold state.
- Identify safe degradation and admission control.

Required evidence

- Workload model
- Performance results
- Capacity and bottleneck analysis

Assessment procedure

- **Examine:** Reproduce a reported benchmark.
- **Interview:** Push beyond target load and observe failure behavior.
- **Test:** Compare environment and workload to production assumptions.

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 25010:2023 — performance efficiency

NORMATIVE CONTROL

MYTHOS-FND-QTV-10 – Resilience and recovery testing

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

Requirement

Critical systems MUST be tested for dependency failure, process crash, network impairment, resource exhaustion, partial writes, corrupted data, clock anomalies, restart, failover, rollback, backup restoration, and operator error as applicable.

Purpose

Validates that recovery mechanisms work under realistic failure rather than ideal conditions.

Applicability

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

Implementation guidance

- Use controlled fault injection and game days.
- Verify data and authorization integrity after recovery.
- Test correlated failures and loss of control-plane services for high-impact environments.

Required evidence

- Fault scenarios
- Exercise results
- Recovery integrity evidence

Assessment procedure

- **Examine:** Inject a selected failure.
- **Interview:** Compare actual recovery to objectives.
- **Test:** Review untested single points of failure.

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 — CP and SI families

NORMATIVE CONTROL

MYTHOS-FND-QTV-11 – Security and privacy verification

FAMILY	PROFILES	FAILURE IMPACT	AUTOMATION POTENTIAL
Security and privacy	Foundational, Advanced, High Assurance	Critical	Partial

Requirement

Security and privacy requirements MUST be verified through a combination of design review, automated analysis, configuration assessment, negative testing, abuse-case testing, adversarial testing, and data-lifecycle validation proportionate to risk.

Purpose

Prevents security claims from resting on functional tests or checklists alone.

Applicability

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

Implementation guidance

- Test authorization bypass, injection, secret exposure, isolation, logging, retention, deletion, exports, and dependency compromise as applicable.
- Use independent penetration testing for high-impact systems.
- Track exploitability and business consequence.

Required evidence

- Security test plan
- Findings and retest evidence
- Privacy lifecycle tests

Assessment procedure

- **Examine:** Attempt selected misuse cases.
- **Interview:** Verify fixed findings are retested.
- **Test:** Review untested trust boundaries.

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

- OWASP ASVS
- NIST SP 800-53A Rev. 5

NORMATIVE CONTROL

MYTHOS-FND-QTV-12 – Accessible and usable interaction validation

FAMILY	PROFILES	FAILURE IMPACT	AUTOMATION POTENTIAL
Accessibility and usability	Foundational, Advanced, High Assurance	Material	Partial

Requirement

User interfaces and user information MUST be evaluated with automated checks, expert review, keyboard and assistive-technology testing, and representative user tasks appropriate to the product and applicable accessibility requirements.

Purpose

Ensures functional correctness is not achieved by excluding users or creating unsafe interaction burden.

Applicability

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

Implementation guidance

- Test focus order, names, roles, states, contrast, scaling, motion, errors, time limits, and alternatives.
- Include high-stress and recovery workflows.
- Treat accessibility defects as product defects.

Required evidence

- Accessibility results
- Usability study records
- Remediation evidence

Assessment procedure

- **Examine:** Perform keyboard-only and screen-reader tasks.
- **Interview:** Review automated findings for false positives and gaps.
- **Test:** Observe representative users completing critical tasks.

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

- WCAG 2.2
- WAI-ARIA 1.2

NORMATIVE CONTROL

MYTHOS-FND-QTV-13 – Data quality, migration, and compatibility validation

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

Requirement

Data pipelines, transformations, schema changes, migrations, imports, exports, and backward-compatibility claims MUST be validated for completeness, correctness, idempotency, lineage, performance, rollback, and privacy effects.

Purpose

Prevents silent corruption and irreversible deployment failures.

Applicability

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

Implementation guidance

- Use representative scale and edge cases.
- Reconcile counts, checksums, invariants, and business totals.
- Test mixed-version operation and rollback where required.
- Preserve pre-change recovery points.

Required evidence

- Migration plan
- Reconciliation results
- Rollback evidence

Assessment procedure

- **Examine:** Run migration on representative data.
- **Interview:** Inject interruption and retry.
- **Test:** Compare pre- and post-change invariants.

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 25010:2023 — compatibility and reliability

NORMATIVE CONTROL

MYTHOS-FND-QTV-14 – AI and probabilistic-system evaluation

FAMILY	PROFILES	FAILURE IMPACT	AUTOMATION POTENTIAL
AI evaluation	Advanced, High Assurance	Critical	High

Requirement

AI-enabled and probabilistic capabilities MUST be evaluated using task-representative datasets and scenarios for utility, correctness, calibration, safety, security, privacy, robustness, bias or disparate effects, grounding, tool use, abstention, and failure recovery.

Purpose

Addresses behavior that cannot be validated through deterministic unit assertions alone.

Applicability

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

Implementation guidance

- Maintain versioned evaluation sets with provenance and contamination controls.
- Separate offline benchmarks from human and production validation.
- Measure distributions and worst-case categories, not only averages.
- Re-evaluate after model, prompt, retrieval, tool, policy, or provider change.

Required evidence

- Evaluation specification
- Dataset records
- Results by category and version

Assessment procedure

- **Examine:** Reproduce sampled evaluations.
- **Interview:** Test adversarial and out-of-distribution cases.
- **Test:** Verify promotion criteria block unacceptable regressions.

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 AI RMF 1.0 — Measure
- NIST AI 600-1

NORMATIVE CONTROL

MYTHOS-FND-QTV-15 – Controlled environments and test data

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

Requirement

Test environments and data MUST be sufficiently representative for the claimed conclusion, isolated from uncontrolled production impact, reproducible, access-controlled, and governed for privacy, retention, and provenance.

Purpose

Prevents misleading results, data leakage, and tests that become operational hazards.

Applicability

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

Implementation guidance

- Record environment, versions, configuration, dependencies, feature flags, and seed data.
- Prefer synthetic or de-identified data unless production data use is approved and protected.
- Detect drift between test and target environments.

Required evidence

- Environment manifests
- Data provenance and approvals
- Drift reports

Assessment procedure

- **Examine:** Recreate a test environment from records.
- **Interview:** Inspect test data for sensitive content.
- **Test:** Compare critical configuration with target deployment.

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 — SA-11 and PT controls

NORMATIVE CONTROL

MYTHOS-FND-QTV-16 – Reproducible and integrity-protected test evidence

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

Requirement

Release-relevant test evidence MUST identify the assessed artifact, requirement, environment, inputs, method, tool versions, time, executor, result, limitations, and artifact integrity information.

Purpose

Makes pass and fail conclusions independently reviewable and resistant to accidental substitution.

Applicability

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

Implementation guidance

- Use immutable or append-only evidence for high-impact releases.
- Hash or sign artifacts where provenance matters.
- Retain failed and superseded evidence with clear status.

Required evidence

- Evidence manifests
- Artifact hashes or signatures
- Reproduction records

Assessment procedure

- **Examine:** Select a release claim and reproduce the result.
- **Interview:** Verify artifact identity.
- **Test:** Check whether failed evidence remains visible.

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 800-53A Rev. 5

NORMATIVE CONTROL

MYTHOS-FND-QTV-17 – Defect, flakiness, and exception governance

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

Requirement

Defects, flaky tests, skipped checks, suppressions, and failed mandatory criteria MUST be classified, owned, time-bounded, tracked to verified closure or formal risk acceptance, and visible in release decisions.

Purpose

Prevents normalization of failure and hidden quality debt.

Applicability

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

Implementation guidance

- Do not rerun away nondeterministic failures without diagnosis.
- Set service levels by consequence and exposure.
- Require expiration and compensating controls for exceptions.

Required evidence

- Defect and exception register
- Flakiness trends
- Closure evidence

Assessment procedure

- **Examine:** Review aging and repeated reopenings.
- **Interview:** Inspect a release with known defects.
- **Test:** Verify suppressions expire or are reapproved.

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 — vulnerability response

NORMATIVE CONTROL

MYTHOS-FND-QTV-18 – Evidence-based quality gates

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

Requirement

Promotion and release gates MUST evaluate applicable mandatory requirements, critical findings, test evidence, known limitations, rollback readiness, operational readiness, and accepted exceptions; failed mandatory gates MUST block promotion unless explicitly permitted by governed emergency procedure.

Purpose

Prevents schedule or aggregate scores from overriding critical evidence.

Applicability

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

Implementation guidance

- Use policy-as-code where practical.
- Make gate inputs and decisions auditable.
- Define emergency release conditions, independent approval, monitoring, and post-release review.

Required evidence

- Gate policy
- Pipeline and approval records
- Release evidence bundle

Assessment procedure

- **Examine:** Cause a mandatory check to fail in a controlled pipeline.
- **Interview:** Review emergency bypasses.
- **Test:** Verify aggregate quality scores do not conceal critical failures.

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 — PS and PW practices

NORMATIVE CONTROL

MYTHOS-FND-QTV-19 – Production quality monitoring and learning

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

Requirement

The organization MUST monitor production indicators, user outcomes, incidents, support signals, performance, reliability, security, privacy, and AI behavior against pre-release assumptions and use findings to update requirements, tests, controls, and risk decisions.

Purpose

Closes the validation loop and detects context-dependent failures that pre-release environments cannot fully reproduce.

Applicability

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

Implementation guidance

- Define canary, feature-flag, rollback, and stop conditions.
- Protect privacy and avoid collecting unnecessary telemetry.
- Link escaped defects to missing or ineffective tests.

Required evidence

- Production quality dashboard
- Incident-to-test links
- Post-release reviews

Assessment procedure

- **Examine:** Trace an escaped defect to corrective action.
- **Interview:** Verify stop conditions can be executed.
- **Test:** Compare production distributions with evaluation assumptions.

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 25010:2023
- NIST AI RMF — Manage

FOUNDATION STANDARD / STRUCTURAL PART

Part V – Implementation and Operations

24. Implementation Profiles

Profile	Required Operating State
Baseline	Risk-based test plan, requirements traceability, static analysis, unit and integration testing, representative end-to-end validation, evidence, defect governance, and release gates.
Enterprise	Automated multi-layer pipelines, performance and resilience labs, production-like test data, accessibility and security gates, flaky-test analytics, and continuous quality reporting.
High Assurance	Independent V&V, formal or model-based analysis, adversarial testing, mutation and fuzzing, digital twins, sustained observation, cryptographically protected evidence, and no unreviewed gate bypass.

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

- Counting tests as a quality measure without coverage or risk context
- Rerunning failed tests until they pass
- Using production customer data without controlled authorization
- Allowing a model to grade its own consequential output
- Treating staging success as production verification
- Skipping accessibility or recovery because automation is difficult

30. Adoption Roadmap from Source Draft

- Define the quality model, critical workflows, risk classification, test strategy, and traceability.

- Build layered automated and manual tests with controlled environments and representative data.
- Add security, privacy, accessibility, resilience, performance, migration, and operational validation.
- Implement evidence manifests, quality gates, defect governance, and production feedback.
- For High Assurance, add independent validation, adversarial testing, fault injection, reproducibility controls, and continuous verification.

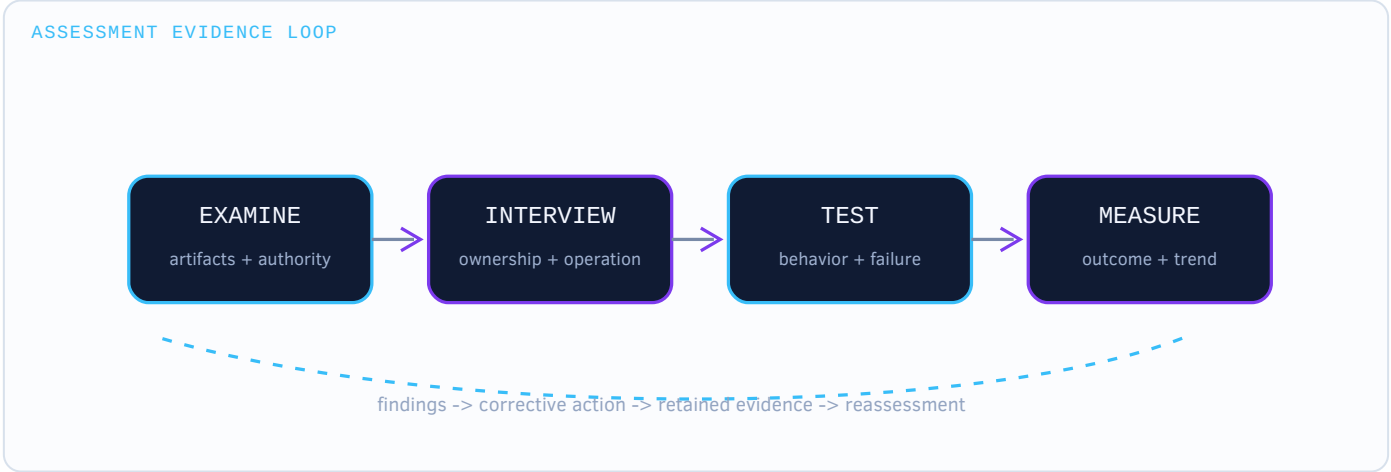
31. Limitations and Residual Risk from Source Draft

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
Requirement verification coverage	Applicable requirements with current passing evidence	100% MUST requirements
		100%

Metric	Definition	Expected use or target
Critical-path scenario coverage	Critical workflows tested across success, failure, degradation, and recovery	
Escaped-defect rate	Defects discovered after promotion, weighted by severity	Tracked and declining
Flaky-test burden	Release-relevant tests with unresolved nondeterminism	0 critical; controlled threshold otherwise
Evidence reproducibility	Sampled results independently reproduced from recorded context	>= 95% Advanced; 100% High Assurance sample

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.

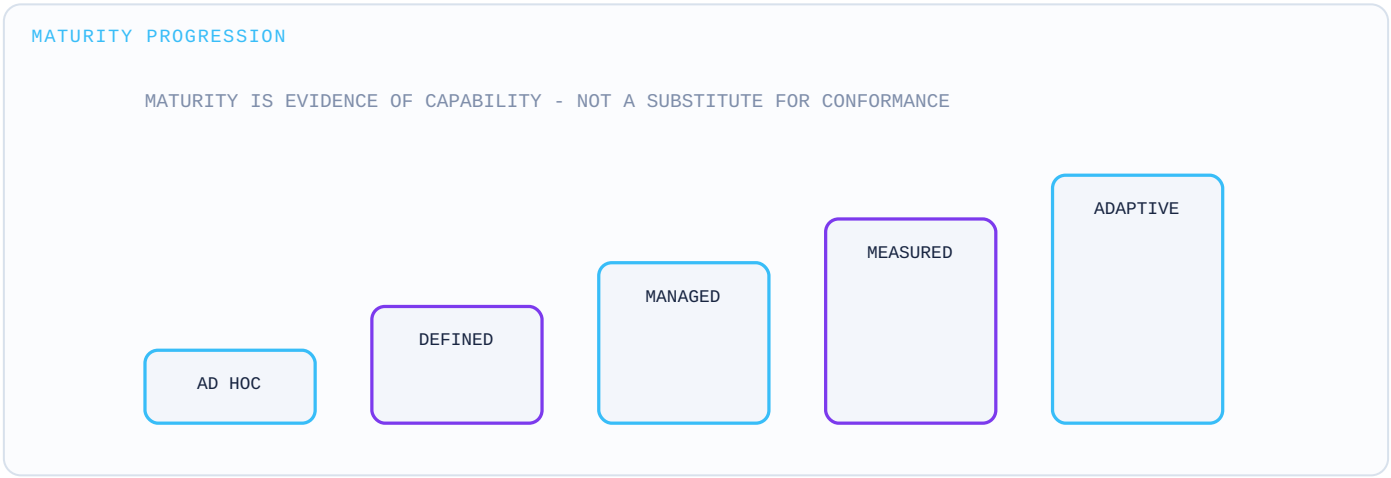
34. Exceptions and Compensating Controls

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
requirements covered by tests	Defined by the adopting organization with owner, source, target, and cadence.
critical risks with independent validation	Defined by the adopting organization with owner, source, target, and cadence.
escaped defects by severity	Defined by the adopting organization with owner, source, target, and cadence.
flaky tests and quarantine age	Defined by the adopting organization with owner, source, target, and cadence.
skipped required tests	Defined by the adopting organization with owner, source, target, and cadence.
mean time to reproduce failure	Defined by the adopting organization with owner, source, target, and cadence.
release gate overrides	Defined by the adopting organization with owner, source, target, and cadence.
AI evaluation regressions	Defined by the adopting organization with owner, source, target, and cadence.
recovery objectives demonstrated in exercise	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
ISO/IEC 25010:2023	Product quality model	https://www.iso.org/standard/78176.html	Published	2026-09-17
ISO/IEC 25020:2019	Quality measurement framework	https://www.iso.org/standard/72117.html	Published	2026-09-17
ISO/IEC/IEEE 29119-1:2013	Software testing concepts and definitions	https://www.iso.org/standard/45142.html	Published	2026-09-17
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
WCAG 2.2	Web accessibility conformance	https://www.w3.org/WAI/standards-guidelines/wcag/	W3C Recommendation	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

- Preserves the source draft's evidence-first posture, layered testing, failure-path coverage, release gates, and production validation.
- Replaces aspirational completeness claims with risk-based sampling, confidence, and residual uncertainty.
- Expands accessibility, privacy, migration, AI evaluation, and test-environment governance.
- Aligns assessment records with the shared Mythos examine/interview/test model.

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-QTV-01	Governance	Quality ownership and independent challenge	Foundational, Advanced, High Assurance	Partial	Critical
MYTHOS-FND-QTV-02	Quality model	Measurable quality attributes	Foundational, Advanced, High Assurance	Partial	Critical
MYTHOS-FND-QTV-03	Strategy	Risk-based verification and validation strategy	Foundational, Advanced, High Assurance	Partial	Critical
MYTHOS-FND-QTV-04	Traceability	Requirement and risk traceability	Foundational, Advanced, High Assurance	High	Critical
MYTHOS-FND-QTV-05	Static assurance	Static analysis and review	Foundational, Advanced, High Assurance	High	Material
MYTHOS-FND-QTV-06	Component quality	Unit and component verification	Foundational, Advanced, High Assurance	High	Material
MYTHOS-FND-QTV-07	Integration	Contract and integration testing	Foundational, Advanced, High Assurance	High	Critical
MYTHOS-FND-QTV-08	System validation	End-to-end workflow and user validation	Foundational, Advanced, High Assurance	Partial	Critical
MYTHOS-FND-QTV-09	Performance	Performance, scalability, and resource validation	Foundational, Advanced, High Assurance	High	Critical
MYTHOS-FND-QTV-10	Reliability	Resilience and recovery testing	Advanced, High Assurance	Partial	Critical
	Security and privacy	Security and privacy verification		Partial	Critical

Control	Family	Title	Profiles	Automation	Impact
MYTHOS-FND-QTV-11			Foundational, Advanced, High Assurance		
MYTHOS-FND-QTV-12	Accessibility and usability	Accessible and usable interaction validation	Foundational, Advanced, High Assurance	Partial	Material
MYTHOS-FND-QTV-13	Data and change	Data quality, migration, and compatibility validation	Foundational, Advanced, High Assurance	High	Critical
MYTHOS-FND-QTV-14	AI evaluation	AI and probabilistic-system evaluation	Advanced, High Assurance	High	Critical
MYTHOS-FND-QTV-15	Test environments	Controlled environments and test data	Foundational, Advanced, High Assurance	High	Critical
MYTHOS-FND-QTV-16	Evidence	Reproducible and integrity-protected test evidence	Foundational, Advanced, High Assurance	High	Critical
MYTHOS-FND-QTV-17	Defects	Defect, flakiness, and exception governance	Foundational, Advanced, High Assurance	High	Critical
MYTHOS-FND-QTV-18	Release gates	Evidence-based quality gates	Foundational, Advanced, High Assurance	High	Critical
MYTHOS-FND-QTV-19	Production validation	Production quality monitoring and learning	Foundational, Advanced, High Assurance	High	Critical

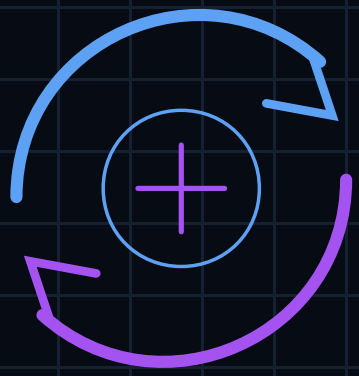
Appendix D – Minimum Conformance Claim Record

```
standard: MYTHOS-FND-0004
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



CANDIDATE STANDARD

Mythos Operations, Release, and Lifecycle Standard

Govern readiness, release, operation, recovery, maintenance, deprecation, and retirement as one lifecycle.

PERMANENT ID
MYTHOS-FND-0005

PUBLICATION CLASS
CANDIDATE STANDARD

VERSION / STATUS
1.0.0-candidate / CANDIDATE

PERMANENT PUBLICATION IDENTITY

Mythos Operations, Release, and Lifecycle Standard

Universal Requirements for Service Ownership, Observability, Change, Release, Reliability, Incident Management, Recovery, Maintenance, and Retirement

Document ID
MYTHOS-FND-0005

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	Site reliability and operations engineers; Software, infrastructure, network, and platform engineers; Release and change managers; Security and incident response teams; Service owners and technical leaders
Publisher / owner	Mythos Systems / Standards Program
Public classification	Public technical standard
Canonical route	/library/standards/foundation/mythos-fnd-0005/

Expected outcomes

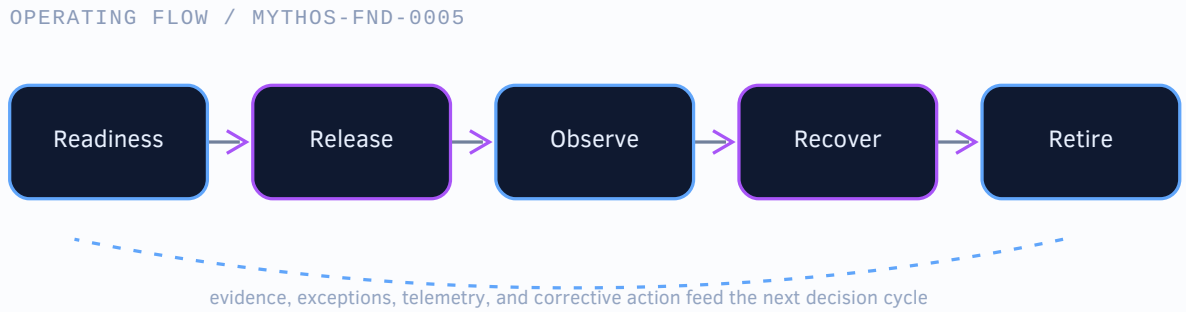
- Ensure every production capability has ownership, objectives, observable health, and operational procedures.
- Make changes controlled, progressive, reversible, and supported by immutable release evidence.
- Reduce incident impact through preparation, rapid containment, reliable recovery, and systemic learning.
- Govern dependencies, data, infrastructure, support, and decommissioning across the full lifecycle.

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.

Document Control 8

Revision Record 8

How to Use This Standard 9

Executive Reading Path 9

Engineering Reading Path 9

Assessment Reading Path 9

Normative and Informative Content 9

Part I – Executive Direction 10

1. Executive Overview 10

2. Executive Findings and Required Direction 10

3. Business and Operational Impact 10

4. Target-State Summary 11

5. Leadership Responsibilities 12

Part II – Standard Foundation 13

6. Purpose and Objectives 13

7. Scope 13

8. Intended Audience 13

9. Requirements Language and Conformance 13

10. Normative References from Source Draft 13

11. Informative References from Source Draft 14

12. Terms and Definitions 14

13. Applicability and Tailoring 15

Part III – Risk and Architecture 16

14. Enterprise Problem and Risk Landscape 16

15. Governing Principles 16

16. Reference Operating Architecture 16
17. Roles and Accountability 17
18. State, Evidence, and Decision Model 18
19. Security and Trust Considerations 18
20. Failure Modes 18
21. Cross-Functional Dependencies 18

Part IV – Normative Control System 19

22. Control-Family Overview 19
23. Normative Controls 20

Part V – Implementation and Operations 40

24. Implementation Profiles 40
25. Implementation Lifecycle 40
26. Integration Requirements 41
27. Failure Handling and Recovery 41
28. Exceptions and Compensating Controls 41
29. Prohibited Practices 41
30. Adoption Roadmap from Source Draft 41
31. Limitations and Residual Risk from Source Draft 42

Part VI – Assurance and Assessment 43

32. Assessment Methodology 43
33. Metrics and Reporting from Source Draft 43
34. Exceptions and Compensating Controls 44
35. Enterprise Metric Set 44
36. Maturity Model 45
37. Assessment Confidence 45
38. Executive Assurance Dashboard 45

Part VII – Authority and Traceability 47

39. Cross-Standard Dependencies from Source Draft 47
40. Current External Authority Register 47

41. Control Traceability 47

42. Source-Draft Preservation 48

Part VIII – Appendices **49**

Appendix A — Source-Draft Evolution Notes 49

Appendix B — Change History 49

Appendix C — Control Summary 49

Appendix D — Minimum Conformance Claim Record 50

Appendix E — Publication Review Checklist 50

NORMATIVE SYSTEM

Control index

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

MYTHOS-FND-ORL-01	Service ownership and catalog	21
MYTHOS-FND-ORL-02	Service-level indicators and objectives	22
MYTHOS-FND-ORL-03	Observable operational state	23
MYTHOS-FND-ORL-04	Operational readiness review	24
MYTHOS-FND-ORL-05	Controlled change management	25
MYTHOS-FND-ORL-06	Release authorization and evidence	26
MYTHOS-FND-ORL-07	Progressive and safe deployment	27
MYTHOS-FND-ORL-08	Authoritative configuration and state management	28
MYTHOS-FND-ORL-09	Rollback and forward-recovery capability	29
MYTHOS-FND-ORL-10	Operational runbooks and automation	30
MYTHOS-FND-ORL-11	Incident command, containment, and communication	31
MYTHOS-FND-ORL-12	Systemic problem management and learning	32
MYTHOS-FND-ORL-13	Capacity, performance, and demand management	33
MYTHOS-FND-ORL-14	Backup, restore, and continuity	34
MYTHOS-FND-ORL-15	Vulnerability, patch, and dependency lifecycle	35
MYTHOS-FND-ORL-16	Operational data integrity and maintenance	37
MYTHOS-FND-ORL-17	Operational access and emergency controls	38
MYTHOS-FND-ORL-18	Controlled deprecation and retirement	39

Document Control

Field	Value
Document ID	MYTHOS-FND-0005
Standard	Operations, Release, and Lifecycle
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

A system is not complete when it compiles or deploys. It is complete only when it can be owned, observed, supported, changed safely, recovered, and retired without losing control of customers, data, dependencies, or evidence. This standard establishes the operating model and release discipline required to convert engineering output into a dependable service.

The institutional objective is to govern service ownership, observability, change, release, deployment, recovery, incident response, capacity, maintenance, deprecation, and retirement across the operating lifecycle. 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
No accountable service ownership	Operational responsibility becomes ambiguous during incidents and lifecycle changes.	Maintain a service catalog with owners, criticality, dependencies, and support obligations.
Opaque operational state	Teams cannot distinguish healthy, degraded, failing, or unknown state.	Define SLIs, SLOs, telemetry, and explicit degraded modes.
Unsafe change and release	Release decisions rely on schedule rather than evidence and recoverability.	Require readiness review, progressive deployment, approval, and verification.
Rollback exists only on paper	Rollback paths are untested or cannot restore data and dependencies.	Test rollback and forward recovery under representative conditions.
Lifecycle debt	Deprecated interfaces, dependencies, data, and access remain indefinitely.	Use controlled deprecation, migration, retention, and retirement plans.

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.

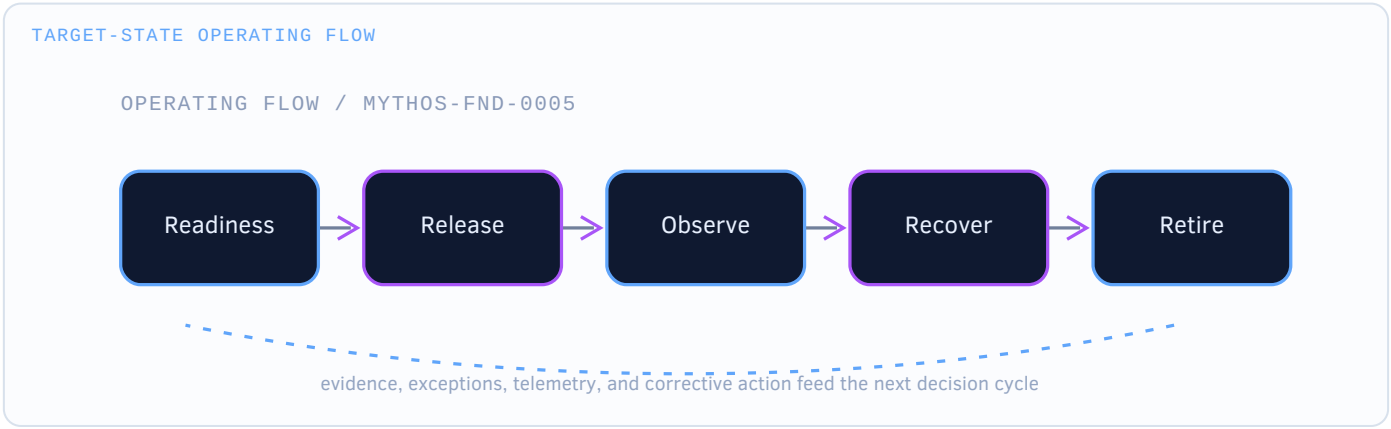
3.3 Security, Privacy, and Trust Impact

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	Service catalog and ownership
2	SLIs, SLOs, and error budgets
3	Operational telemetry and state model
4	Operational readiness review
5	Change and release governance
6	Progressive deployment and canary
7	Configuration and desired-state authority
8	Rollback and forward recovery
9	Runbooks and operational automation
10	Incident command and communication
11	Problem management and learning
12	Capacity and performance
13	Backup, restore, and continuity
14	Patch and dependency lifecycle

#	Target-State Component
15	Operational access and emergency controls
16	Deprecation and retirement

```
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
Service owner	Owns service health, risk, support, and lifecycle.
Operations or SRE lead	Owns reliability model, telemetry, readiness, and response.
Release authority	Approves release based on evidence and policy.
Change owner	Owns scope, implementation, verification, and rollback.
Incident commander	Coordinates incident response and communication.
Problem manager	Drives systemic corrective action.
Security operations	Coordinates exposure, patching, and emergency controls.
Business owner	Defines criticality, service expectations, and continuity priorities.

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

- Ensure every production capability has ownership, objectives, observable health, and operational procedures.
- Make changes controlled, progressive, reversible, and supported by immutable release evidence.
- Reduce incident impact through preparation, rapid containment, reliable recovery, and systemic learning.
- Govern dependencies, data, infrastructure, support, and decommissioning across the full lifecycle.

7. Scope

Applies to production and pre-production services, applications, infrastructure, data platforms, networks, automation, models, agents, integrations, extensions, and supporting operational processes.

8. Intended Audience

- Site reliability and operations engineers
- Software, infrastructure, network, and platform engineers
- Release and change managers
- Security and incident response teams
- Service owners and technical leaders

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

- **ISO/IEC/IEEE 15288:2023** — Systems and software engineering — System life cycle processes. https://www.iso.org/standard/81702.html
- **NIST CSWP 29** — The NIST Cybersecurity Framework (CSF) 2.0. https://doi.org/10.6028/NIST.CSWP.29
- **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
- **NIST SP 800-61 Rev. 3** — Incident Response Recommendations and Considerations for Cybersecurity Risk Management. https://csrc.nist.gov/pubs/sp/800/61/r3/final
- **CISA CPG 2.0** — Cross-Sector Cybersecurity Performance Goals 2.0. https://www.cisa.gov/cybersecurity-performance-goals-2-0-cpg-2-0
- **CIS Controls v8.1** — CIS Critical Security Controls. https://www.cisecurity.org/controls/v8-1
- **NIST SP 800-218 v1.1** — Secure Software Development Framework (SSDF). https://csrc.nist.gov/pubs/sp/800/218/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.
Service objective	A measurable target for user- or mission-relevant service behavior over a defined interval.
Error budget	The tolerated amount of objective nonconformance used to govern risk and change velocity.
Progressive delivery	Controlled exposure of a change to increasing scope while observing defined guardrails.
Operational readiness	Evidence that a capability can be deployed, observed, supported, secured, recovered, and retired safely.
Retirement	The controlled removal of a capability, dependency, interface, data set, credential, and supporting obligation.

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

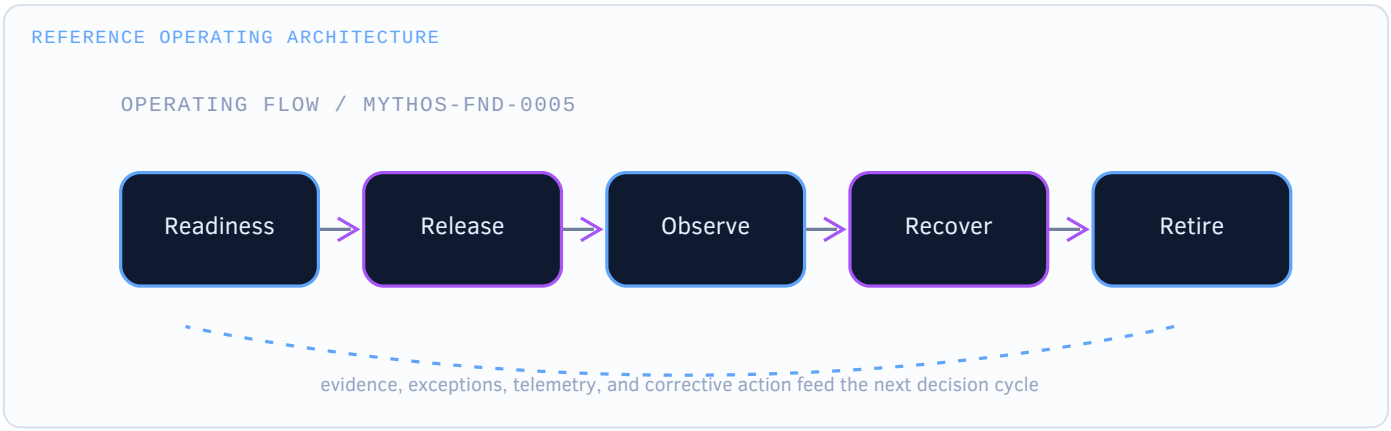
The principal enterprise risks addressed by this standard include inconsistent ownership, undocumented authority, uncontrolled change, local optimization, evidence gaps, stale assumptions, supplier dependence, false assurance, and the inability to determine whether the operating system still matches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

- Production ownership is explicit and follows the service lifecycle.
- User-visible and mission-relevant health is measured, not inferred from process uptime alone.
- Changes are small, observable, progressively exposed, and reversible where practical.
- Recovery is validated by exercise and integrity checks.
- Incidents are sources of system learning, not individual blame.
- Retirement is engineered with the same discipline as release.

16. 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
Service owner	Owns service health, risk, support, and lifecycle.
Operations or SRE lead	Owns reliability model, telemetry, readiness, and response.
Release authority	Approves release based on evidence and policy.
Change owner	Owns scope, implementation, verification, and rollback.
Incident commander	Coordinates incident response and communication.
Problem manager	Drives systemic corrective action.
Security operations	Coordinates exposure, patching, and emergency controls.
Business owner	Defines criticality, service expectations, and continuity priorities.

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
Declaring success when deployment completes without post-checks	Failure can create hidden risk, misleading assurance, uncontrolled cost, or unsafe operation.
Using dashboards without defined service objectives	Failure can create hidden risk, misleading assurance, uncontrolled cost, or unsafe operation.
Treating backup completion as proof of recovery	Failure can create hidden risk, misleading assurance, uncontrolled cost, or unsafe operation.
Allowing emergency access to become permanent	Failure can create hidden risk, misleading assurance, uncontrolled cost, or unsafe operation.
Running high-risk changes without verified rollback	Failure can create hidden risk, misleading assurance, uncontrolled cost, or unsafe operation.
Retiring services without data, identity, dependency, and customer migration	Failure can create hidden risk, misleading assurance, uncontrolled cost, or unsafe operation.

21. Cross-Functional Dependencies

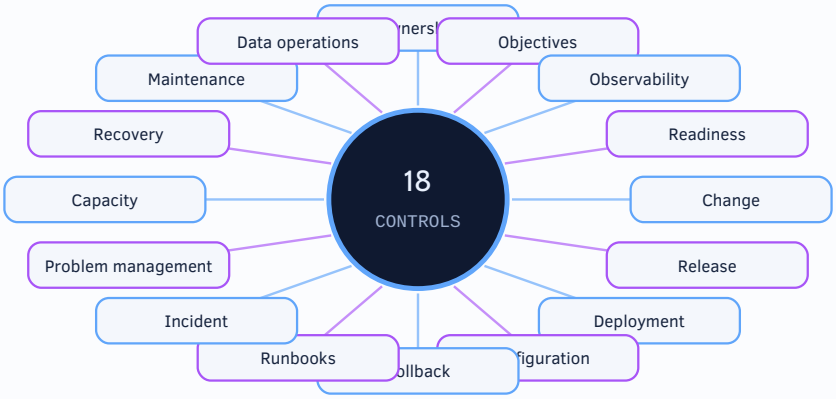
This Foundation standard depends on the remaining MYTHOS-FND standards for documentation, security and trust, quality, operations, data and integration, interfaces, extensions, AI-first behavior, and agentic orchestration. An adopting organization MUST resolve overlapping requirements through the stricter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

- Ownership
- Objectives
- Observability
- Readiness
- Change
- Release
- Deployment
- Configuration
- Rollback
- Runbooks
- Incident
- Problem management
- Capacity
- Recovery
- Maintenance
- Data operations
- Security operations
- Retirement

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-ORL-01 – Service ownership and catalog

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

Requirement

Every production service and material operational capability MUST have an accountable owner, support model, criticality classification, dependency record, lifecycle status, and escalation path in an authoritative service catalog.

Purpose

Prevents ownerless production systems and ambiguous response during change or failure.

Applicability

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

Implementation guidance

- Include technical and business ownership.
- Record supported hours, environments, users, data classes, upstream and downstream dependencies, and recovery tier.
- Review ownership after reorganizations and supplier changes.

Required evidence

- Service catalog
- Ownership attestations
- Escalation records

Assessment procedure

- **Examine:** Sample catalog entries against deployed inventory.
- **Interview:** Interview on-call and accountable owners.
- **Test:** Review orphan services and stale contacts.

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 CSF 2.0 — GV.RR and ID.AM

NORMATIVE CONTROL

MYTHOS-FND-ORL-02 – Service-level indicators and objectives

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

Requirement

Critical services MUST define user- or mission-relevant service-level indicators, objectives, measurement windows, exclusions, error budgets, data sources, and response rules for objective breaches.

Purpose

Directs reliability effort toward meaningful outcomes rather than infrastructure signals alone.

Applicability

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

Implementation guidance

- Measure availability, latency, correctness, freshness, durability, or workflow completion as appropriate.
- Avoid excluding difficult traffic without transparent rationale.
- Use objective health to inform release velocity and capacity work.

Required evidence

- SLI/SLO definitions
- Measurement queries
- Objective review records

Assessment procedure

- **Examine:** Recalculate selected objectives.
- **Interview:** Compare user impact with reported objective status.
- **Test:** Review actions taken after error-budget exhaustion.

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 CSF 2.0 — ID.IM and PR.IR

NORMATIVE CONTROL

MYTHOS-FND-ORL-03 – Observable operational state

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

Requirement

Systems MUST emit and retain sufficient metrics, logs, traces, events, topology, configuration, and business or workflow signals to determine health, diagnose failure, attribute consequential actions, and verify recovery without exposing unnecessary sensitive data.

Purpose

Enables timely detection and evidence-based diagnosis while controlling telemetry risk.

Applicability

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

Implementation guidance

- Define telemetry standards and required correlation identifiers.
- Monitor control-plane and data-plane behavior.
- Detect telemetry gaps and clock drift.
- Preserve high-value forensic evidence according to retention requirements.

Required evidence

- Observability specification
- Dashboards and alerts
- Telemetry-gap tests

Assessment procedure

- **Examine:** Trace a transaction across boundaries.
- **Interview:** Simulate telemetry loss.
- **Test:** Review signal-to-action usefulness and sensitive-data exposure.

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, SI-4
- CISA CPG 2.0 — logging

NORMATIVE CONTROL

MYTHOS-FND-ORL-04 – Operational readiness review

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

Requirement

A new or materially changed production capability MUST pass an operational readiness review covering ownership, objectives, capacity, dependencies, observability, security, privacy, support, runbooks, deployment, rollback, recovery, documentation, and retirement assumptions.

Purpose

Prevents deployment of capabilities that function in testing but cannot be safely operated.

Applicability

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

Implementation guidance

- Scale review depth by impact.
- Require evidence, not checklist assertions.
- Record unresolved conditions and accepted risk.

Required evidence

- Readiness checklist and evidence
- Approval record
- Open-risk register

Assessment procedure

- **Examine:** Sample a released capability.
- **Interview:** Verify checklist statements against evidence.
- **Test:** Review recurring readiness exceptions.

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 — transition and operation

NORMATIVE CONTROL

MYTHOS-FND-ORL-05 – Controlled change management

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

Requirement

Material production changes MUST have an identified owner, scope, risk and dependency analysis, validation, approval path, deployment plan, monitoring, rollback or recovery plan, and preserved change record.

Purpose

Reduces outages and security exposure caused by poorly understood or untraceable changes.

Applicability

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

Implementation guidance

- Classify standard, normal, and emergency changes.
- Automate low-risk repeatable changes only after validating guardrails.
- Include configuration, policy, data, model, prompt, provider, certificate, and infrastructure changes.

Required evidence

- Change records
- Risk and impact analysis
- Deployment and rollback evidence

Assessment procedure

- **Examine:** Trace sampled changes from request through observed outcome.
- **Interview:** Attempt an unapproved high-risk change in a test environment.
- **Test:** Review emergency changes.

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 — CM-3
- NIST CSF 2.0 — PR.PS

NORMATIVE CONTROL

MYTHOS-FND-ORL-06 – Release authorization and evidence

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

Requirement

Release authorization MUST be based on identified artifacts, passing mandatory quality and security criteria, compatibility and migration status, operational readiness, known limitations, accepted exceptions, and an immutable or integrity-protected evidence manifest.

Purpose

Prevents version ambiguity and promotion without reviewable evidence.

Applicability

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

Implementation guidance

- Bind authorization to artifact hashes or equivalent identity.
- Separate build completion from release approval.
- Publish release notes and support implications.

Required evidence

- Release manifest
- Gate results
- Approval and artifact identity

Assessment procedure

- **Examine:** Verify deployed artifacts match authorization.
- **Interview:** Review failed gates and exceptions.
- **Test:** Reproduce selected evidence.

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 — PS.2 and PW.9

NORMATIVE CONTROL

MYTHOS-FND-ORL-07 – Progressive and safe deployment

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

Requirement

High-impact changes SHOULD use staged, canary, blue-green, feature-flag, shadow, or equivalent progressive delivery with predefined health guardrails, stop conditions, and controlled expansion.

Purpose

Limits blast radius and creates early production evidence.

Applicability

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

Implementation guidance

- Select strategy based on state compatibility and rollback risk.
- Observe technical and outcome indicators.
- Prevent partial exposure from violating tenant, privacy, or authorization expectations.

Required evidence

- Deployment strategy
- Exposure and guardrail records
- Promotion history

Assessment procedure

- **Examine:** Observe a progressive deployment.
- **Interview:** Trigger a safe guardrail failure.
- **Test:** Verify expansion stops and exposure can be identified.

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 — SI-2 and CM-3

NORMATIVE CONTROL

MYTHOS-FND-ORL-08 – Authoritative configuration and state management

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

Requirement

Production configuration, policy, infrastructure, schemas, feature flags, and model or routing state MUST have an authoritative source, controlled change history, environment scoping, secret separation, drift detection, and recovery method.

Purpose

Prevents undocumented runtime state and configuration drift from becoming hidden architecture.

Applicability

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

Implementation guidance

- Prefer declarative, reviewable configuration where feasible.
- Record runtime overrides and expiration.
- Detect changes outside approved channels.

Required evidence

- Configuration inventory
- Drift reports
- Override and recovery records

Assessment procedure

- **Examine:** Compare live state to authority.
- **Interview:** Make a controlled out-of-band change and verify detection.
- **Test:** Restore a known-good configuration.

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 — CM family

NORMATIVE CONTROL

MYTHOS-FND-ORL-09 – Rollback and forward-recovery capability

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

Requirement

Material changes MUST have a validated rollback or forward-recovery strategy that addresses code, configuration, data, schemas, integrations, credentials, and side effects, with criteria for choosing and initiating recovery.

Purpose

Avoids plans that restore binaries while leaving incompatible or corrupted state.

Applicability

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

Implementation guidance

- Classify irreversible changes before deployment.
- Use expand-contract or compatible migration patterns.
- Protect recovery points and test restoration.

Required evidence

- Rollback plan
- Exercise results
- Irreversibility assessment

Assessment procedure

- **Examine:** Execute rollback in a representative environment.
- **Interview:** Interrupt a migration and recover.
- **Test:** Verify state integrity and duplicate-action handling.

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 CSF 2.0 — RC.RP

NORMATIVE CONTROL

MYTHOS-FND-ORL-10 – Operational runbooks and automation

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

Requirement

Critical alerts, incidents, maintenance tasks, recovery procedures, and privileged operations MUST have current, actionable runbooks or governed automation that includes prerequisites, safety limits, verification, rollback, escalation, and evidence preservation.

Purpose

Reduces cognitive load and unsafe improvisation during high-pressure operations.

Applicability

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

Implementation guidance

- Automate deterministic steps while keeping decision points explicit.
- Use least-privilege execution identities.
- Exercise runbooks and update them from actual use.

Required evidence

- Runbooks or automation definitions
- Exercise logs
- Change history

Assessment procedure

- **Examine:** Observe execution.
- **Interview:** Test a failure path and escalation.
- **Test:** Verify automation cannot exceed its declared authority.

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-ORL-11 – Incident command, containment, and communication

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

Requirement

The organization MUST define and exercise incident severity, command, technical response, evidence, communications, decision logging, containment authority, recovery, and external-notification processes.

Purpose

Creates coordinated action and accountability during events that cross teams and systems.

Applicability

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

Implementation guidance

- Use a single incident authority and timeline.
- Predefine safe containment options.
- Track customer, privacy, legal, and supplier obligations.
- Preserve uncertainty and avoid premature root-cause claims.

Required evidence

- Incident plan
- Exercise and incident timelines
- Communication records

Assessment procedure

- **Examine:** Run a cross-functional exercise.
- **Interview:** Review a sampled incident for role clarity and evidence.
- **Test:** Test after-hours escalation.

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
- NIST CSF 2.0 — Respond

NORMATIVE CONTROL

MYTHOS-FND-ORL-12 – Systemic problem management and learning

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

Requirement

Significant incidents, recurring defects, near misses, and objective breaches MUST receive causal analysis that identifies contributing system conditions and produces owned, prioritized, verifiable corrective actions.

Purpose

Prevents recurrence and avoids reducing complex failures to individual error.

Applicability

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

Implementation guidance

- Separate trigger from systemic contributors.
- Examine design, process, incentives, capacity, telemetry, dependencies, and documentation.
- Validate that corrective actions reduce the identified risk.

Required evidence

- Post-incident review
- Corrective action register
- Effectiveness evidence

Assessment procedure

- **Examine:** Trace corrective actions to closure.
- **Interview:** Look for repeated causal patterns.
- **Test:** Verify lessons changed tests, controls, or architecture.

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 CSF 2.0 — ID.IM

NORMATIVE CONTROL

MYTHOS-FND-ORL-13 – Capacity, performance, and demand management

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

Requirement

Critical services MUST forecast and monitor demand, saturation, quotas, dependency limits, cost, and failure thresholds and maintain tested responses for overload and abnormal demand.

Purpose

Prevents predictable exhaustion and unsafe scaling behavior.

Applicability

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

Implementation guidance

- Define headroom by lead time and consequence.
- Include human, network, storage, queue, rate, model, and supplier capacity.
- Use admission control, prioritization, and graceful degradation.

Required evidence

- Capacity model
- Forecast and saturation dashboard
- Load-shedding tests

Assessment procedure

- **Examine:** Compare forecast to actual demand.
- **Interview:** Drive a test environment to saturation.
- **Test:** Verify critical traffic remains prioritized.

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 25010:2023 — performance efficiency

NORMATIVE CONTROL

MYTHOS-FND-ORL-14 – Backup, restore, and continuity

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

Requirement

Critical data and services MUST have documented and exercised backup, restoration, continuity, and disaster-recovery controls that meet approved recovery objectives and verify confidentiality, authorization, integrity, and completeness after recovery.

Purpose

Ensures recoverability rather than backup-job completion.

Applicability

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

Implementation guidance

- Protect backups from common compromise.
- Test regional, supplier, identity, key, and control-plane loss as applicable.
- Record gaps between objectives and observed results.

Required evidence

- Backup inventory
- Restore and continuity exercises
- Recovery validation

Assessment procedure

- **Examine:** Restore sampled data and services.
- **Interview:** Test recovery without a key dependency.
- **Test:** Review recovery objective exceptions.

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 — CP family
- NIST CSF 2.0 — Recover

NORMATIVE CONTROL

MYTHOS-FND-ORL-15 – Vulnerability, patch, and dependency lifecycle

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

Requirement

The organization MUST monitor, prioritize, test, deploy, verify, and, when necessary, roll back security patches, defect fixes, certificates, firmware, models, dependencies, and supplier changes according to risk and support status.

Purpose

Reduces exposure while controlling update-induced failure.

Applicability

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

Implementation guidance

- Maintain supported-version inventory and end-of-life dates.
- Use emergency pathways for active exploitation.
- Test updates against critical workflows and compatibility.
- Plan replacement before support expiry.

Required evidence

- Lifecycle inventory
- Patch and update records
- Verification and exception records

Assessment procedure

- **Examine:** Sample aged dependencies and critical updates.
- **Interview:** Verify deployment and remediation.
- **Test:** Review end-of-life exposure.

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 Release 5.2.0 — SI-2
- CISA CPG 2.0

NORMATIVE CONTROL

MYTHOS-FND-ORL-16 – Operational data integrity and maintenance

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

Requirement

Operational data jobs, retention processes, reconciliation, reindexing, compaction, replication, archival, and deletion MUST be observable, recoverable, authorization-controlled, and validated for correctness and privacy impact.

Purpose

Prevents maintenance operations from silently corrupting or over-retaining data.

Applicability

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

Implementation guidance

- Use checkpoints and idempotency for long-running jobs.
- Reconcile totals and invariants.
- Separate operator authority from application authority for high-impact actions.

Required evidence

- Job definitions
- Reconciliation reports
- Authorization and recovery tests

Assessment procedure

- **Examine:** Interrupt and resume a maintenance job.
- **Interview:** Verify duplicate execution is safe.
- **Test:** Review deletion and archival outcomes.

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 — SI-7, SI-12

NORMATIVE CONTROL

MYTHOS-FND-ORL-17 – Operational access and emergency controls

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

Requirement

Operational and support access MUST use distinct identities, least privilege, approved channels, time-bounded elevation, complete audit, and post-use review for high-impact or break-glass activity.

Purpose

Constrains powerful operational authority and supports accountability.

Applicability

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

Implementation guidance

- Disallow shared administrative credentials.
- Broker sessions and record commands or actions where justified.
- Test emergency access without weakening ordinary controls.

Required evidence

- Privileged access policy
- Elevation and session records
- Break-glass exercise

Assessment procedure

- **Examine:** Review sampled privileged sessions.
- **Interview:** Attempt expired elevation.
- **Test:** Verify break-glass use triggers review.

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-2, AC-6, AU-12

NORMATIVE CONTROL

MYTHOS-FND-ORL-18 – Controlled deprecation and retirement

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

Requirement

Services, interfaces, data stores, models, extensions, credentials, infrastructure, and operational obligations MUST be retired through a controlled plan that addresses consumers, migration, communication, data disposition, access revocation, dependency removal, evidence retention, and post-retirement verification.

Purpose

Prevents abandoned systems, orphan data, lingering credentials, and hidden dependencies.

Applicability

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

Implementation guidance

- Define deprecation windows and compatibility support.
- Discover consumers rather than relying only on registration.
- Remove monitoring and cost only after verifying absence of required use.

Required evidence

- Retirement plan
- Consumer and migration records
- Post-retirement verification

Assessment procedure

- **Examine:** Search for remaining traffic, credentials, data, and dependencies.
- **Interview:** Verify user communication and migration.
- **Test:** Review rollback or contingency for failed retirement.

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 — disposal

FOUNDATION STANDARD / STRUCTURAL PART

Part V – Implementation and Operations

24. Implementation Profiles

Profile	Required Operating State
Baseline	Service owner, catalog, SLIs/SLOs, telemetry, readiness review, controlled release, rollback, runbooks, incident response, backups, patching, and retirement.
Enterprise	Central service management, progressive delivery, automated evidence, error budgets, configuration reconciliation, capacity forecasting, problem analytics, and regular recovery exercises.
High Assurance	Independent release authorization, multi-region or equivalent resilience, continuous verification, immutable evidence, strict change windows, proven failover, cryptographic artifact admission, and supervised emergency authority.

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

- Declaring success when deployment completes without post-checks
- Using dashboards without defined service objectives
- Treating backup completion as proof of recovery
- Allowing emergency access to become permanent
- Running high-risk changes without verified rollback
- Retiring services without data, identity, dependency, and customer migration

30. Adoption Roadmap from Source Draft

- Create service ownership, catalog, criticality, objectives, telemetry, and operational-readiness criteria.

- Standardize change, release, deployment, rollback, configuration, and runbook controls.
- Implement incident, problem, vulnerability, capacity, backup, recovery, and continuity practices.
- Add progressive delivery, automated gates, lifecycle intelligence, and dependency health monitoring.
- For High Assurance, continuously verify controls, exercise severe scenarios, preserve tamper-evident evidence, and test retirement and recovery end to end.

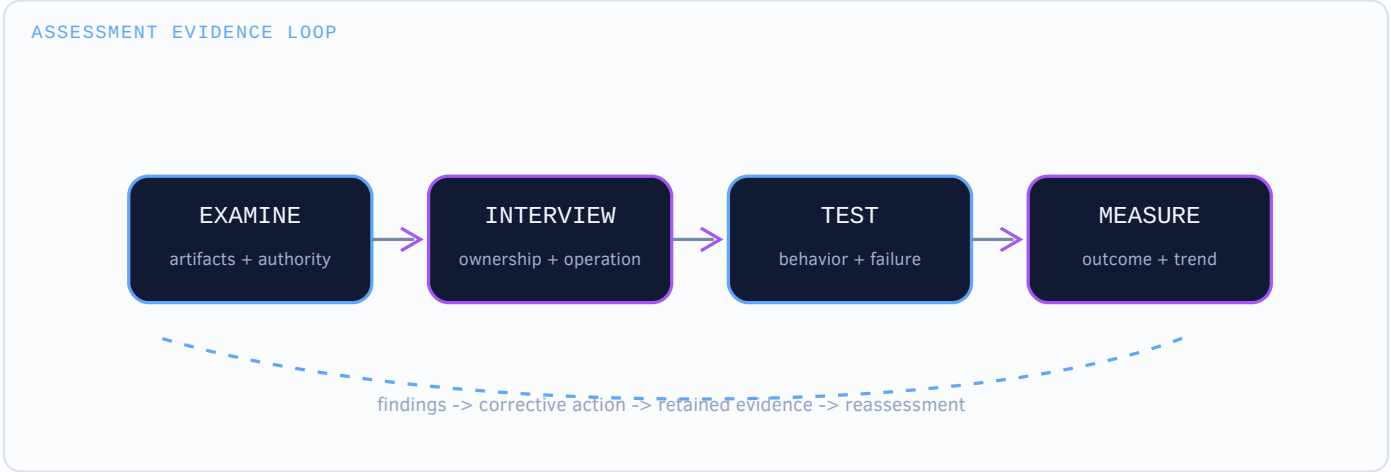
31. Limitations and Residual Risk from Source Draft

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
Objective attainment	Time and request volume meeting defined service objectives	Within approved error budget
Change failure rate	Changes causing rollback, incident, hotfix, or objective breach	Tracked by service and risk class; declining trend

Metric	Definition	Expected use or target
Recovery performance	Observed recovery time and point versus objectives	Meets objective in exercises and incidents
Detection and containment time	Elapsed time from impact to detection and containment	Risk-defined; trend reviewed
Operational-readiness coverage	Production capabilities with current owners, SLOs, runbooks, telemetry, rollback, and recovery evidence	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.

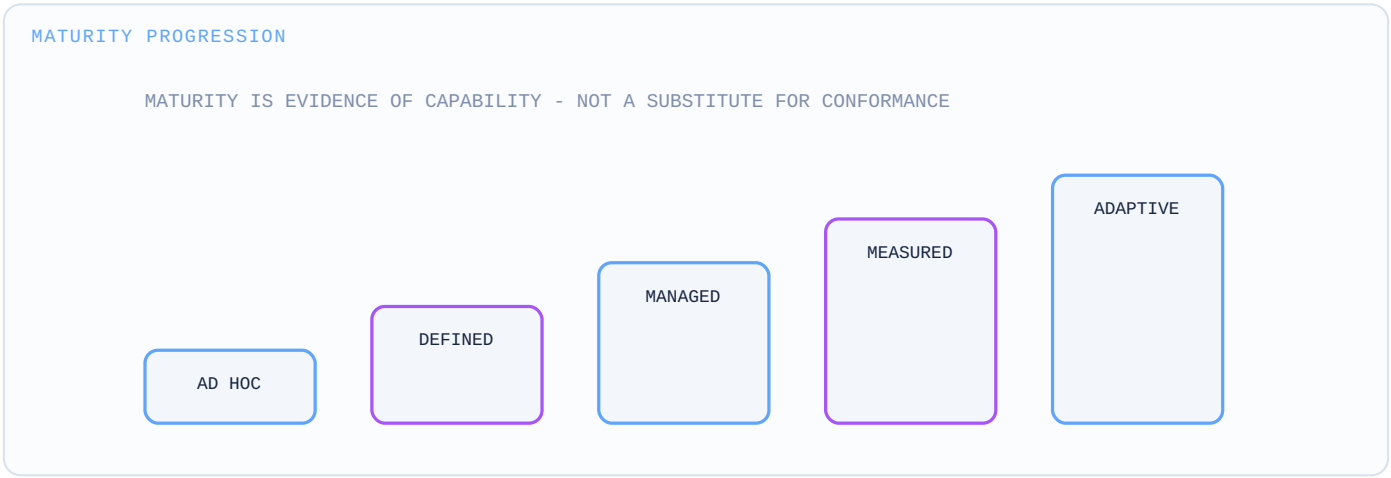
34. Exceptions and Compensating Controls

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
services without current owner	Defined by the adopting organization with owner, source, target, and cadence.
SLO attainment and error-budget consumption	Defined by the adopting organization with owner, source, target, and cadence.
changes causing incident or rollback	Defined by the adopting organization with owner, source, target, and cadence.
release gate overrides	Defined by the adopting organization with owner, source, target, and cadence.
mean time to detect, contain, restore, and learn	Defined by the adopting organization with owner, source, target, and cadence.
restore tests meeting objectives	Defined by the adopting organization with owner, source, target, and cadence.
critical dependencies beyond patch target	Defined by the adopting organization with owner, source, target, and cadence.
deprecated interfaces past retirement date	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
ISO/IEC 20000-1:2018	Service management system requirements	https://www.iso.org/standard/70636.html	Published	2026-09-17
ISO 22301:2019	Business continuity management systems	https://www.iso.org/standard/75106.html	Published	2026-09-17
ISO/IEC/IEEE 15288:2023	System life cycle processes	https://www.iso.org/standard/81702.html	Published	2026-09-17
NIST CSF 2.0	Cybersecurity governance and recovery	https://www.nist.gov/cyberframework	Current	2026-09-17
NIST SP 800-53 Rev. 5	Contingency, configuration, incident, maintenance, and audit controls	https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final	Final update 1	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

- Preserves the source draft's release gates, evidence folders, runbooks, rollback discipline, observability, incident management, and current-state lifecycle control.
- Generalizes tool-specific operational recommendations into outcome-based requirements.
- Strengthens service objectives, progressive delivery, configuration authority, dependency retirement, and operational evidence.
- Separates emergency change flexibility from ungoverned bypass.

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-ORL-01	Ownership	Service ownership and catalog	Foundational, Advanced, High Assurance	High	Critical
MYTHOS-FND-ORL-02	Objectives	Service-level indicators and objectives	Foundational, Advanced, High Assurance	High	Critical
MYTHOS-FND-ORL-03	Observability	Observable operational state	Foundational, Advanced, High Assurance	High	Critical
MYTHOS-FND-ORL-04	Readiness	Operational readiness review	Foundational, Advanced, High Assurance	Partial	Critical
MYTHOS-FND-ORL-05	Change	Controlled change management	Foundational, Advanced, High Assurance	High	Critical
MYTHOS-FND-ORL-06	Release	Release authorization and evidence	Foundational, Advanced, High Assurance	High	Critical
MYTHOS-FND-ORL-07	Deployment	Progressive and safe deployment	Advanced, High Assurance	High	Critical
MYTHOS-FND-ORL-08	Configuration	Authoritative configuration and state management	Foundational, Advanced, High Assurance	High	Critical
MYTHOS-FND-ORL-09	Rollback	Rollback and forward-recovery capability	Foundational, Advanced, High Assurance	Partial	Critical
MYTHOS-FND-ORL-10	Runbooks	Operational runbooks and automation	Foundational, Advanced, High Assurance	Partial	Critical

Control	Family	Title	Profiles	Automation	Impact
MYTHOS-FND-ORL-11	Incident	Incident command, containment, and communication	Foundational, Advanced, High Assurance	Partial	Critical
MYTHOS-FND-ORL-12	Problem management	Systemic problem management and learning	Foundational, Advanced, High Assurance	Partial	Material
MYTHOS-FND-ORL-13	Capacity	Capacity, performance, and demand management	Foundational, Advanced, High Assurance	High	Critical
MYTHOS-FND-ORL-14	Recovery	Backup, restore, and continuity	Foundational, Advanced, High Assurance	Partial	Critical
MYTHOS-FND-ORL-15	Maintenance	Vulnerability, patch, and dependency lifecycle	Foundational, Advanced, High Assurance	High	Critical
MYTHOS-FND-ORL-16	Data operations	Operational data integrity and maintenance	Foundational, Advanced, High Assurance	High	Critical
MYTHOS-FND-ORL-17	Security operations	Operational access and emergency controls	Foundational, Advanced, High Assurance	High	Critical
MYTHOS-FND-ORL-18	Retirement	Controlled deprecation and retirement	Foundational, Advanced, High Assurance	Partial	Critical

Appendix D – Minimum Conformance Claim Record

```
standard: MYTHOS-FND-0005
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

CANDIDATE STANDARD

Mythos Data, API, and Integration Standard

Make data meaning, contracts, interfaces, events, lineage, reliability, and compatibility explicit and testable.

PERMANENT ID
MYTHOS-FND-0006

PUBLICATION CLASS
CANDIDATE STANDARD

VERSION / STATUS
1.0.0-candidate / CANDIDATE

PERMANENT PUBLICATION IDENTITY

Mythos Data, API, and Integration Standard

Universal Requirements for Data Governance, Contracts, APIs, Events, Reliability, Security, Lineage, Compatibility, and Integration Operations

Document ID
MYTHOS-FND-0006

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	19	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	Data, API, integration, and platform engineers; Application and infrastructure architects; Security, privacy, and governance teams; Product and service owners; Operations and reliability engineers
Publisher / owner	Mythos Systems / Standards Program
Public classification	Public technical standard
Canonical route	/library/standards/foundation/mythos-fnd-0006/

Expected outcomes

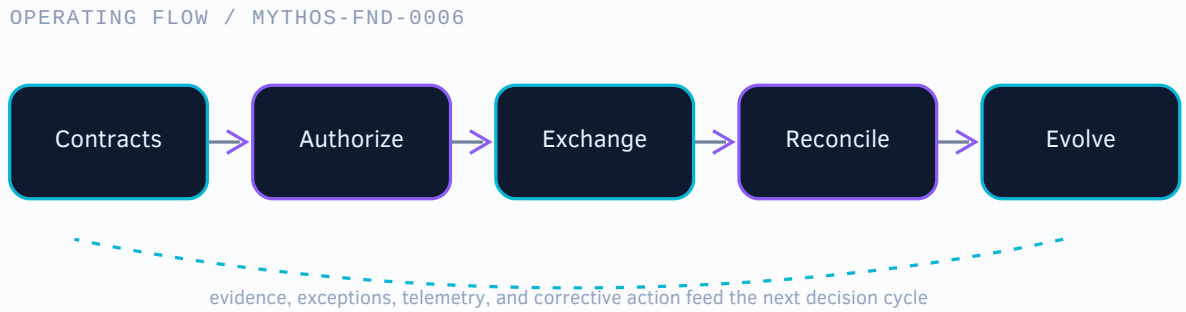
- Make data meaning, ownership, quality, sensitivity, and lifecycle explicit.
- Create stable, testable, evolvable contracts for synchronous and asynchronous integration.
- Prevent distributed failure, duplicate effects, unauthorized access, and silent data corruption.
- Provide evidence for compatibility, lineage, operational health, and deprecation decisions.

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.

Document Control 8

Revision Record 8

How to Use This Standard 9

Executive Reading Path 9

Engineering Reading Path 9

Assessment Reading Path 9

Normative and Informative Content 9

Part I – Executive Direction 10

1. Executive Overview 10

2. Executive Findings and Required Direction 10

3. Business and Operational Impact 10

4. Target-State Summary 11

5. Leadership Responsibilities 12

Part II – Standard Foundation 13

6. Purpose and Objectives 13

7. Scope 13

8. Intended Audience 13

9. Requirements Language and Conformance 13

10. Normative References from Source Draft 13

11. Informative References from Source Draft 14

12. Terms and Definitions 14

13. Applicability and Tailoring 15

Part III – Risk and Architecture 16

14. Enterprise Problem and Risk Landscape 16

15. Governing Principles 16

16. Reference Operating Architecture 16

17. Roles and Accountability 17

18. State, Evidence, and Decision Model 18

19. Security and Trust Considerations 18

20. Failure Modes 18

21. Cross-Functional Dependencies 18

Part IV – Normative Control System **19**

22. Control-Family Overview 19

23. Normative Controls 20

Part V – Implementation and Operations **40**

24. Implementation Profiles 40

25. Implementation Lifecycle 40

26. Integration Requirements 41

27. Failure Handling and Recovery 41

28. Exceptions and Compensating Controls 41

29. Prohibited Practices 41

30. Adoption Roadmap from Source Draft 42

31. Limitations and Residual Risk from Source Draft 42

Part VI – Assurance and Assessment **43**

32. Assessment Methodology 43

33. Metrics and Reporting from Source Draft 43

34. Exceptions and Compensating Controls 44

35. Enterprise Metric Set 44

36. Maturity Model 45

37. Assessment Confidence 45

38. Executive Assurance Dashboard 45

Part VII – Authority and Traceability **47**

39. Cross-Standard Dependencies from Source Draft 47

40. Current External Authority Register 47

41. Control Traceability 47

42. Source-Draft Preservation 48

Part VIII – Appendices **49**

Appendix A — Source-Draft Evolution Notes 49

Appendix B — Change History 49

Appendix C — Control Summary 49

Appendix D — Minimum Conformance Claim Record 50

Appendix E — Publication Review Checklist 50

NORMATIVE SYSTEM

Control index

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

MYTHOS-FND-DAI-01	Data and integration ownership	21
MYTHOS-FND-DAI-02	Data classification and permitted use	22
MYTHOS-FND-DAI-03	Versioned data contracts	23
MYTHOS-FND-DAI-04	Consistent resource and operation design	24
MYTHOS-FND-DAI-05	Identity, authorization, and tenant context	25
MYTHOS-FND-DAI-06	Idempotency and duplicate-effect control	26
MYTHOS-FND-DAI-07	Concurrency, ordering, and consistency	27
MYTHOS-FND-DAI-08	Structured errors and failure semantics	28
MYTHOS-FND-DAI-09	Rate limits, quotas, backpressure, and admission control	29
MYTHOS-FND-DAI-10	Event and messaging semantics	30
MYTHOS-FND-DAI-11	Data quality objectives and controls	31
MYTHOS-FND-DAI-12	Lineage, provenance, and transformation accountability	32
MYTHOS-FND-DAI-13	Integration observability and reconciliation	33
MYTHOS-FND-DAI-14	Dependency failure and retry control	34
MYTHOS-FND-DAI-15	Schema and data migration safety	35
MYTHOS-FND-DAI-16	Versioning, compatibility, and deprecation	36
MYTHOS-FND-DAI-17	Third-party integration boundary control	37
MYTHOS-FND-DAI-18	Contract, compatibility, and failure testing	38
MYTHOS-FND-DAI-19	Discoverable interface documentation	39

Document Control

Field	Value
Document ID	MYTHOS-FND-0006
Standard	Data, API, and Integration
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

Enterprise systems fail at boundaries. Data changes meaning, requests are duplicated, events arrive out of order, dependencies throttle or disappear, and undocumented compatibility assumptions become production outages. This standard defines the contract and operating discipline required for data, APIs, events, and integrations to remain secure, observable, evolvable, and accountable.

The institutional objective is to establish durable contracts, data authority, identity context, failure semantics, lineage, observability, compatibility, and lifecycle controls for data exchange and system integration. 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
Contract ambiguity	Consumers infer behavior from examples or implementation rather than versioned contracts.	Use explicit schemas, operation semantics, compatibility rules, and ownership.
Duplicate and concurrent effects	Retries and concurrent updates create unintended repeated or lost actions.	Define idempotency, concurrency, ordering, and conflict semantics.
Identity and tenant leakage	Integration context is lost or inconsistently enforced across boundaries.	Propagate authenticated identity, authorization, purpose, and tenant context.
Failure hidden as success	Unstructured errors and partial outcomes prevent reliable recovery.	Define machine-readable errors, indeterminate outcomes, retries, and reconciliation.
Third-party dependency opacity	External service limits, changes, and outages are not governed as product risk.	Maintain dependency contracts, quotas, health, fallback, exit, and evidence.

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.

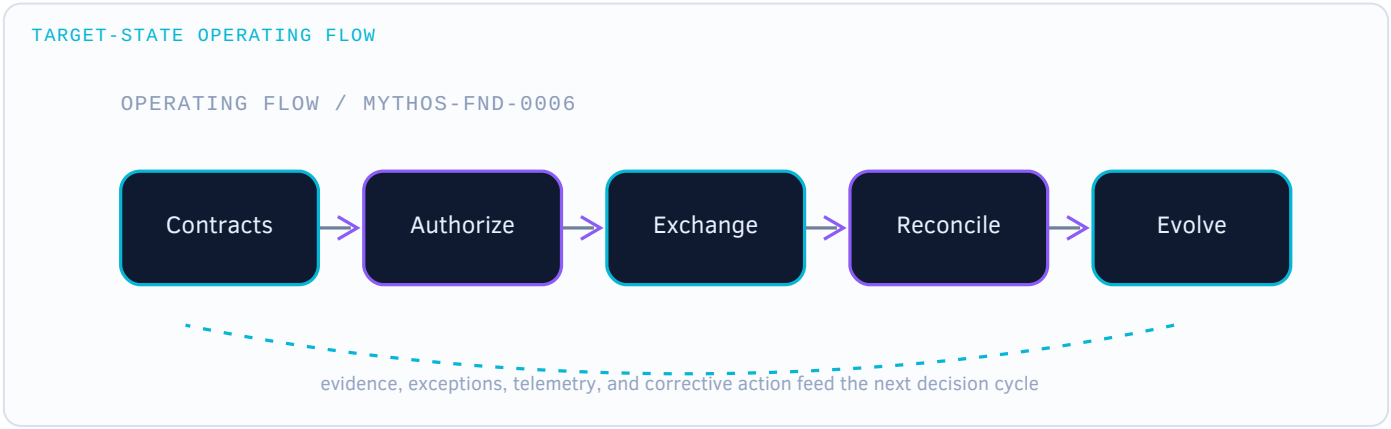
3.3 Security, Privacy, and Trust Impact

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	Data and integration ownership
2	Classification and permitted use
3	Versioned schemas and contracts
4	Resource and operation design
5	Identity and tenant context
6	Idempotency and duplicate-effect control
7	Concurrency, ordering, and consistency
8	Structured errors and failure states
9	Rate limits, quotas, backpressure, and admission
10	Events and messaging
11	Data quality and lineage
12	Observability and reconciliation
13	Retry and dependency failure
14	Migration and compatibility

#	Target-State Component
15	Third-party boundary control
16	Contract and failure testing
17	Discoverable documentation

```
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
Data owner	Owns meaning, permitted use, quality, retention, and authority.
API or integration owner	Owns contract, compatibility, operations, and support.
Domain architect	Defines resource, event, and consistency boundaries.
Security and privacy lead	Approves identity, authorization, data movement, and retention.
Platform engineering	Provides gateways, schemas, messaging, telemetry, and policy enforcement.
Consumer owner	Validates use and migration obligations.
Reliability owner	Defines retry, backpressure, failure, and reconciliation.
Independent assessor	Tests contract and operational behavior.

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

- Make data meaning, ownership, quality, sensitivity, and lifecycle explicit.
- Create stable, testable, evolvable contracts for synchronous and asynchronous integration.
- Prevent distributed failure, duplicate effects, unauthorized access, and silent data corruption.
- Provide evidence for compatibility, lineage, operational health, and deprecation decisions.

7. Scope

Applies to databases, files, messages, event streams, APIs, webhooks, batch transfers, device protocols, data pipelines, caches, search indexes, analytics, model data paths, and third-party integrations.

8. Intended Audience

- Data, API, integration, and platform engineers
- Application and infrastructure architects
- Security, privacy, and governance teams
- Product and service owners
- Operations and reliability engineers

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

- **OpenAPI Specification 3.2.1** — OpenAPI Initiative specification. https://spec.openapis.org/oas/v3.2.1.html
- **JSON Schema Draft 2020-12** — JSON Schema Core and Validation. https://json-schema.org/draft/2020-12
- **AsyncAPI Specification 3.1.0** — AsyncAPI Initiative specification. https://www.asyncapi.com/docs/reference/specification/v3.1.0
- **CloudEvents 1.0.2** — Cloud Native Computing Foundation event format. https://github.com/cloudevents/spec/tree/v1.0.2
- **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
- **NIST Privacy Framework 1.0** — A Tool for Improving Privacy through Enterprise Risk Management. https://www.nist.gov/privacy-framework/privacy-framework
- **ISO/IEC 25010:2023** — Systems and software Quality Requirements and Evaluation — Product quality model. https://www.iso.org/standard/78176.html
- **NIST SP 800-218 v1.1** — Secure Software Development Framework (SSDF). https://csrc.nist.gov/pubs/sp/800/218/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.
Data contract	A versioned agreement defining data semantics, schema, quality, ownership, access, lifecycle, and compatibility expectations.
Idempotency	The property that repeated processing of the same logical request or event does not create unintended additional effects.
Lineage	The recorded origin, transformations, movement, and use of data or derived artifacts.

Term	Definition
Compatibility window	The period and version range during which producers and consumers are expected to interoperate.
Integration boundary	A change in ownership, trust, protocol, data semantics, availability, or operational responsibility.

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.

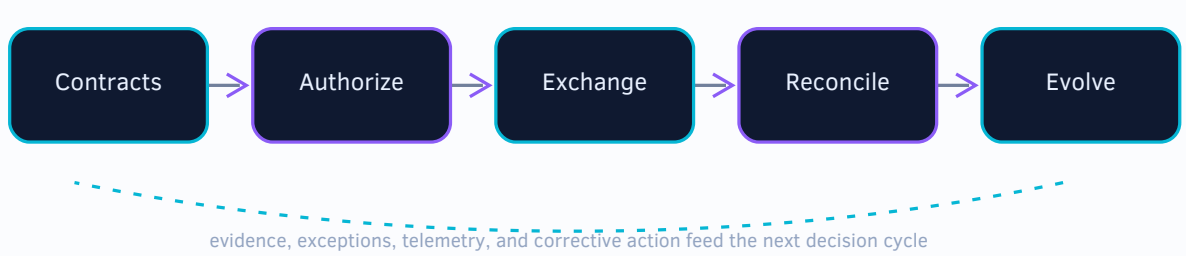
Adopting organizations SHOULD maintain a domain-specific risk register that identifies cause, affected asset or stakeholder, credible scenario, impact, existing controls, residual risk, owner, review trigger, and evidence. Risks that cross standards MUST be linked rather than copied into disconnected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

15. Governing Principles

- Data and interfaces have accountable owners and explicit contracts.
- Compatibility is designed and tested, not assumed.
- At-least-once delivery and partial failure are normal distributed-system conditions.
- Authorization is enforced at the authoritative boundary and at the resource level.
- Data quality, lineage, retention, and privacy follow derived data and secondary stores.
- Third-party integration failures must be contained and observable.

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
Data owner	Owns meaning, permitted use, quality, retention, and authority.
API or integration owner	Owns contract, compatibility, operations, and support.
Domain architect	Defines resource, event, and consistency boundaries.
Security and privacy lead	Approves identity, authorization, data movement, and retention.
Platform engineering	Provides gateways, schemas, messaging, telemetry, and policy enforcement.
Consumer owner	Validates use and migration obligations.
Reliability owner	Defines retry, backpressure, failure, and reconciliation.
Independent assessor	Tests contract and operational behavior.

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
Using documentation examples as the only contract	Failure can create hidden risk, misleading assurance, uncontrolled cost, or unsafe operation.
Retries without idempotency analysis	Failure can create hidden risk, misleading assurance, uncontrolled cost, or unsafe operation.
Returning generic errors without machine-readable cause	Failure can create hidden risk, misleading assurance, uncontrolled cost, or unsafe operation.
Assuming exactly-once delivery without an effect strategy	Failure can create hidden risk, misleading assurance, uncontrolled cost, or unsafe operation.
Embedding tenant identity only in request payload	Failure can create hidden risk, misleading assurance, uncontrolled cost, or unsafe operation.
Changing schemas in place without compatibility testing	Failure can create hidden risk, misleading assurance, uncontrolled cost, or unsafe operation.
Integrating third parties without exit or degraded-mode design	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 **19 controls** across the following families:

- Governance
- Classification
- Contracts
- API design
- Authorization
- Reliability
- Concurrency
- Errors
- Flow control
- Events
- Quality
- Lineage
- Observability
- Resilience
- Migrations
- Lifecycle
- Third parties
- Testing

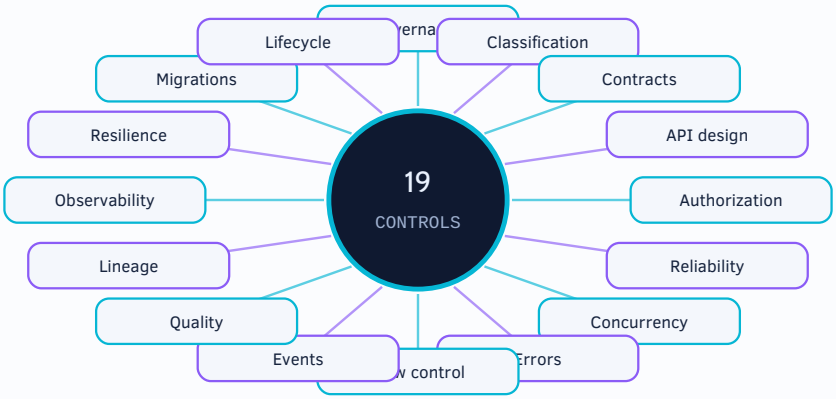
- Documentation

23. Normative Controls

CONTROL SET	PROFILES	ASSESSMENT
19	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-DAI-01 – Data and integration ownership

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

Requirement

Every material data domain, data product, API, event channel, pipeline, and external integration MUST have accountable ownership for semantics, access, quality, lifecycle, compatibility, and operational support.

Purpose

Prevents ownerless interfaces and ambiguous responsibility for data defects or breaking changes.

Applicability

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

Implementation guidance

- Separate producer, consumer, platform, and business ownership where useful.
- Record criticality, support expectations, and escalation.
- Review ownership after organizational or supplier change.

Required evidence

- Data and interface catalog
- Ownership records
- Escalation tests

Assessment procedure

- **Examine:** Sample catalog entries against deployed systems.
- **Interview:** Interview owners and consumers.
- **Test:** Review unowned or stale entries.

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 CSF 2.0 — ID.AM and GV.RR

NORMATIVE CONTROL

MYTHOS-FND-DAI-02 – Data classification and permitted use

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

Requirement

Data fields, records, streams, files, embeddings, indexes, logs, and derived outputs MUST inherit or receive classification, purpose, access, residency, retention, integrity, and privacy handling requirements.

Purpose

Ensures protections follow data across transformations and secondary stores.

Applicability

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

Implementation guidance

- Classify unknown or mixed data conservatively.
- Record sensitive-field semantics in schemas.
- Prevent lower-classification outputs when transformations do not reliably remove sensitivity.

Required evidence

- Classification map
- Schema annotations
- Handling-policy tests

Assessment procedure

- **Examine:** Trace sensitive data through a pipeline.
- **Interview:** Inspect caches and logs.
- **Test:** Test enforcement of residency or export restrictions.

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 — RA-2, MP family
- NIST Privacy Framework

NORMATIVE CONTROL

MYTHOS-FND-DAI-03 – Versioned data contracts

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

Requirement

Material data exchanges MUST have versioned contracts defining semantics, schema, required and optional fields, identifiers, units, nullability, quality expectations, ownership, security, lifecycle, and compatibility rules.

Purpose

Prevents syntactically valid but semantically incompatible integration.

Applicability

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

Implementation guidance

- Use machine-readable schemas where practical.
- Define examples and counterexamples.
- Treat semantic changes as potentially breaking even when syntax is unchanged.

Required evidence

- Data contracts
- Schema repository
- Contract review records

Assessment procedure

- **Examine:** Validate samples and counterexamples.
- **Interview:** Interview producer and consumer about field meaning.
- **Test:** Detect an undeclared semantic change in a test workflow.

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
- OpenAPI 3.2.1

NORMATIVE CONTROL

MYTHOS-FND-DAI-04 – Consistent resource and operation design

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

Requirement

APIs MUST define stable resource or operation semantics, authentication, authorization, request and response schemas, status and error behavior, limits, idempotency expectations, versioning, and lifecycle status in an authoritative specification.

Purpose

Creates predictable, testable interfaces and reduces consumer-specific behavior.

Applicability

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

Implementation guidance

- Use nouns and commands consistently.
- Model asynchronous operations explicitly.
- Document partial success, long-running operations, and cancellation.
- Avoid exposing internal implementation structures as accidental contracts.

Required evidence

- API specification
- Design review
- Conformance tests

Assessment procedure

- **Examine:** Validate implementation against specification.
- **Interview:** Test undocumented fields and behavior.
- **Test:** Review consistency across similar APIs.

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

- OpenAPI Specification 3.2.1

NORMATIVE CONTROL

MYTHOS-FND-DAI-05 – Identity, authorization, and tenant context

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

Requirement

Every integration request, event publication, subscription, data operation, and administrative action MUST be authorized at an authoritative enforcement point using current identity, scope, resource, tenant or trust-domain context, and policy.

Purpose

Prevents confused-deputy, cross-tenant, frontend-only, and overly broad service access.

Applicability

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

Implementation guidance

- Use workload identities and narrow scopes.
- Propagate context through asynchronous paths with integrity protection.
- Do not trust caller-supplied tenant identifiers without binding to identity and policy.

Required evidence

- Authorization policy
- Identity and scope inventory
- Negative tests

Assessment procedure

- **Examine:** Attempt direct unauthorized access.
- **Interview:** Replay an event under a different tenant.
- **Test:** Test revoked scopes.

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 and IA families

NORMATIVE CONTROL

MYTHOS-FND-DAI-06 – Idempotency and duplicate-effect control

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

Requirement

Operations that may be retried, replayed, duplicated, or resumed MUST define idempotency or duplicate-detection behavior and preserve enough state to prevent unintended repeated effects.

Purpose

Addresses normal distributed-system delivery behavior and uncertain outcomes.

Applicability

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

Implementation guidance

- Use client or server idempotency keys for consequential commands.
- Define retention and conflict behavior.
- Make consumers resilient to duplicate events.
- Distinguish safe reads from mutating actions.

Required evidence

- Idempotency design
- Duplicate and replay tests
- State records

Assessment procedure

- **Examine:** Submit duplicate and concurrent requests.
- **Interview:** Replay events after restart.
- **Test:** Verify conflicting keys fail safely.

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

- CloudEvents 1.0.2 — event identity

NORMATIVE CONTROL

MYTHOS-FND-DAI-07 – Concurrency, ordering, and consistency

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

Requirement

Data and integration designs MUST state and enforce concurrency, ordering, transactional, consistency, conflict, and stale-read semantics for operations where competing actions can affect correctness.

Purpose

Prevents lost updates, double execution, inconsistent decisions, and hidden assumptions about distributed state.

Applicability

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

Implementation guidance

- Use optimistic concurrency, leases, sequencing, partition keys, or transactions as appropriate.
- Document where eventual consistency is acceptable.
- Define reconciliation and conflict resolution.

Required evidence

- Consistency model
- Concurrency tests
- Reconciliation procedures

Assessment procedure

- **Examine:** Run concurrent conflicting operations.
- **Interview:** Reorder events.
- **Test:** Verify conflict evidence and recovery.

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 25010:2023 — reliability and functional correctness

NORMATIVE CONTROL

MYTHOS-FND-DAI-08 – Structured errors and failure semantics

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

Requirement

Interfaces MUST return structured, stable, non-sensitive error information that distinguishes caller errors, authorization denial, conflicts, throttling, dependency failure, transient unavailability, and internal failure and provides correlation for support.

Purpose

Enables safe recovery without leaking secrets or forcing consumers to parse human text.

Applicability

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

Implementation guidance

- Use stable machine codes and human-readable messages.
- Define retryability and backoff hints.
- Preserve root-cause detail in protected telemetry rather than public responses.

Required evidence

- Error catalog
- Contract tests
- Redaction review

Assessment procedure

- **Examine:** Trigger each major error class.
- **Interview:** Verify clients do not retry permanent failures.
- **Test:** Inspect responses for sensitive content.

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

- OpenAPI 3.2.1

NORMATIVE CONTROL

MYTHOS-FND-DAI-09 – Rate limits, quotas, backpressure, and admission control

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

Requirement

APIs, event systems, pipelines, and integrations MUST define and enforce capacity limits, quotas, backpressure, queue bounds, timeout budgets, and overload behavior proportionate to service and tenant risk.

Purpose

Prevents cascading failure, unfair resource capture, and unbounded queues.

Applicability

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

Implementation guidance

- Expose limits and reset behavior.
- Prioritize critical workloads.
- Bound retries and concurrency.
- Use dead-letter or quarantine paths with operational ownership.

Required evidence

- Limit policy
- Load and overload tests
- Queue and retry telemetry

Assessment procedure

- **Examine:** Exceed quotas and capacity.
- **Interview:** Verify graceful degradation.
- **Test:** Inspect unbounded or ownerless queues.

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 25010:2023 — performance efficiency and reliability

NORMATIVE CONTROL

MYTHOS-FND-DAI-10 – Event and messaging semantics

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

Requirement

Event channels MUST define event identity, source, type, time semantics, subject, schema, ordering scope, delivery guarantee, retention, replay, consumer ownership, sensitive-data handling, and evolution policy.

Purpose

Makes asynchronous behavior explicit and operable.

Applicability

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

Implementation guidance

- Use a standard envelope such as CloudEvents where appropriate.
- Separate facts from commands.
- Define poison-message handling and replay authorization.
- Avoid embedding mutable external state without version or reference.

Required evidence

- Event catalog
- AsyncAPI or equivalent specification
- Replay and poison-message tests

Assessment procedure

- **Examine:** Inspect sampled events.
- **Interview:** Replay across schema versions.
- **Test:** Test unauthorized subscription or replay.

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

- AsyncAPI 3.1.0
- CloudEvents 1.0.2

NORMATIVE CONTROL

MYTHOS-FND-DAI-11 – Data quality objectives and controls

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

Requirement

Critical data products and fields MUST have defined and monitored quality objectives for accuracy, completeness, validity, consistency, timeliness, uniqueness, lineage, and fitness for intended use.

Purpose

Prevents technically available but misleading or unsafe data from being treated as trustworthy.

Applicability

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

Implementation guidance

- Define ownership and thresholds by use case.
- Quarantine, annotate, or block data that fails critical constraints.
- Distinguish observed quality from inferred confidence.

Required evidence

- Data quality specification
- Quality dashboard
- Exception and remediation records

Assessment procedure

- **Examine:** Recalculate selected metrics.
- **Interview:** Inject invalid data.
- **Test:** Review downstream behavior when quality falls below threshold.

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 25010:2023 — data-related quality characteristics

NORMATIVE CONTROL

MYTHOS-FND-DAI-12 – Lineage, provenance, and transformation accountability

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

Requirement

Critical data and derived artifacts MUST record source, collection or creation context, transformations, responsible process, versions, timestamps, and integrity information sufficient to reproduce or explain material outputs.

Purpose

Supports audit, debugging, privacy, model governance, and correction of upstream defects.

Applicability

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

Implementation guidance

- Capture field-level lineage where consequence warrants.
- Include manual edits and external enrichments.
- Preserve provenance across exports and model inputs.

Required evidence

- Lineage graph
- Transformation manifests
- Reproduction records

Assessment procedure

- **Examine:** Trace an output to original sources.
- **Interview:** Change an upstream record and identify affected derivatives.
- **Test:** Verify provenance survives export or handoff.

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 AI 600-1 — provenance
- NIST SP 800-53 — AU family

NORMATIVE CONTROL

MYTHOS-FND-DAI-13 – Integration observability and reconciliation

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

Requirement

Integrations MUST expose end-to-end correlation, success and failure outcomes, latency, retry, queue, freshness, volume, schema, and reconciliation signals sufficient to detect silent loss, duplication, delay, or corruption.

Purpose

Makes distributed data movement diagnosable and measurable.

Applicability

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

Implementation guidance

- Use business reconciliation in addition to transport metrics.
- Monitor expected absence and stale data.
- Correlate across asynchronous boundaries without leaking sensitive payloads.

Required evidence

- Telemetry specification
- Reconciliation reports
- Alert tests

Assessment procedure

- **Examine:** Trace a transaction or batch end to end.
- **Interview:** Drop or duplicate a message in a test environment.
- **Test:** Verify alerts and reconciliation identify the issue.

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-12, SI-4

NORMATIVE CONTROL

MYTHOS-FND-DAI-14 – Dependency failure and retry control

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

Requirement

Integrations MUST define timeout, retry, backoff, circuit breaking, fallback, cache, compensation, and manual reconciliation behavior based on operation semantics and dependency failure modes.

Purpose

Prevents retry storms, cascading failure, stale authority, and duplicate side effects.

Applicability

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

Implementation guidance

- Use deadline budgets across call chains.
- Do not retry non-idempotent actions without protection.
- Define stale-data limits and user-visible degraded state.
- Test provider throttling and partial response.

Required evidence

- Resilience policy
- Failure-injection results
- Fallback and reconciliation procedures

Assessment procedure

- **Examine:** Disable or slow a dependency.
- **Interview:** Verify retries are bounded.
- **Test:** Inspect correctness under stale or partial data.

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 25010:2023 — reliability

NORMATIVE CONTROL

MYTHOS-FND-DAI-15 – Schema and data migration safety

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

Requirement

Schema and data migrations MUST be versioned, reviewed, tested at representative scale, observable, resumable or safely restartable, compatible with deployment sequence, backed by recovery points, and verified through reconciliation.

Purpose

Controls one of the most common sources of irreversible production failure.

Applicability

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

Implementation guidance

- Prefer expand-and-contract changes.
- Avoid long blocking operations without explicit impact control.
- Test mixed-version clients.
- Record irreversible transformations.

Required evidence

- Migration plan and scripts
- Scale and compatibility tests
- Reconciliation and rollback evidence

Assessment procedure

- **Examine:** Interrupt and resume a migration.
- **Interview:** Run old and new clients concurrently.
- **Test:** Verify data invariants.

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 — CM-3 and SI-7

NORMATIVE CONTROL

MYTHOS-FND-DAI-16 – Versioning, compatibility, and deprecation

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

Requirement

Interfaces and schemas MUST have a documented versioning and compatibility policy, supported-version window, deprecation notice, migration path, consumer discovery, and retirement verification.

Purpose

Allows evolution without surprise breakage or indefinite support burden.

Applicability

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

Implementation guidance

- Differentiate additive, behavior-changing, and breaking changes.
- Measure actual use before retirement.
- Keep security fixes possible within support windows.

Required evidence

- Version policy
- Consumer and usage records
- Deprecation and retirement evidence

Assessment procedure

- **Examine:** Test a compatibility claim.
- **Interview:** Identify unknown consumers.
- **Test:** Verify retired versions no longer receive traffic.

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

- OpenAPI 3.2.1
- AsyncAPI 3.1.0

NORMATIVE CONTROL

MYTHOS-FND-DAI-17 – Third-party integration boundary control

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

Requirement

Third-party integrations MUST be treated as untrusted and failure-prone boundaries with explicit data disclosure, identity, rate, retention, contract, security, privacy, availability, observability, incident, and exit requirements.

Purpose

Contains external risk and prevents supplier behavior from becoming implicit system policy.

Applicability

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

Implementation guidance

- Use provider adapters or anti-corruption layers for critical dependencies.
- Validate responses and signatures.
- Document provider data use and subprocessor implications.
- Maintain replacement or degraded-mode plans.

Required evidence

- Provider assessment
- Integration boundary design
- Exit and failure tests

Assessment procedure

- **Examine:** Return malformed or malicious provider data.
- **Interview:** Disable the provider.
- **Test:** Verify data disclosure matches approval.

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-DAI-18 – Contract, compatibility, and failure testing

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

Requirement

Data and integration changes MUST pass automated contract, schema, authorization, compatibility, idempotency, concurrency, performance, and failure-path tests appropriate to risk before promotion.

Purpose

Turns interface expectations into enforceable evidence.

Applicability

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

Implementation guidance

- Run provider and consumer tests.
- Use malformed, boundary, delayed, duplicated, and out-of-order inputs.
- Preserve representative fixtures without exposing sensitive data.

Required evidence

- Test suites
- Compatibility matrix
- Failure evidence

Assessment procedure

- **Examine:** Introduce a breaking schema change.
- **Interview:** Replay duplicate and reordered messages.
- **Test:** Attempt unauthorized resource access.

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
- OpenAPI 3.2.1

NORMATIVE CONTROL

MYTHOS-FND-DAI-19 – Discoverable interface documentation

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

Requirement

Consumers MUST have access to current interface and data documentation covering purpose, authentication, authorization, contracts, examples, limits, errors, operational expectations, versioning, deprecation, support, and known limitations.

Purpose

Reduces unsafe reverse engineering and inconsistent consumer behavior.

Applicability

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

Implementation guidance

- Generate documentation from authoritative contracts where practical.
- Validate examples.
- Separate public, partner, and internal access while preserving required operational knowledge.

Required evidence

- Developer portal or documentation
- Example validation results
- Support and change records

Assessment procedure

- **Examine:** Complete a representative integration from documentation.
- **Interview:** Verify examples compile or validate.
- **Test:** Check superseded versions are clearly labeled.

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 26514:2022

FOUNDATION STANDARD / STRUCTURAL PART

Part V – Implementation and Operations

24. Implementation Profiles

Profile	Required Operating State
Baseline	Owned data and APIs, classification, versioned contracts, identity, idempotency, errors, limits, observability, migration, compatibility, and documentation.
Enterprise	Central schema registry, automated contract testing, event governance, lineage, policy enforcement, reconciliation, consumer analytics, and managed third-party gateways.
High Assurance	Cryptographic message integrity, formal compatibility analysis, deterministic replay, independently tested failure semantics, strict tenant isolation, signed contracts, and continuous reconciliation.

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

- Using documentation examples as the only contract
- Retries without idempotency analysis
- Returning generic errors without machine-readable cause
- Assuming exactly-once delivery without an effect strategy
- Embedding tenant identity only in request payload
- Changing schemas in place without compatibility testing
- Integrating third parties without exit or degraded-mode design

30. Adoption Roadmap from Source Draft

- Establish ownership, classification, data contracts, interface inventory, and authoritative schemas.
- Standardize API, event, error, authorization, versioning, and reliability behaviors.
- Add lineage, quality objectives, observability, migration, retention, and third-party resilience.
- Automate contract generation, validation, compatibility testing, policy enforcement, and deprecation monitoring.
- For High Assurance, add integrity protection, replay testing, fault injection, independent contract review, and continuous data reconciliation.

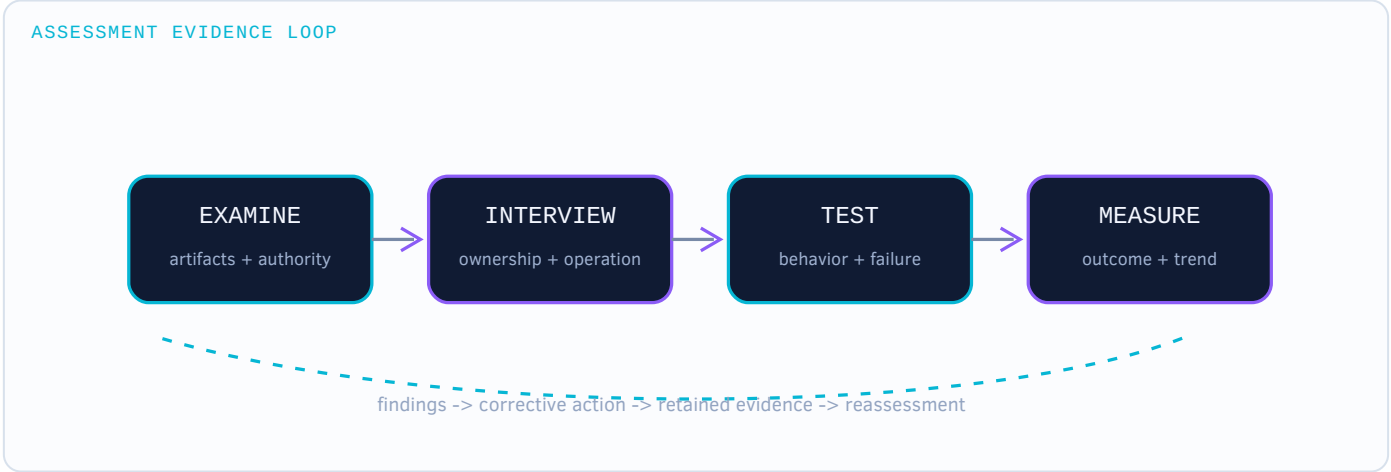
31. Limitations and Residual Risk from Source Draft

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
Contract coverage	Production integrations represented by current versioned contracts	100% material integrations
	Undeclared incompatible changes reaching consumers	0

Metric	Definition	Expected use or target
Breaking-change escape rate		
Data quality objective attainment	Critical data products meeting defined quality objectives	Within approved thresholds
Integration recovery rate	Failed operations safely retried, reconciled, or compensated	Risk-defined; all critical paths tested
Lineage completeness	Critical fields and derived artifacts with source and transformation lineage	>= 95% Advanced; 100% selected High Assurance scope

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.

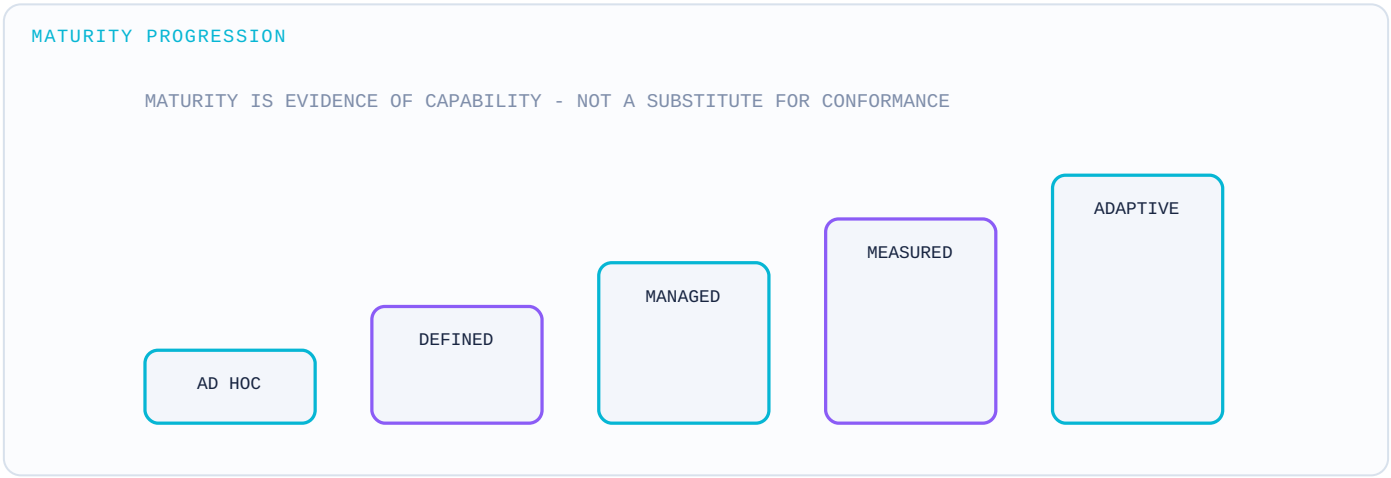
34. Exceptions and Compensating Controls

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
interfaces with current owner and contract	Defined by the adopting organization with owner, source, target, and cadence.
breaking changes without approved migration	Defined by the adopting organization with owner, source, target, and cadence.
duplicate-effect incidents	Defined by the adopting organization with owner, source, target, and cadence.
requests ending indeterminate without reconciliation	Defined by the adopting organization with owner, source, target, and cadence.
schema validation failures	Defined by the adopting organization with owner, source, target, and cadence.
consumer versions beyond support window	Defined by the adopting organization with owner, source, target, and cadence.
third-party errors and quota saturation	Defined by the adopting organization with owner, source, target, and cadence.
data quality objectives outside target	Defined by the adopting organization with owner, source, target, and cadence.
events without lineage or correlation	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
OpenAPI Specification 3.2.1	Language-agnostic HTTP API description	https://spec.openapis.org/oas/v3.2.1.html	Current 3.2 patch release	2026-09-17
JSON Schema 2020-12	JSON structure and validation	https://json-schema.org/draft/2020-12	Current published dialect	2026-09-17
RFC 9110	HTTP Semantics	https://www.rfc-editor.org/rfc/rfc9110	Internet Standard	2026-09-17
RFC 9457	Problem Details for HTTP APIs	https://www.rfc-editor.org/info/rfc9457/	Proposed Standard	2026-09-17
RFC 9421	HTTP Message Signatures	https://www.rfc-editor.org/info/rfc9421/	Proposed Standard	2026-09-17
RFC 9530	Digest Fields	https://www.rfc-editor.org/info/rfc9530/	Proposed Standard	2026-09-17
CloudEvents 1.0.2	Event envelope specification	https://github.com/cloudevents/spec/blob/v1.0.2/cloudevents/spec.md	Released	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

- Preserves the source draft's contract-first approach, provider abstraction, repository and data-store guidance, migration safety, and explicit integration boundaries.
- Generalizes database- and framework-specific prescriptions into outcome-based controls.
- Adds event semantics, idempotency, backpressure, lineage, deprecation telemetry, and third-party containment.
- Aligns API documentation with current OpenAPI, JSON Schema, AsyncAPI, and CloudEvents specifications.

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-DAI-01	Governance	Data and integration ownership	Foundational, Advanced, High Assurance	High	Critical
MYTHOS-FND-DAI-02	Classification	Data classification and permitted use	Foundational, Advanced, High Assurance	High	Critical
MYTHOS-FND-DAI-03	Contracts	Versioned data contracts	Foundational, Advanced, High Assurance	High	Critical
MYTHOS-FND-DAI-04	API design	Consistent resource and operation design	Foundational, Advanced, High Assurance	High	Critical
MYTHOS-FND-DAI-05	Authorization	Identity, authorization, and tenant context	Foundational, Advanced, High Assurance	High	Critical
MYTHOS-FND-DAI-06	Reliability	Idempotency and duplicate-effect control	Foundational, Advanced, High Assurance	High	Critical
MYTHOS-FND-DAI-07	Concurrency	Concurrency, ordering, and consistency	Foundational, Advanced, High Assurance	Partial	Critical
MYTHOS-FND-DAI-08	Errors	Structured errors and failure semantics	Foundational, Advanced, High Assurance	High	Material
MYTHOS-FND-DAI-09	Flow control	Rate limits, quotas, backpressure, and admission control	Foundational, Advanced, High Assurance	High	Critical
MYTHOS-FND-DAI-10	Events	Event and messaging semantics	Foundational, Advanced, High Assurance	High	Critical

Control	Family	Title	Profiles	Automation	Impact
MYTHOS-FND-DAI-11	Quality	Data quality objectives and controls	Foundational, Advanced, High Assurance	High	Critical
MYTHOS-FND-DAI-12	Lineage	Lineage, provenance, and transformation accountability	Advanced, High Assurance	High	Critical
MYTHOS-FND-DAI-13	Observability	Integration observability and reconciliation	Foundational, Advanced, High Assurance	High	Critical
MYTHOS-FND-DAI-14	Resilience	Dependency failure and retry control	Foundational, Advanced, High Assurance	Partial	Critical
MYTHOS-FND-DAI-15	Migrations	Schema and data migration safety	Foundational, Advanced, High Assurance	High	Critical
MYTHOS-FND-DAI-16	Lifecycle	Versioning, compatibility, and deprecation	Foundational, Advanced, High Assurance	High	Critical
MYTHOS-FND-DAI-17	Third parties	Third-party integration boundary control	Foundational, Advanced, High Assurance	Partial	Critical
MYTHOS-FND-DAI-18	Testing	Contract, compatibility, and failure testing	Foundational, Advanced, High Assurance	High	Critical
MYTHOS-FND-DAI-19	Documentation	Discoverable interface documentation	Foundational, Advanced, High Assurance	Partial	Material

Appendix D – Minimum Conformance Claim Record

```
standard: MYTHOS-FND-0006
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

CANDIDATE STANDARD

Mythos Interface Standards

Design human interfaces that preserve understanding, accessibility, authority, safety, feedback, and recovery.

PERMANENT ID
MYTHOS-FND-0007

PUBLICATION CLASS
CANDIDATE STANDARD

VERSION / STATUS
1.0.0-candidate / CANDIDATE

PERMANENT PUBLICATION IDENTITY

Mythos Interface Standards

Universal Requirements for Human Interfaces, Administrative Surfaces, Accessibility, Safety, Feedback, and Trustworthy Interaction

Document ID
MYTHOS-FND-0007

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	Product and interface designers; Frontend and platform engineers; Accessibility and quality specialists; Security and privacy teams; Operators, administrators, and assessors
Publisher / owner	Mythos Systems / Standards Program
Public classification	Public technical standard
Canonical route	/library/standards/foundation/mythos-fnd-0007/

Expected outcomes

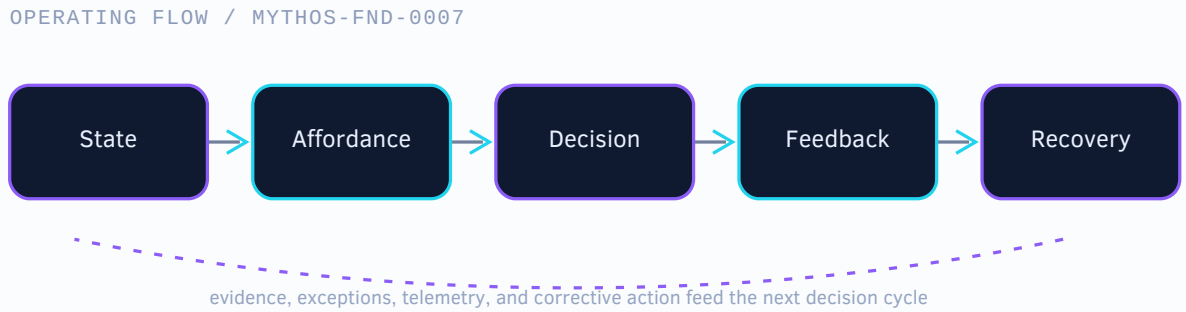
- Make interfaces understandable, accessible, predictable, and safe.
- Prevent visual design from obscuring authority, risk, system state, or irreversible consequences.
- Establish assessable requirements for administrative, operational, consumer, and AI-mediated interfaces.
- Ensure interaction design remains effective under failure, latency, degraded connectivity, and assistive technology.

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.

Document Control 8

Revision Record 8

How to Use This Standard 9

Executive Reading Path 9

Engineering Reading Path 9

Assessment Reading Path 9

Normative and Informative Content 9

Part I – Executive Direction 10

1. Executive Overview 10

2. Executive Findings and Required Direction 10

3. Business and Operational Impact 10

4. Target-State Summary 11

5. Leadership Responsibilities 12

Part II – Standard Foundation 13

6. Purpose and Objectives 13

7. Scope 13

8. Intended Audience 13

9. Requirements Language and Conformance 13

10. Normative References from Source Draft 13

11. Informative References from Source Draft 14

12. Terms and Definitions 14

13. Applicability and Tailoring 15

Part III – Risk and Architecture 16

14. Enterprise Problem and Risk Landscape 16

15. Governing Principles 16

16. Reference Operating Architecture 16

17. Roles and Accountability 17

18. State, Evidence, and Decision Model 18

19. Security and Trust Considerations 18

20. Failure Modes 18

21. Cross-Functional Dependencies 18

Part IV – Normative Control System **19**

22. Control-Family Overview 19

23. Normative Controls 20

Part V – Implementation and Operations **39**

24. Implementation Profiles 39

25. Implementation Lifecycle 39

26. Integration Requirements 40

27. Failure Handling and Recovery 40

28. Exceptions and Compensating Controls 40

29. Prohibited Practices 40

30. Adoption Roadmap from Source Draft 41

31. Limitations and Residual Risk from Source Draft 41

Part VI – Assurance and Assessment **42**

32. Assessment Methodology 42

33. Metrics and Reporting from Source Draft 42

34. Exceptions and Compensating Controls 43

35. Enterprise Metric Set 43

36. Maturity Model 44

37. Assessment Confidence 44

38. Executive Assurance Dashboard 44

Part VII – Authority and Traceability **46**

39. Cross-Standard Dependencies from Source Draft 46

40. Current External Authority Register 46

41. Control Traceability 46

42. Source-Draft Preservation 47

Part VIII – Appendices **48**

Appendix A — Source-Draft Evolution Notes 48

Appendix B — Change History 48

Appendix C — Control Summary 48

Appendix D — Minimum Conformance Claim Record 49

Appendix E — Publication Review Checklist 49

NORMATIVE SYSTEM

Control index

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

MYTHOS-FND-UI-01	Interface ownership and critical-flow inventory	21
MYTHOS-FND-UI-02	Authoritative and unambiguous system state	22
MYTHOS-FND-UI-03	Scope, identity, and environment visibility	23
MYTHOS-FND-UI-04	Safe critical-action design	24
MYTHOS-FND-UI-05	Undo, cancellation, and recovery	25
MYTHOS-FND-UI-06	Accessibility baseline	26
MYTHOS-FND-UI-07	Input validation and constraint communication	27
MYTHOS-FND-UI-08	Timely and actionable feedback	28
MYTHOS-FND-UI-09	Non-sensitive error communication	29
MYTHOS-FND-UI-10	Privacy-respecting interaction	30
MYTHOS-FND-UI-11	Session and sensitive-data handling	31
MYTHOS-FND-UI-12	Consistent interaction semantics	32
MYTHOS-FND-UI-13	Perceived and actual responsiveness	33
MYTHOS-FND-UI-14	Degraded and offline behavior	34
MYTHOS-FND-UI-15	AI-generated output and action boundaries	35
MYTHOS-FND-UI-16	Locale, language, time, and unit correctness	36
MYTHOS-FND-UI-17	Interaction auditability	37
MYTHOS-FND-UI-18	Representative interface validation	38

Document Control

Field	Value
Document ID	MYTHOS-FND-0007
Standard	Interface Standards
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

Interfaces are operational control surfaces. Ambiguous state, hidden scope, inaccessible interaction, unsafe confirmation, or misleading AI presentation can cause the same level of harm as backend defects. This standard defines interfaces as part of the system safety and trust architecture, with particular attention to critical actions, state authority, recovery, accessibility, privacy, degraded behavior, and AI-generated content.

The institutional objective is to establish safe, accessible, comprehensible, responsive, privacy-respecting, and auditable human-system interfaces across ordinary, degraded, critical, and AI-assisted workflows. 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
Ambiguous state	Users cannot tell whether work is proposed, approved, executing, verified, failed, or unknown.	Present authoritative state and its source without relying on color alone.
Unsafe critical actions	Generic confirmation and hidden scope cause destructive mistakes.	Show identity, environment, target, effect, reversibility, and exact action.
Accessibility deferred	Interfaces exclude users and create operational risk when accessibility is treated as polish.	Apply accessibility requirements from design through representative validation.
Recovery omitted	Users cannot cancel, undo, resume, or understand partial completion.	Design cancellation, undo, recovery, and indeterminate states explicitly.
AI presented as authority	Generated suggestions are visually indistinguishable from system facts or executed outcomes.	Label AI content, sources, uncertainty, action boundaries, and verification.

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.

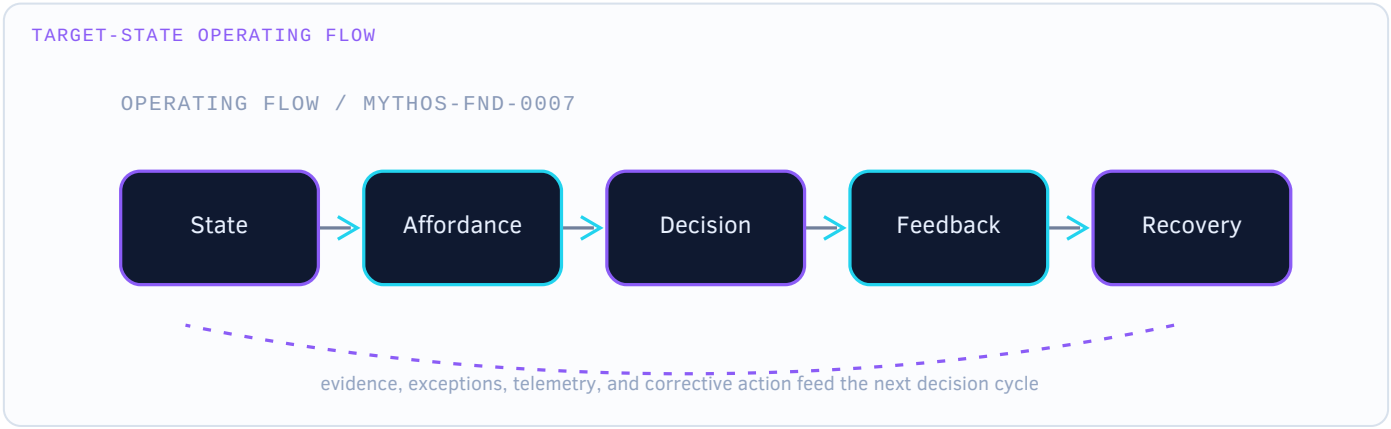
3.3 Security, Privacy, and Trust Impact

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	Interface ownership and critical-flow inventory
2	Authoritative state model
3	Identity, scope, and environment context
4	Critical-action safety
5	Undo, cancellation, and recovery
6	Accessibility baseline
7	Validation and constraints
8	Feedback and progress
9	Safe error communication
10	Privacy and sensitive-data handling
11	Consistent interaction semantics
12	Performance and responsiveness
13	Degraded and offline behavior
14	AI output and action boundaries

#	Target-State Component
15	Locale, language, time, and units
16	Interaction auditability
17	Representative validation

```
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
Product owner	Owns user outcomes and critical workflow inventory.
Design authority	Owns interaction principles, consistency, and design system.
Accessibility lead	Defines accessibility requirements and representative evaluation.
Security and privacy lead	Reviews critical actions, sensitive data, identity, and disclosure.
Frontend engineering	Implements state, performance, keyboard, assistive technology, and error behavior.
Operations representative	Validates operational and degraded workflows.
User research lead	Validates with representative users and contexts.
Independent assessor	Tests accessibility, safety, and evidence.

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

- Make interfaces understandable, accessible, predictable, and safe.
- Prevent visual design from obscuring authority, risk, system state, or irreversible consequences.
- Establish assessable requirements for administrative, operational, consumer, and AI-mediated interfaces.
- Ensure interaction design remains effective under failure, latency, degraded connectivity, and assistive technology.

7. Scope

Applies to graphical, command-line, conversational, voice, immersive, embedded, mobile, desktop, web, and machine-assisted human interfaces. It includes setup, operations, administration, approval, recovery, support, and decommissioning workflows.

8. Intended Audience

- Product and interface designers
- Frontend and platform engineers
- Accessibility and quality specialists
- Security and privacy teams
- 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

- **W3C WCAG 2.2** — Web Content Accessibility Guidelines 2.2. https://www.w3.org/TR/WCAG22/
- **W3C WAI-ARIA 1.2** — Accessible Rich Internet Applications 1.2. https://www.w3.org/TR/wai-aria-1.2/
- **ISO/IEC 25010:2023** — Systems and software Quality Requirements and Evaluation — Product quality model. https://www.iso.org/standard/78176.html
- **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
- **NIST Privacy Framework 1.0** — A Tool for Improving Privacy through Enterprise Risk Management. https://www.nist.gov/privacy-framework/privacy-framework

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.
Critical action	An action that can cause material loss, exposure, outage, irreversible change, legal effect, or significant user harm.
System state	The authoritative condition of a system, operation, resource, or workflow at a point in time.
Progressive disclosure	Presentation of essential information first, with additional complexity available when needed.
Interaction evidence	Records demonstrating that a user was shown relevant information, possessed required authority, and completed or declined an action.

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.

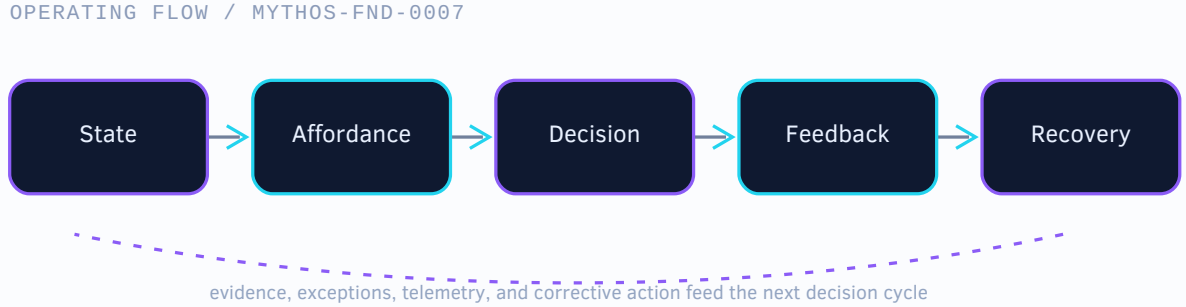
Adopting organizations SHOULD maintain a domain-specific risk register that identifies cause, affected asset or stakeholder, credible scenario, impact, existing controls, residual risk, owner, review trigger, and evidence. Risks that cross standards MUST be linked rather than copied into disconnected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

15. Governing Principles

- Clarity outranks ornament when consequences are material.
- State, authority, scope, and consequence must be visible before commitment.
- Accessibility is a design constraint, not a post-release accommodation.
- Errors should be prevented where practical and recoverable where prevention is impossible.
- The interface must not claim success before authoritative completion.
- High-consequence automation requires meaningful human control or explicitly approved autonomous authority.

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
Product owner	Owns user outcomes and critical workflow inventory.
Design authority	Owns interaction principles, consistency, and design system.
Accessibility lead	Defines accessibility requirements and representative evaluation.
Security and privacy lead	Reviews critical actions, sensitive data, identity, and disclosure.
Frontend engineering	Implements state, performance, keyboard, assistive technology, and error behavior.
Operations representative	Validates operational and degraded workflows.
User research lead	Validates with representative users and contexts.
Independent assessor	Tests accessibility, safety, and evidence.

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
Generic approve or delete buttons without scope	Failure can create hidden risk, misleading assurance, uncontrolled cost, or unsafe operation.
Using color as the only status signal	Failure can create hidden risk, misleading assurance, uncontrolled cost, or unsafe operation.
Hiding errors behind friendly but non-actionable language	Failure can create hidden risk, misleading assurance, uncontrolled cost, or unsafe operation.
Automatic destructive actions from AI suggestions	Failure can create hidden risk, misleading assurance, uncontrolled cost, or unsafe operation.
Modal confirmations that repeat no new information	Failure can create hidden risk, misleading assurance, uncontrolled cost, or unsafe operation.
Inaccessible custom controls	Failure can create hidden risk, misleading assurance, uncontrolled cost, or unsafe operation.
Infinite loading states without timeout or recovery	Failure can create hidden risk, misleading assurance, uncontrolled cost, or unsafe operation.

21. Cross-Functional Dependencies

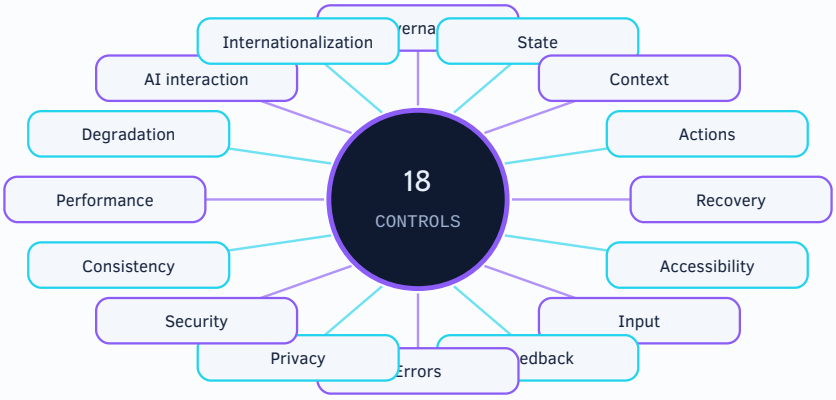
This Foundation standard depends on the remaining MYTHOS-FND standards for documentation, security and trust, quality, operations, data and integration, interfaces, extensions, AI-first behavior, and agentic orchestration. An adopting organization MUST resolve overlapping requirements through the stricter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

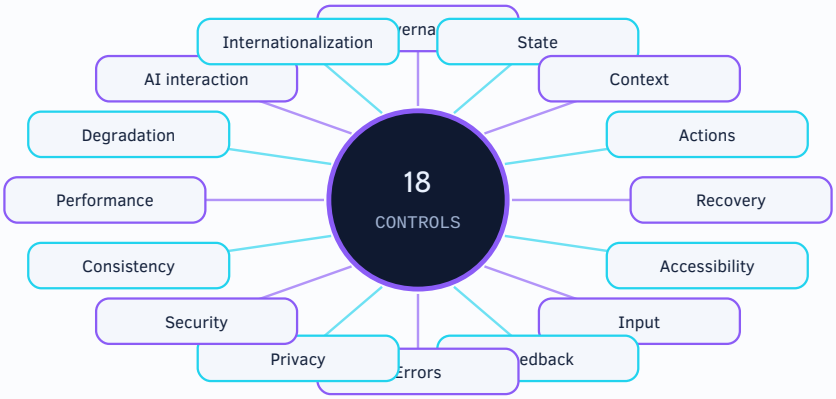
- Governance
- State
- Context
- Actions
- Recovery
- Accessibility
- Input
- Feedback
- Errors
- Privacy
- Security
- Consistency
- Performance
- Degradation
- AI interaction
- Internationalization
- Evidence
- Testing

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-UI-01 – Interface ownership and critical-flow inventory

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

Requirement

The organization MUST assign accountable owners for each material interface and maintain an inventory of critical user journeys, supported modalities, user populations, risk classifications, and authoritative backend dependencies.

Purpose

Creates ownership and ensures high-risk interactions receive proportionate review.

Applicability

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

Implementation guidance

- Classify administrative and irreversible actions.
- Record supported assistive technologies and locales.

Required evidence

- Interface inventory
- Critical-flow register
- Ownership records

Assessment procedure

- **Examine:** Sample interfaces against the inventory.
- **Interview:** Interview owners.
- **Test:** Identify an unregistered critical flow.

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 25010:2023

NORMATIVE CONTROL

MYTHOS-FND-UI-02 – Authoritative and unambiguous system state

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

Requirement

Interfaces MUST present current, pending, failed, degraded, stale, and completed states distinctly and MUST NOT represent an operation as successful before authoritative confirmation.

Purpose

Prevents false confidence and unsafe follow-on action.

Applicability

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

Implementation guidance

- Use correlation identifiers for long-running actions.
- Show data freshness and source where material.

Required evidence

- State model
- UI tests
- Telemetry

Assessment procedure

- **Examine:** Inject delayed and failed operations.
- **Interview:** Verify stale data indicators.
- **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 and SI families

NORMATIVE CONTROL

MYTHOS-FND-UI-03 – Scope, identity, and environment visibility

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

Requirement

Before a material action, the interface MUST display the acting identity, target scope, tenant or trust domain, environment, affected resources, and effective privilege when confusion could cause harm.

Purpose

Reduces wrong-target, wrong-environment, and confused-deputy errors.

Applicability

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

Implementation guidance

- Use persistent production indicators.
- Show inherited or delegated authority.

Required evidence

- Context design
- Critical-action screenshots
- Tests

Assessment procedure

- **Examine:** Switch tenants or environments.
- **Interview:** Verify context remains visible through confirmation.
- **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-UI-04 – Safe critical-action design

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

Requirement

Critical actions MUST require explicit intent, validate preconditions and authority, disclose material consequences, and provide preview, confirmation, approval, delay, rollback, or equivalent safeguards proportionate to risk.

Purpose

Prevents accidental or unauthorized high-impact change.

Applicability

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

Implementation guidance

- Avoid generic confirmation text.
- Require typed or scoped confirmation only where it adds meaningful friction.

Required evidence

- Action classification
- Safeguard rules
- Test evidence

Assessment procedure

- **Examine:** Attempt action with failed preconditions.
- **Interview:** Verify confirmation reflects exact 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 — CM-3

NORMATIVE CONTROL

MYTHOS-FND-UI-05 – Undo, cancellation, and recovery

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

Requirement

Interfaces MUST expose cancellation, retry, rollback, compensation, support, or recovery paths for recoverable failures and MUST clearly identify irreversible operations before commitment.

Purpose

Limits impact when mistakes or failures occur.

Applicability

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

Implementation guidance

- Preserve user input where safe.
- Explain partial success.

Required evidence

- Recovery design
- Failure tests
- Support procedures

Assessment procedure

- **Examine:** Interrupt representative workflows.
- **Interview:** Verify partial effects are reconciled.
- **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 25010:2023 — reliability

NORMATIVE CONTROL

MYTHOS-FND-UI-06 – Accessibility baseline

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

Requirement

Interfaces MUST satisfy applicable WCAG 2.2 Level AA requirements and MUST support keyboard operation, semantic structure, focus visibility, readable contrast, non-color cues, scalable text, and assistive-technology interpretation for critical workflows.

Purpose

Ensures equitable and reliable access.

Applicability

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

Implementation guidance

- Document exceptions by platform limitation.
- Test with representative assistive technologies.

Required evidence

- Accessibility report
- Automated scans
- Manual test records

Assessment procedure

- **Examine:** Perform keyboard-only and screen-reader tests.
- **Interview:** Check zoom and contrast.
- **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

- WCAG 2.2
- WAI-ARIA 1.2

NORMATIVE CONTROL

MYTHOS-FND-UI-07 – Input validation and constraint communication

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

Requirement

Interfaces MUST validate inputs as early as practical, preserve authoritative server-side validation, explain constraints, reject ambiguous values, and prevent unsafe defaults.

Purpose

Reduces malformed, unintended, and insecure requests.

Applicability

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

Implementation guidance

- Use units and formats explicitly.
- Do not rely on placeholders as labels.

Required evidence

- Validation rules
- Negative tests
- Error catalog

Assessment procedure

- **Examine:** Submit boundary, malformed, and conflicting inputs.
- **Interview:** Bypass client validation.
- **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

- OWASP ASVS

NORMATIVE CONTROL

MYTHOS-FND-UI-08 – Timely and actionable feedback

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

Requirement

Interfaces MUST provide feedback for accepted input, processing, completion, failure, conflict, timeout, throttling, and recovery, with actionable next steps and correlation where support may be required.

Purpose

Maintains user control and enables diagnosis.

Applicability

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

Implementation guidance

- Avoid indefinite spinners.
- Distinguish retryable from permanent failures.

Required evidence

- Feedback catalog
- Latency tests
- Support records

Assessment procedure

- **Examine:** Simulate each major outcome.
- **Interview:** Measure announcement to assistive technology.
- **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 25010:2023

NORMATIVE CONTROL

MYTHOS-FND-UI-09 – Non-sensitive error communication

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

Requirement

User-facing errors MUST be specific enough to support safe correction while excluding secrets, internal topology, sensitive identifiers, stack traces, or exploitable implementation detail.

Purpose

Balances usability with confidentiality and security.

Applicability

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

Implementation guidance

- Log protected diagnostic detail with correlation.
- Localize without changing machine codes.

Required evidence

- Error catalog
- Redaction rules
- Tests

Assessment procedure

- **Examine:** Trigger internal failures.
- **Interview:** Inspect output and logs.
- **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

- OWASP ASVS
- NIST SP 800-53 — SI-11

NORMATIVE CONTROL

MYTHOS-FND-UI-10 – Privacy-respecting interaction

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

Requirement

Interfaces MUST disclose material data collection and sharing at the point of interaction, minimize requested data, provide appropriate preference and consent controls, and avoid coercive or deceptive choice architecture.

Purpose

Protects autonomy and privacy.

Applicability

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

Implementation guidance

- Separate necessary processing from optional personalization.
- Make rejection no harder than acceptance where choice is genuine.

Required evidence

- Data-flow map
- Consent records
- UX review

Assessment procedure

- **Examine:** Trace collected fields to purpose.
- **Interview:** Test withdrawal or preference change.
- **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-UI-11 – Session and sensitive-data handling

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

Requirement

Interfaces MUST protect authentication state, secrets, sensitive values, clipboard use, cached data, screenshots, exports, and inactivity behavior according to risk and platform capability.

Purpose

Reduces exposure through the interaction layer.

Applicability

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

Implementation guidance

- Mask by default without making verification impossible.
- Clear sensitive transient state.

Required evidence

- Session policy
- Storage review
- Security tests

Assessment procedure

- **Examine:** Inspect local storage and caches.
- **Interview:** Test session expiry and reauthentication.
- **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-UI-12 – Consistent interaction semantics

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

Requirement

Equivalent controls, terms, states, shortcuts, and navigation patterns SHOULD behave consistently across the product unless a documented safety or platform constraint requires variation.

Purpose

Reduces cognitive load and operational error.

Applicability

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

Implementation guidance

- Maintain a governed component and terminology system.
- Version breaking interaction changes.

Required evidence

- Design system
- Terminology register
- Regression tests

Assessment procedure

- **Examine:** Compare equivalent workflows.
- **Interview:** Review justified deviations.
- **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 25010:2023 — usability

NORMATIVE CONTROL

MYTHOS-FND-UI-13 – Perceived and actual responsiveness

FAMILY	PROFILES	FAILURE IMPACT	AUTOMATION POTENTIAL
Performance	Advanced, High Assurance	Material	High

Requirement

Critical workflows MUST define response, feedback, rendering, and completion objectives and MUST remain operable under expected latency, scale, and constrained-device conditions.

Purpose

Prevents latency from producing duplicate actions or abandonment.

Applicability

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

Implementation guidance

- Acknowledge input quickly while preserving true completion state.
- Budget client and server latency.

Required evidence

- Performance objectives
- Real-user telemetry
- Load tests

Assessment procedure

- **Examine:** Throttle network and CPU.
- **Interview:** Measure duplicate submissions.
- **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 25010:2023 — performance efficiency

NORMATIVE CONTROL

MYTHOS-FND-UI-14 – Degraded and offline behavior

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

Requirement

Interfaces MUST define behavior for unavailable dependencies, stale data, lost connectivity, partial permissions, and incompatible versions and MUST fail safely without concealing reduced capability.

Purpose

Maintains trust and safety under non-ideal conditions.

Applicability

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

Implementation guidance

- Disable actions that cannot be safely completed.
- Queue only when semantics and user expectations are explicit.

Required evidence

- Degradation design
- Failure tests
- User messaging

Assessment procedure

- **Examine:** Disconnect dependencies mid-workflow.
- **Interview:** Verify no false success.
- **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 25010:2023 — reliability

NORMATIVE CONTROL

MYTHOS-FND-UI-15 – AI-generated output and action boundaries

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

Requirement

Interfaces presenting AI-generated content or recommendations MUST identify material uncertainty, distinguish generated from authoritative information, expose relevant sources or evidence where available, and clearly separate recommendation from execution authority.

Purpose

Prevents automation bias and accidental delegation.

Applicability

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

Implementation guidance

- Show model or policy limitations in context.
- Require review for consequential actions unless autonomy is approved.

Required evidence

- AI interaction specification
- Evaluation results
- Action logs

Assessment procedure

- **Examine:** Present conflicting evidence.
- **Interview:** Attempt to execute from unverified output.
- **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 AI RMF 1.0
- NIST AI 600-1

NORMATIVE CONTROL

MYTHOS-FND-UI-16 – Locale, language, time, and unit correctness

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

Requirement

Interfaces used across locales MUST represent language, names, addresses, numbers, currencies, units, time zones, dates, sorting, and text direction without ambiguous or lossy assumptions.

Purpose

Prevents operational and financial errors across regions.

Applicability

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

Implementation guidance

- Store canonical values separately from display forms.
- Display time zone for material timestamps.

Required evidence

- Locale matrix
- Translation records
- Tests

Assessment procedure

- **Examine:** Test boundary dates, RTL text, and unit changes.
- **Interview:** Verify round trips.
- **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

- WCAG 2.2

NORMATIVE CONTROL

MYTHOS-FND-UI-17 – Interaction auditability

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

Requirement

Material approvals, administrative actions, policy changes, and irreversible operations MUST produce tamper-resistant records of actor, authority, target, request, presented context, decision, outcome, time, and correlation.

Purpose

Supports accountability, incident response, and dispute resolution.

Applicability

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

Implementation guidance

- Avoid logging sensitive content unnecessarily.
- Link UI evidence to backend execution evidence.

Required evidence

- Audit records
- Integrity controls
- Reconstruction tests

Assessment procedure

- **Examine:** Reconstruct a sampled action end to end.
- **Interview:** Attempt log alteration.
- **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-UI-18 – Representative interface validation

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

Requirement

Critical interfaces MUST be tested with representative users, assistive technologies, devices, browsers or runtimes, permissions, data conditions, failures, and adversarial misuse before release and after material change.

Purpose

Finds failures not visible in ideal-path automation.

Applicability

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

Implementation guidance

- Combine automated, expert, and user testing.
- Prioritize consequential and high-frequency flows.

Required evidence

- Test plan
- Participant and environment matrix
- Findings

Assessment procedure

- **Examine:** Review coverage against the inventory.
- **Interview:** Reproduce a closed high-severity finding.
- **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

- WCAG 2.2
- ISO/IEC 25010:2023

FOUNDATION STANDARD / STRUCTURAL PART

Part V – Implementation and Operations

24. Implementation Profiles

Profile	Required Operating State
Baseline	Authoritative state, safe actions, accessible interaction, validation, feedback, privacy, recovery, responsive behavior, AI labeling, and representative testing.
Enterprise	Shared design system, automated accessibility and visual regression, critical-flow analytics, cross-product semantics, offline/degraded patterns, and auditable user action records.
High Assurance	Independent usability and accessibility validation, high-risk action simulation, formally reviewed state machines, multi-channel confirmation, assistive redundancy, and evidence-backed human-factors assurance.

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

- Generic approve or delete buttons without scope
- Using color as the only status signal
- Hiding errors behind friendly but non-actionable language
- Automatic destructive actions from AI suggestions
- Modal confirmations that repeat no new information
- Inaccessible custom controls
- Infinite loading states without timeout or recovery

30. Adoption Roadmap from Source Draft

- Inventory interfaces and classify critical workflows.
- Establish an interaction-state model, design tokens, accessibility baseline, and critical-action pattern library.
- Instrument outcome, error, latency, abandonment, and recovery telemetry.
- Add independent accessibility and adversarial usability testing for Advanced adoption.
- Continuously validate critical workflows across supported devices, locales, input modes, and degraded conditions.

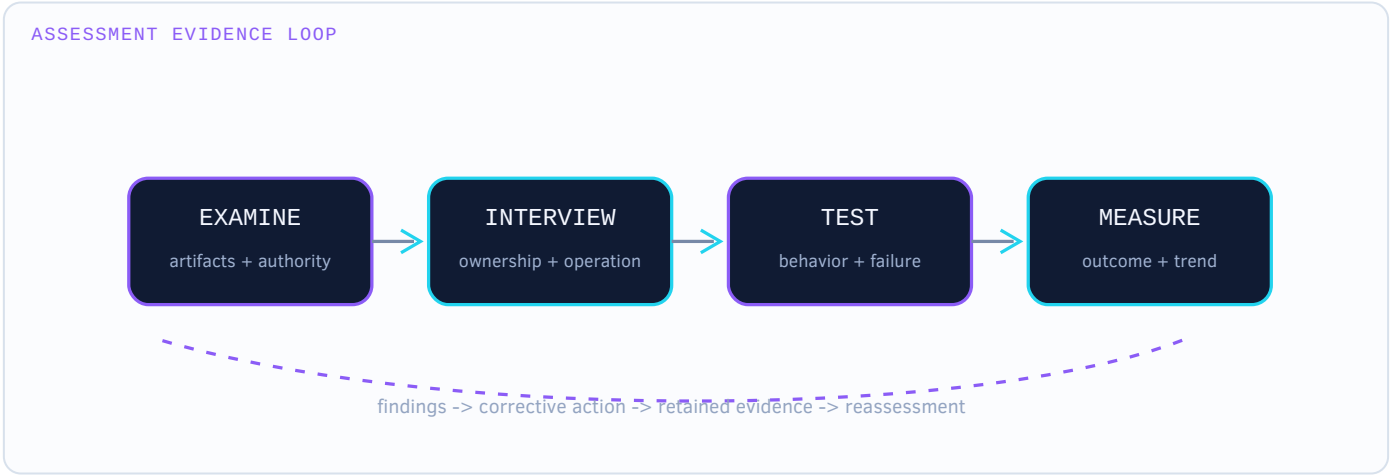
31. Limitations and Residual Risk from Source Draft

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
Critical-flow completion	Successful completion of representative critical workflows without assistance	Target defined per user population and risk
	Applicable WCAG 2.2 success criteria satisfied	AA baseline; stronger criteria by profile

Metric	Definition	Expected use or target
Accessibility conformance		
False-success rate	Operations shown as complete before authoritative success	0 for critical actions
Recovery success	Users able to recover from injected errors	Measured for all critical workflows
Unsafe-action prevention	Material actions blocked or challenged when preconditions fail	100% of defined preconditions

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.

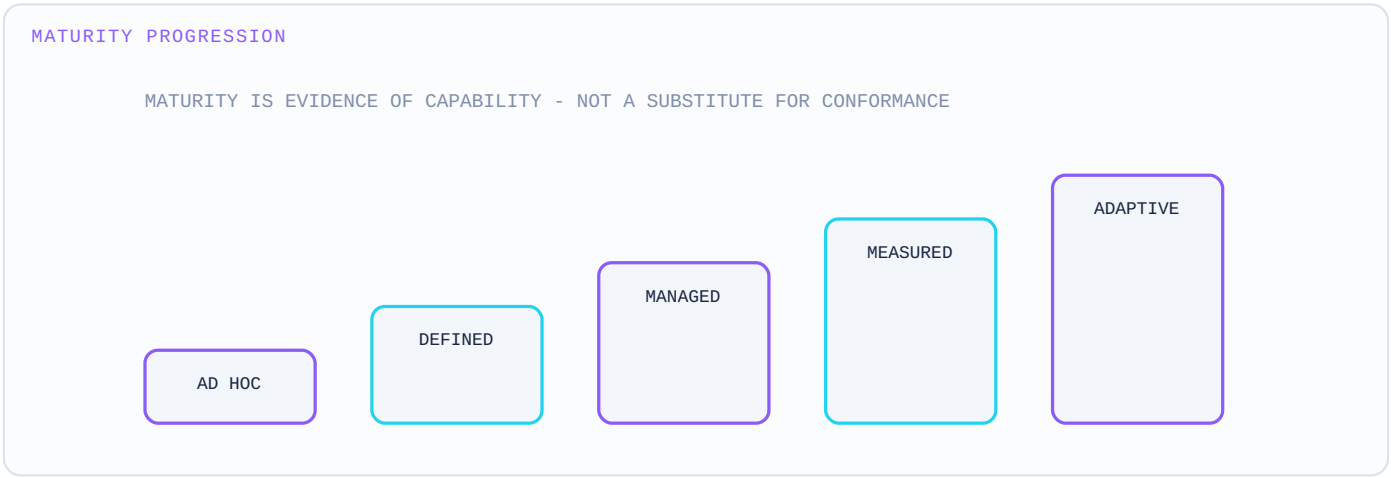
34. Exceptions and Compensating Controls

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
critical flows with current owner	Defined by the adopting organization with owner, source, target, and cadence.
WCAG 2.2 AA success criteria failures	Defined by the adopting organization with owner, source, target, and cadence.
critical actions with explicit scope and effect	Defined by the adopting organization with owner, source, target, and cadence.
user errors leading to rollback or incident	Defined by the adopting organization with owner, source, target, and cadence.
cancel and recovery success rate	Defined by the adopting organization with owner, source, target, and cadence.
unresolved accessibility defects	Defined by the adopting organization with owner, source, target, and cadence.
AI outputs without provenance or status label	Defined by the adopting organization with owner, source, target, and cadence.
p95 interaction and feedback latency	Defined by the adopting organization with owner, source, target, and cadence.
degraded-mode exercises passed	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
WCAG 2.2	Web Content Accessibility Guidelines	https://www.w3.org/WAI/standards-guidelines/wcag/	W3C Recommendation	2026-09-17
WCAG-EM	Website Accessibility Conformance Evaluation Methodology	https://www.w3.org/WAI/test-evaluate/conformance/wcag-em/	W3C methodology	2026-09-17
WAI-ARIA 1.2	Accessible Rich Internet Applications	https://www.w3.org/TR/wai-aria-1.2/	W3C Recommendation	2026-09-17
ISO 9241-210:2019	Human-centred design for interactive systems	https://www.iso.org/standard/77520.html	Published	2026-09-17
EN 301 549 V3.2.1	Accessibility requirements for ICT products and services	https://www.etsi.org/deliver/etsi_en/301500_301599/301549/03.02.01_60/en_301549v030201p.pdf	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

- Retains the source draft's broad interface coverage while removing aesthetic prescriptions from normative requirements.
- Converts design advice into testable controls centered on state, authority, consequence, accessibility, and recovery.
- Treats conversational and AI interfaces as interface modalities subject to the same trust requirements.

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-UI-01	Governance	Interface ownership and critical-flow inventory	Foundational, Advanced, High Assurance	High	Critical
MYTHOS-FND-UI-02	State	Authoritative and unambiguous system state	Foundational, Advanced, High Assurance	High	Critical
MYTHOS-FND-UI-03	Context	Scope, identity, and environment visibility	Foundational, Advanced, High Assurance	High	Critical
MYTHOS-FND-UI-04	Actions	Safe critical-action design	Foundational, Advanced, High Assurance	High	Critical
MYTHOS-FND-UI-05	Recovery	Undo, cancellation, and recovery	Foundational, Advanced, High Assurance	Partial	Critical
MYTHOS-FND-UI-06	Accessibility	Accessibility baseline	Foundational, Advanced, High Assurance	Partial	Critical
MYTHOS-FND-UI-07	Input	Input validation and constraint communication	Foundational, Advanced, High Assurance	High	Material
MYTHOS-FND-UI-08	Feedback	Timely and actionable feedback	Foundational, Advanced, High Assurance	Partial	Material
MYTHOS-FND-UI-09	Errors	Non-sensitive error communication	Foundational, Advanced, High Assurance	High	Critical
MYTHOS-FND-UI-10	Privacy	Privacy-respecting interaction	Foundational, Advanced, High Assurance	Partial	Critical
	Security	Session and sensitive-data handling		High	Critical

Control	Family	Title	Profiles	Automation	Impact
MYTHOS-FND-UI-11			Foundational, Advanced, High Assurance		
MYTHOS-FND-UI-12	Consistency	Consistent interaction semantics	Foundational, Advanced, High Assurance	Partial	Material
MYTHOS-FND-UI-13	Performance	Perceived and actual responsiveness	Advanced, High Assurance	High	Material
MYTHOS-FND-UI-14	Degradation	Degraded and offline behavior	Advanced, High Assurance	Partial	Critical
MYTHOS-FND-UI-15	AI interaction	AI-generated output and action boundaries	Foundational, Advanced, High Assurance	Partial	Critical
MYTHOS-FND-UI-16	Internationalization	Locale, language, time, and unit correctness	Advanced, High Assurance	Partial	Material
MYTHOS-FND-UI-17	Evidence	Interaction auditability	Advanced, High Assurance	High	Critical
MYTHOS-FND-UI-18	Testing	Representative interface validation	Foundational, Advanced, High Assurance	Partial	Critical

Appendix D – Minimum Conformance Claim Record

```
standard: MYTHOS-FND-0007
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

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

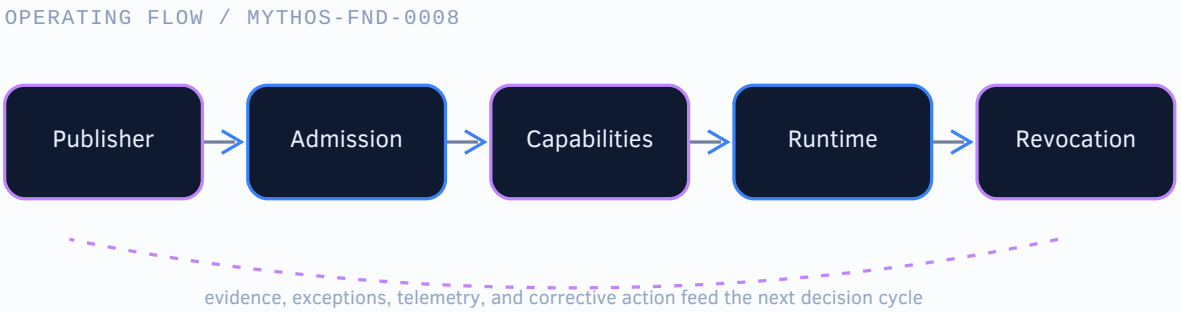
- Enable useful extensibility through explicit, least-privilege contracts.
- Constrain supply-chain, tenant-isolation, data-exfiltration, and persistence risks.
- Make extension behavior, provenance, authority, and lifecycle assessable.
- Support open ecosystems without requiring blind trust in publishers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

Document Control 8

Revision Record 8

How to Use This Standard 9

Executive Reading Path 9

Engineering Reading Path 9

Assessment Reading Path 9

Normative and Informative Content 9

Part I – Executive Direction 10

1. Executive Overview 10

2. Executive Findings and Required Direction 10

3. Business and Operational Impact 10

4. Target-State Summary 11

5. Leadership Responsibilities 12

Part II – Standard Foundation 13

6. Purpose and Objectives 13

7. Scope 13

8. Intended Audience 13

9. Requirements Language and Conformance 13

10. Normative References from Source Draft 13

11. Informative References from Source Draft 14

12. Terms and Definitions 14

13. Applicability and Tailoring 15

Part III – Risk and Architecture 16

14. Enterprise Problem and Risk Landscape 16

15. Governing Principles 16

16. Reference Operating Architecture 16
17. Roles and Accountability 17
18. State, Evidence, and Decision Model 18
19. Security and Trust Considerations 18
20. Failure Modes 18
21. Cross-Functional Dependencies 18

Part IV – Normative Control System 19

22. Control-Family Overview 19
23. Normative Controls 20

Part V – Implementation and Operations 39

24. Implementation Profiles 39
25. Implementation Lifecycle 39
26. Integration Requirements 40
27. Failure Handling and Recovery 40
28. Exceptions and Compensating Controls 40
29. Prohibited Practices 40
30. Adoption Roadmap from Source Draft 41
31. Limitations and Residual Risk from Source Draft 41

Part VI – Assurance and Assessment 42

32. Assessment Methodology 42
33. Metrics and Reporting from Source Draft 42
34. Exceptions and Compensating Controls 43
35. Enterprise Metric Set 43
36. Maturity Model 44
37. Assessment Confidence 44
38. Executive Assurance Dashboard 44

Part VII – Authority and Traceability 46

39. Cross-Standard Dependencies from Source Draft 46
40. Current External Authority Register 46

41. Control Traceability 46

42. Source-Draft Preservation 47

Part VIII – Appendices **48**

Appendix A — Source-Draft Evolution Notes 48

Appendix B — Change History 48

Appendix C — Control Summary 48

Appendix D — Minimum Conformance Claim Record 49

Appendix E — Publication Review Checklist 49

NORMATIVE SYSTEM

Control index

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

MYTHOS-FND-EXT-01	Extension classification and ownership	21
MYTHOS-FND-EXT-02	Versioned extension contract	22
MYTHOS-FND-EXT-03	Verified publisher and artifact identity	23
MYTHOS-FND-EXT-04	Build and dependency provenance	24
MYTHOS-FND-EXT-05	Risk-based admission and review	25
MYTHOS-FND-EXT-06	Explicit least-privilege grants	26
MYTHOS-FND-EXT-07	Runtime isolation and resource control	27
MYTHOS-FND-EXT-08	Brokered secret access	28
MYTHOS-FND-EXT-09	Egress and external-service governance	29
MYTHOS-FND-EXT-10	Extension data-use boundaries	30
MYTHOS-FND-EXT-11	Secure update and rollback	31
MYTHOS-FND-EXT-12	Runtime accountability	32
MYTHOS-FND-EXT-13	Conformance and adversarial testing	33
MYTHOS-FND-EXT-14	Transparent listing and ranking	34
MYTHOS-FND-EXT-15	Emergency disablement and revocation	35
MYTHOS-FND-EXT-16	Disablement, uninstall, and orphan handling	36
MYTHOS-FND-EXT-17	Ecosystem incident coordination	37
MYTHOS-FND-EXT-18	Interoperability and exit	38

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.

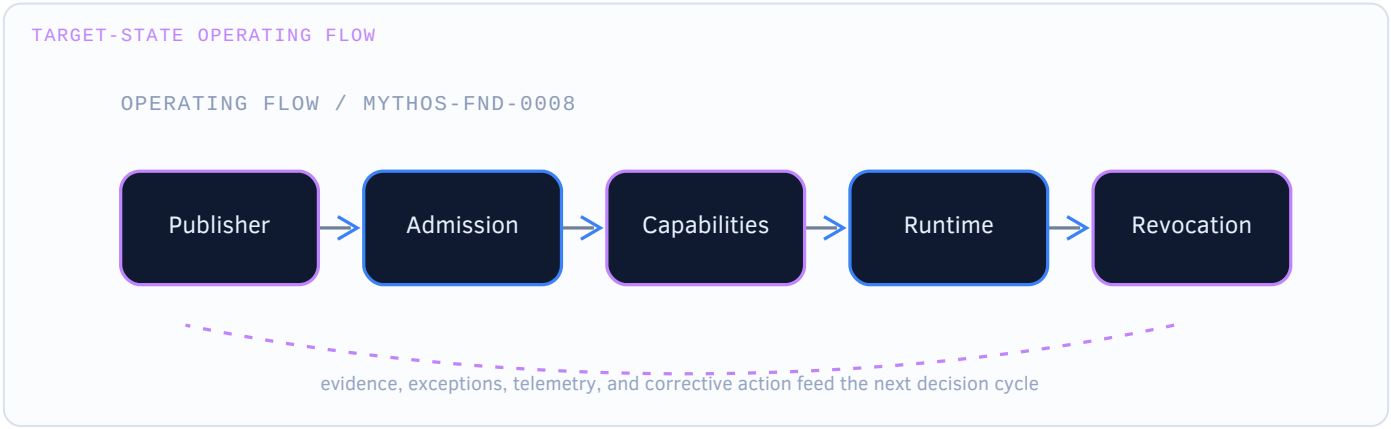
3.3 Security, Privacy, and Trust Impact

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.

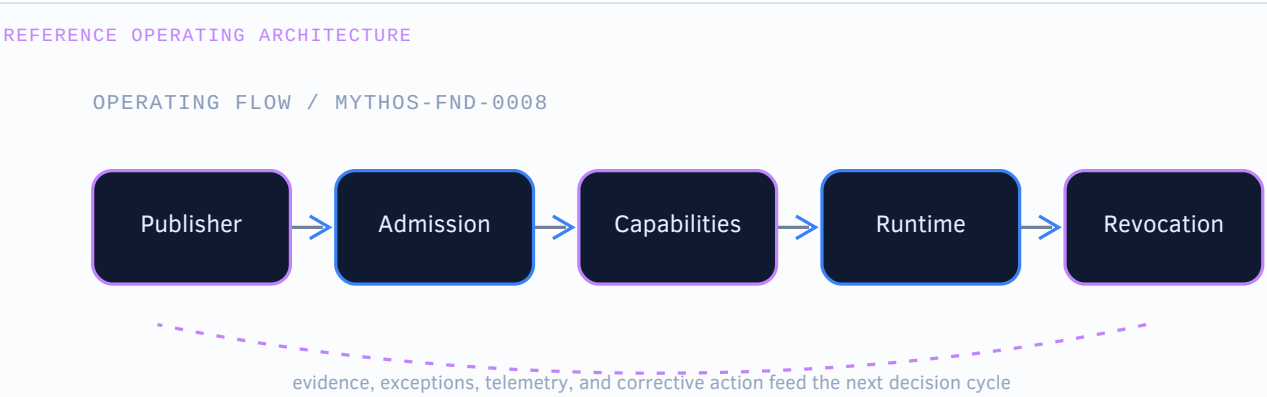
Adopting organizations SHOULD maintain a domain-specific risk register that identifies cause, affected asset or stakeholder, credible scenario, impact, existing controls, residual risk, owner, review trigger, and evidence. Risks that cross standards MUST be linked rather than copied into disconnected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

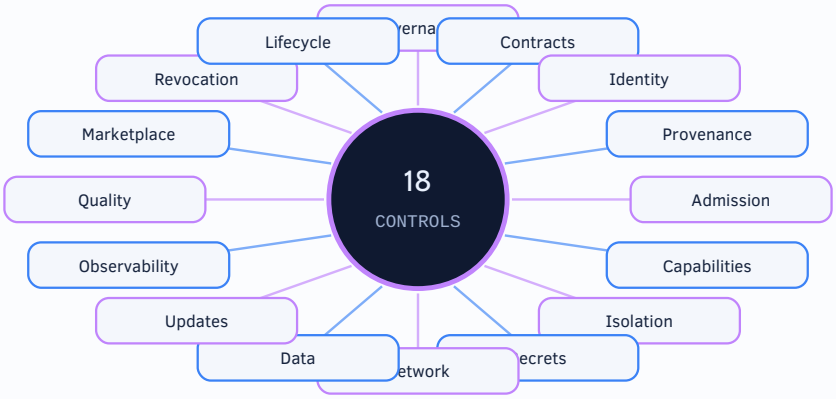
This Foundation standard depends on the remaining MYTHOS-FND standards for documentation, security and trust, quality, operations, data and integration, interfaces, extensions, AI-first behavior, and agentic orchestration. An adopting organization MUST resolve overlapping requirements through the stricter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

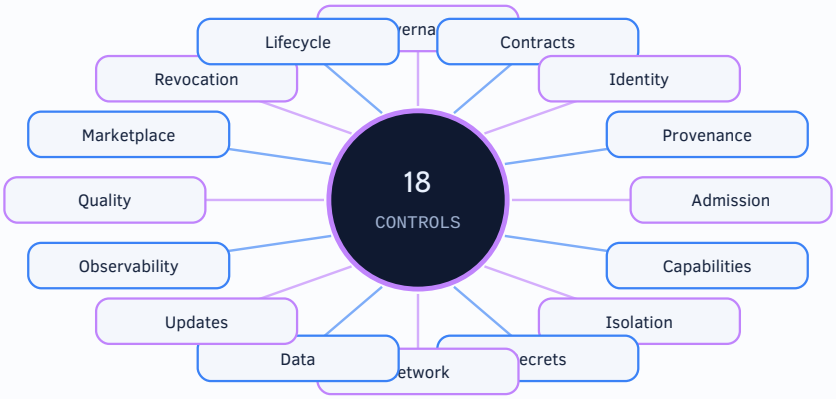
- Governance
- Contracts
- Identity
- Provenance
- Admission
- Capabilities
- Isolation
- Secrets
- Network
- Data
- Updates
- Observability
- Quality
- Marketplace
- Revocation
- Lifecycle
- Incident response
- Portability

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.

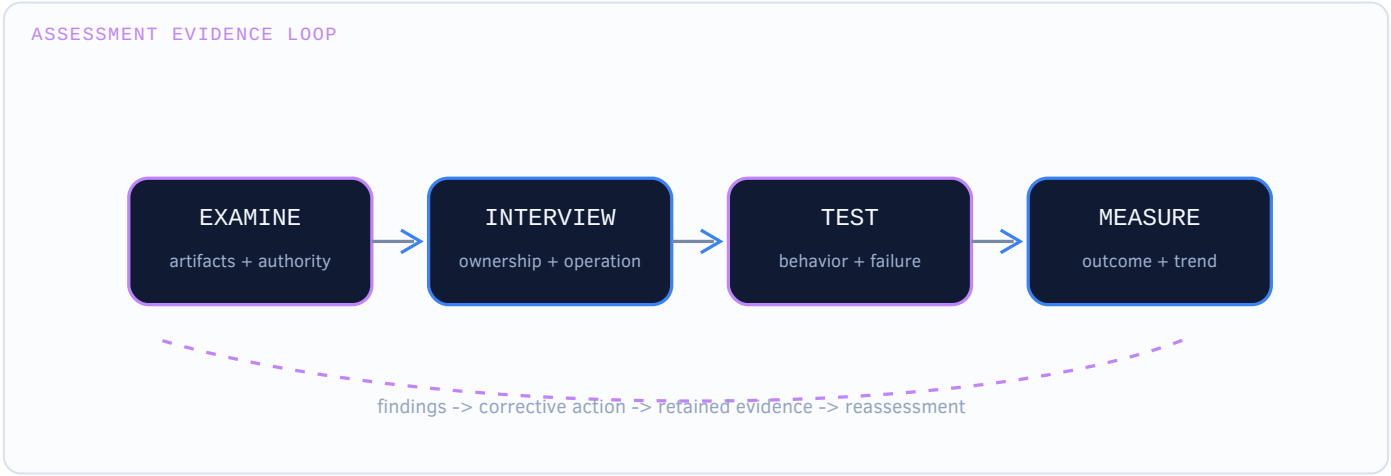
31. Limitations and Residual Risk from Source Draft

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.

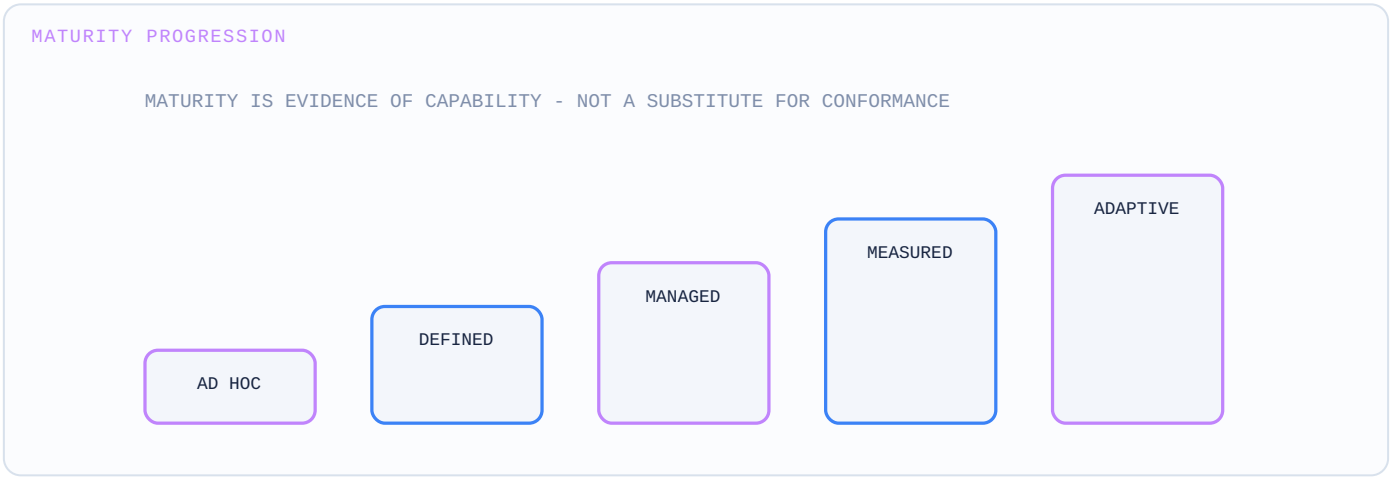
34. Exceptions and Compensating Controls

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

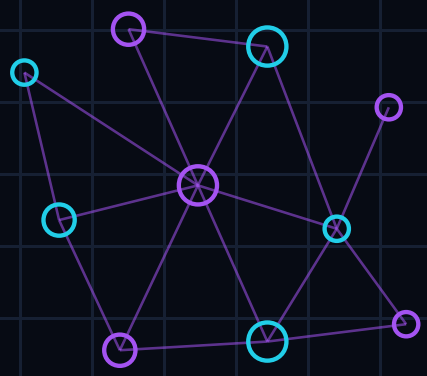
Appendix D – Minimum Conformance Claim Record

```
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



CANDIDATE STANDARD

Mythos AI-First Application Standard

Govern material AI behavior through justified use, impact analysis, evaluation, grounding, human control, and lifecycle evidence.

PERMANENT ID
MYTHOS-FND-0009

PUBLICATION CLASS
CANDIDATE STANDARD

VERSION / STATUS
1.0.0-candidate / CANDIDATE

PERMANENT PUBLICATION IDENTITY

Mythos AI-First Application Standard

Universal Requirements for Responsible, Secure, Evaluated, and Operable AI-Enabled Applications

Document ID
MYTHOS-FND-0009

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	19	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	AI product and engineering teams; Security, privacy, legal, risk, and safety teams; Data and model owners; Operators and incident responders; Assessors and procurement teams
Publisher / owner	Mythos Systems / Standards Program
Public classification	Public technical standard
Canonical route	/library/standards/foundation/mythos-fnd-0009/

Expected outcomes

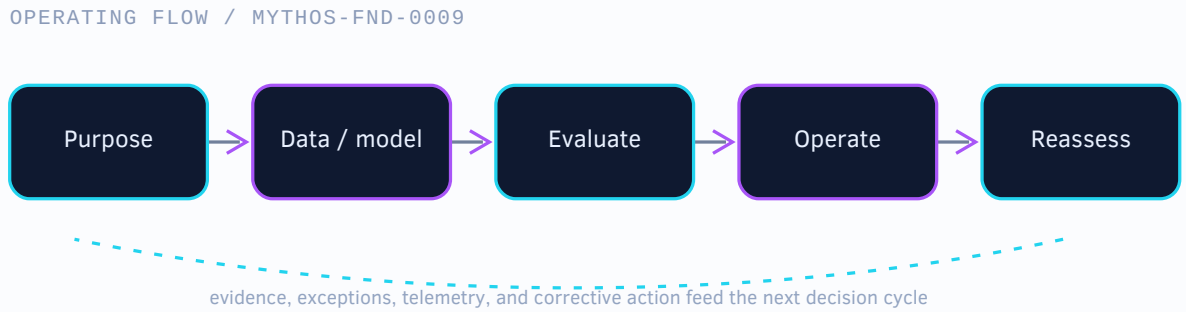
- Use AI only where it provides defensible value relative to simpler alternatives.
- Make model uncertainty, limitations, and authority boundaries explicit.
- Require evaluation against representative tasks, harms, abuse, and operational conditions.
- Preserve accountability and safe fallback across model, provider, and data changes.

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.

Document Control 8

Revision Record 8

How to Use This Standard 9

Executive Reading Path 9

Engineering Reading Path 9

Assessment Reading Path 9

Normative and Informative Content 9

Part I – Executive Direction 10

1. Executive Overview 10

2. Executive Findings and Required Direction 10

3. Business and Operational Impact 10

4. Target-State Summary 11

5. Leadership Responsibilities 12

Part II – Standard Foundation 13

6. Purpose and Objectives 13

7. Scope 13

8. Intended Audience 13

9. Requirements Language and Conformance 13

10. Normative References from Source Draft 13

11. Informative References from Source Draft 14

12. Terms and Definitions 14

13. Applicability and Tailoring 15

Part III – Risk and Architecture 16

14. Enterprise Problem and Risk Landscape 16

15. Governing Principles 16

16. Reference Operating Architecture 16

17. Roles and Accountability 17

18. State, Evidence, and Decision Model 18

19. Security and Trust Considerations 18

20. Failure Modes 18

21. Cross-Functional Dependencies 18

Part IV – Normative Control System **19**

22. Control-Family Overview 19

23. Normative Controls 20

Part V – Implementation and Operations **40**

24. Implementation Profiles 40

25. Implementation Lifecycle 40

26. Integration Requirements 41

27. Failure Handling and Recovery 41

28. Exceptions and Compensating Controls 41

29. Prohibited Practices 41

30. Adoption Roadmap from Source Draft 42

31. Limitations and Residual Risk from Source Draft 42

Part VI – Assurance and Assessment **43**

32. Assessment Methodology 43

33. Metrics and Reporting from Source Draft 43

34. Exceptions and Compensating Controls 44

35. Enterprise Metric Set 44

36. Maturity Model 45

37. Assessment Confidence 45

38. Executive Assurance Dashboard 45

Part VII – Authority and Traceability **47**

39. Cross-Standard Dependencies from Source Draft 47

40. Current External Authority Register 47

41. Control Traceability 47

42. Source-Draft Preservation 48

Part VIII – Appendices **49**

Appendix A — Source-Draft Evolution Notes 49

Appendix B — Change History 49

Appendix C — Control Summary 49

Appendix D — Minimum Conformance Claim Record 50

Appendix E — Publication Review Checklist 50

NORMATIVE SYSTEM

Control index

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

MYTHOS-FND-AIA-01	AI use-case justification and baseline	21
MYTHOS-FND-AIA-02	AI impact and risk assessment	22
MYTHOS-FND-AIA-03	Accountability and decision rights	23
MYTHOS-FND-AIA-04	Training, retrieval, and inference data governance	24
MYTHOS-FND-AIA-05	Model and provider inventory	25
MYTHOS-FND-AIA-06	Model selection by measured fitness	26
MYTHOS-FND-AIA-07	Representative predeployment evaluation	27
MYTHOS-FND-AIA-08	Grounding and source integrity	28
MYTHOS-FND-AIA-09	Prompt and instruction governance	29
MYTHOS-FND-AIA-10	Action and decision boundaries	30
MYTHOS-FND-AIA-11	Meaningful human oversight and recourse	31
MYTHOS-FND-AIA-12	User disclosure and output provenance	32
MYTHOS-FND-AIA-13	AI threat model and abuse resistance	33
MYTHOS-FND-AIA-14	Privacy-preserving AI operation	34
MYTHOS-FND-AIA-15	Fallback, abstention, and degraded mode	35
MYTHOS-FND-AIA-16	Model, prompt, and provider change control	36
MYTHOS-FND-AIA-17	Production performance and harm monitoring	37
MYTHOS-FND-AIA-18	AI incident response and shutdown	38
MYTHOS-FND-AIA-19	Retirement, replacement, and record retention	39

Document Control

Field	Value
Document ID	MYTHOS-FND-0009
Standard	AI-First Application
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

AI should be introduced because it improves a defined outcome under acceptable risk, not because it is available. AI-first applications require governance beyond conventional software because behavior may be probabilistic, provider-dependent, data-sensitive, difficult to explain, and capable of influencing or performing consequential actions. This standard establishes a full lifecycle for justifying, evaluating, constraining, monitoring, and retiring AI-enabled application behavior.

The institutional objective is to govern when and how AI is used in applications, including impact, data, model selection, evaluation, grounding, prompts, action boundaries, oversight, transparency, privacy, fallback, change, monitoring, incident response, and retirement. 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
AI without baseline justification	Teams use AI where deterministic methods would be safer, cheaper, or more reliable.	Compare against a non-AI baseline and document the reason for AI use.
Opaque model and provider dependency	Organizations cannot reproduce which model produced an outcome or where data went.	Inventory exact model, provider, runtime, configuration, data handling, and route.
Anecdotal evaluation	Demo quality replaces representative and harm-aware evaluation.	Use task-specific datasets, repeated trials, subgroup analysis, and regression gates.
Grounding and instruction failures	Models treat untrusted content as instructions or generate unsupported claims.	Separate instructions from sources, require citations where relevant, and validate outputs.
AI action authority	Generated text or tool calls can become system changes without independent control.	Keep authorization and execution outside the model and provide recourse, fallback, and shutdown.

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.

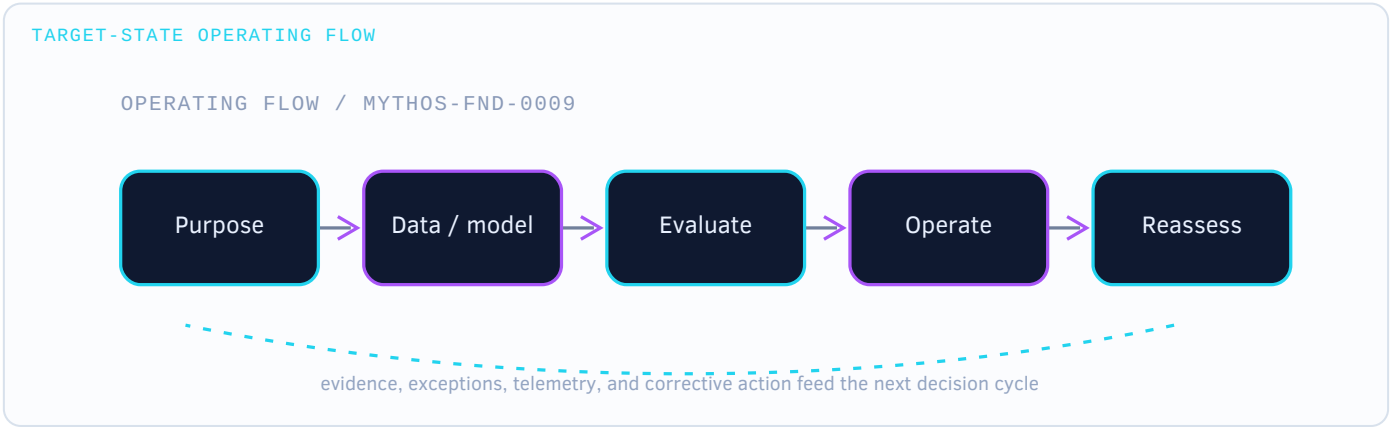
3.3 Security, Privacy, and Trust Impact

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	AI use-case and baseline assessment
2	Impact and risk assessment
3	Accountability and decision rights
4	Training, retrieval, and inference data governance
5	Model and provider inventory
6	Fitness-based model selection
7	Representative evaluation
8	Grounding and source integrity
9	Prompt and instruction governance
10	Action and decision boundaries
11	Human oversight and recourse
12	User disclosure and provenance
13	AI threat model and abuse resistance
14	Privacy-preserving operation

#	Target-State Component
15	Fallback, abstention, and degraded mode
16	Model, prompt, and provider change control
17	Production monitoring
18	AI incident response and shutdown
19	Retirement and records

```
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
AI accountable executive	Owns AI risk appetite and portfolio governance.
Product owner	Owns the user outcome and non-AI baseline.
AI system owner	Owns model, prompt, data, evaluation, provider, and lifecycle.
Model risk or validation lead	Independently evaluates fitness and harm.
Data owner	Approves training, retrieval, inference, and retention use.
Security and privacy lead	Owns threat model, data movement, abuse, and incident controls.
Human-oversight owner	Designs intervention, recourse, appeal, and escalation.
Operations owner	Monitors performance, drift, cost, incidents, and shutdown readiness.

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

- Use AI only where it provides defensible value relative to simpler alternatives.
- Make model uncertainty, limitations, and authority boundaries explicit.
- Require evaluation against representative tasks, harms, abuse, and operational conditions.
- Preserve accountability and safe fallback across model, provider, and data changes.

7. Scope

Applies to applications using predictive, generative, multimodal, retrieval-augmented, fine-tuned, embedded, local, hosted, or third-party AI models. It covers assistive and autonomous behavior but excludes purely deterministic software falsely marketed as AI.

8. Intended Audience

- AI product and engineering teams
- Security, privacy, legal, risk, and safety teams
- Data and model owners
- Operators and incident responders
- Assessors and procurement teams

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 AI 100-1** — Artificial Intelligence Risk Management Framework (AI RMF 1.0). https://doi.org/10.6028/NIST.AI.100-1
- **NIST AI 600-1** — Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile. https://doi.org/10.6028/NIST.AI.600-1
- **NIST SP 800-218A** — Secure Software Development Practices for Generative AI and Dual-Use Foundation Models. https://csrc.nist.gov/pubs/sp/800/218/a/final
- **ISO/IEC 42001:2023** — Artificial intelligence — Management system. https://www.iso.org/standard/81230.html
- **ISO/IEC 23894:2023** — Artificial intelligence — Guidance on risk management. https://www.iso.org/standard/77304.html
- **ISO/IEC 42005:2025** — Artificial intelligence — AI system impact assessment. https://www.iso.org/standard/44545.html
- **OWASP Top 10 for LLM Applications 2025** — Risk taxonomy for applications using large language models. https://genai.owasp.org/llm-top-10/
- **NIST Privacy Framework 1.0** — A Tool for Improving Privacy through Enterprise Risk Management. https://www.nist.gov/privacy-framework/privacy-framework

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.

Term	Definition
AI-first application	An application whose intended value or material behavior depends on one or more AI models rather than treating AI as a superficial add-on.
Model authority	The set of decisions, actions, tools, data, and resources a model or AI workflow is permitted to influence or control.
Evaluation case	A versioned input, context, expected properties, scoring method, and acceptance rule used to evaluate an AI behavior.
Fallback mode	A defined operating state used when a model, provider, retrieval source, or safety control is unavailable or untrusted.

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.

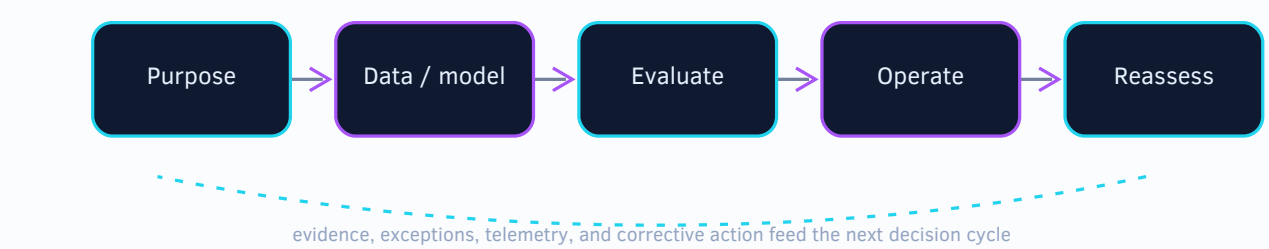
Adopting organizations SHOULD maintain a domain-specific risk register that identifies cause, affected asset or stakeholder, credible scenario, impact, existing controls, residual risk, owner, review trigger, and evidence. Risks that cross standards MUST be linked rather than copied into disconnected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

15. Governing Principles

- A credible non-AI baseline is part of AI design.
- Model output is untrusted until validated for its intended use.
- Evaluation must match the actual task, users, context, and consequence.
- Human review is not a control unless the reviewer has time, competence, evidence, and authority.
- Provider convenience does not override data, security, or accountability requirements.
- Every model-dependent behavior requires an explicit failure and retirement strategy.

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
AI accountable executive	Owns AI risk appetite and portfolio governance.
Product owner	Owns the user outcome and non-AI baseline.
AI system owner	Owns model, prompt, data, evaluation, provider, and lifecycle.
Model risk or validation lead	Independently evaluates fitness and harm.
Data owner	Approves training, retrieval, inference, and retention use.
Security and privacy lead	Owns threat model, data movement, abuse, and incident controls.
Human-oversight owner	Designs intervention, recourse, appeal, and escalation.
Operations owner	Monitors performance, drift, cost, incidents, and shutdown readiness.

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
Using AI where a deterministic control is available and adequate	Failure can create hidden risk, misleading assurance, uncontrolled cost, or unsafe operation.
Evaluating only with hand-selected prompts	Failure can create hidden risk, misleading assurance, uncontrolled cost, or unsafe operation.
Allowing model-generated confidence to serve as verification	Failure can create hidden risk, misleading assurance, uncontrolled cost, or unsafe operation.
Sending sensitive context to a provider without policy approval	Failure can create hidden risk, misleading assurance, uncontrolled cost, or unsafe operation.
Hiding AI involvement from affected users	Failure can create hidden risk, misleading assurance, uncontrolled cost, or unsafe operation.
Changing model or prompt without regression testing	Failure can create hidden risk, misleading assurance, uncontrolled cost, or unsafe operation.
Removing fallback because the primary model is usually available	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 **19 controls** across the following families:

- Purpose
- Impact
- Ownership
- Data
- Models
- Selection
- Evaluation
- Grounding
- Prompts
- Authority
- Human control
- Transparency
- Security
- Privacy
- Reliability
- Change
- Monitoring
- Incident

- Lifecycle

23. Normative Controls

CONTROL SET	PROFILES	ASSESSMENT
19	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-AIA-01 – AI use-case justification and baseline

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

Requirement

Each material AI capability MUST document the problem, intended users, expected benefit, non-AI baseline, reasons AI is appropriate, failure consequences, and criteria for retaining, replacing, or removing AI.

Purpose

Prevents unjustified complexity and automation theater.

Applicability

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

Implementation guidance

- Compare rules, search, statistics, and human workflow alternatives.
- Include cost, latency, privacy, and operability.

Required evidence

- Use-case record
- Baseline comparison
- Decision approval

Assessment procedure

- **Examine:** Review whether evidence supports AI selection.
- **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 AI RMF 1.0

NORMATIVE CONTROL

MYTHOS-FND-AIA-02 – AI impact and risk assessment

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

Requirement

Before deployment and after material change, the organization MUST assess affected people, rights, safety, security, privacy, environment, business processes, misuse, systemic effects, and reversibility.

Purpose

Makes consequence visible before commitment.

Applicability

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

Implementation guidance

- Include direct, indirect, cumulative, and reasonably foreseeable impacts.
- Engage affected expertise.

Required evidence

- Impact assessment
- Risk register
- Review record

Assessment procedure

- **Examine:** Trace mitigations to identified impacts.
- **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 42005:2025
- NIST AI RMF 1.0

NORMATIVE CONTROL

MYTHOS-FND-AIA-03 – Accountability and decision rights

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

Requirement

AI systems MUST have accountable owners for product outcome, model behavior, data, security, privacy, evaluation, operation, incident response, and risk acceptance, with conflicts and escalation paths documented.

Purpose

Prevents responsibility gaps across providers and teams.

Applicability

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

Implementation guidance

- Do not assign accountability to the model or vendor.

Required evidence

- RACI or equivalent
- Escalation map
- Approvals

Assessment procedure

- **Examine:** Interview owners on failure scenarios.
- **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 42001:2023

NORMATIVE CONTROL

MYTHOS-FND-AIA-04 – Training, retrieval, and inference data governance

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

Requirement

Data used for training, tuning, retrieval, evaluation, prompting, and inference MUST have documented provenance, rights, purpose, quality, sensitivity, retention, access, deletion, contamination, and representativeness controls.

Purpose

Controls legal, privacy, quality, and security risk.

Applicability

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

Implementation guidance

- Separate evaluation data from optimization.
- Detect secrets and personal data.

Required evidence

- Data inventory
- Lineage
- Rights and quality records

Assessment procedure

- **Examine:** Trace samples to source and purpose.
- **Interview:** Test deletion.
- **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 AI 600-1
- NIST Privacy Framework 1.0

NORMATIVE CONTROL

MYTHOS-FND-AIA-05 – Model and provider inventory

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

Requirement

The organization MUST maintain an inventory of models, versions, providers, deployment locations, licenses, capabilities, limitations, data-use terms, dependencies, safety settings, and approved use cases.

Purpose

Enables change control and incident response.

Applicability

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

Implementation guidance

- Include embeddings, rerankers, classifiers, and guard models.

Required evidence

- Model registry
- Provider assessments
- Deployment records

Assessment procedure

- **Examine:** Compare production calls to registry.
- **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 42001:2023

NORMATIVE CONTROL

MYTHOS-FND-AIA-06 – Model selection by measured fitness

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

Requirement

Model and provider selection MUST be based on versioned evaluation of task quality, risk, latency, reliability, cost, context behavior, data handling, portability, and operational constraints rather than reputation alone.

Purpose

Aligns model choice to real requirements.

Applicability

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

Implementation guidance

- Evaluate multiple sizes and local options.
- Record tradeoffs and lock-in.

Required evidence

- Selection benchmark
- Decision record
- Cost model

Assessment procedure

- **Examine:** Re-run selected cases.
- **Interview:** Inspect rejected alternatives.
- **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 AI RMF 1.0

NORMATIVE CONTROL

MYTHOS-FND-AIA-07 – Representative predeployment evaluation

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

Requirement

AI capabilities MUST pass versioned evaluations covering normal, boundary, ambiguous, multilingual or multimodal where applicable, adversarial, harmful, privacy, security, bias, hallucination, refusal, tool-use, latency, cost, and failure conditions.

Purpose

Provides evidence beyond demonstrations.

Applicability

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

Implementation guidance

- Use blinded or independent review where stakes warrant.
- Report confidence intervals and limitations.

Required evidence

- Evaluation suite
- Results
- Acceptance rules

Assessment procedure

- **Examine:** Reproduce sampled cases.
- **Interview:** Inspect hidden test separation.
- **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 AI 600-1
- NIST SP 800-218A

NORMATIVE CONTROL

MYTHOS-FND-AIA-08 – Grounding and source integrity

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

Requirement

When outputs depend on external knowledge, the system MUST define authoritative sources, retrieval permissions, freshness, provenance, ranking, conflict handling, citation behavior, injection resistance, and abstention criteria.

Purpose

Reduces unsupported and manipulated outputs.

Applicability

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

Implementation guidance

- Preserve source boundaries and access controls.
- Do not treat retrieved text as instruction by default.

Required evidence

- Retrieval design
- Source registry
- Grounding evaluations

Assessment procedure

- **Examine:** Inject conflicting and malicious documents.
- **Interview:** Verify access filtering.
- **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 AI 600-1
- OWASP Top 10 for LLM Applications 2025

NORMATIVE CONTROL

MYTHOS-FND-AIA-09 – Prompt and instruction governance

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

Requirement

Material system prompts, policies, tools, templates, and context assembly logic MUST be versioned, reviewed, tested, access-controlled, and traceable to deployed behavior.

Purpose

Treats instructions as executable policy.

Applicability

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

Implementation guidance

- Separate trusted policy from untrusted content.
- Prevent tenant leakage through shared context.

Required evidence

- Prompt registry
- Diffs and approvals
- Tests

Assessment procedure

- **Examine:** Verify deployed hash.
- **Interview:** Attempt instruction override.
- **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 800-218A

NORMATIVE CONTROL

MYTHOS-FND-AIA-10 – Action and decision boundaries

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

Requirement

AI-generated recommendations, decisions, and actions MUST be constrained by explicit policy, identity, authorization, resource, budget, temporal, and consequence boundaries enforced outside the model.

Purpose

Prevents language output from becoming ambient authority.

Applicability

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

Implementation guidance

- Use deterministic validation and approval for consequential actions.

Required evidence

- Authority policy
- Gateway configuration
- Negative tests

Assessment procedure

- **Examine:** Attempt unauthorized tool and resource use.
- **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 AI RMF 1.0
- OWASP LLM Top 10

NORMATIVE CONTROL

MYTHOS-FND-AIA-11 – Meaningful human oversight and recourse

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

Requirement

Where human review or intervention is required, the system MUST provide adequate context, uncertainty, alternatives, time, competence, authority, escalation, and recourse; nominal approval alone MUST NOT be treated as effective oversight.

Purpose

Prevents rubber-stamping and accountability theater.

Applicability

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

Implementation guidance

- Measure override and disagreement patterns.
- Support appeal for affected users.

Required evidence

- Oversight design
- Training records
- Decision samples

Assessment procedure

- **Examine:** Observe representative reviews.
- **Interview:** Test escalation and appeal.
- **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 AI RMF 1.0
- ISO/IEC 42005:2025

NORMATIVE CONTROL

MYTHOS-FND-AIA-12 – User disclosure and output provenance

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

Requirement

Users MUST be informed when AI materially generates, transforms, ranks, recommends, or acts, and consequential outputs MUST carry provenance sufficient to identify model or workflow version, relevant sources, transformations, and review status.

Purpose

Supports informed reliance and investigation.

Applicability

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

Implementation guidance

- Avoid implying human authorship or certainty.

Required evidence

- Disclosure design
- Provenance records
- User tests

Assessment procedure

- **Examine:** Trace a material output to its generation context.
- **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 AI 600-1

NORMATIVE CONTROL

MYTHOS-FND-AIA-13 – AI threat model and abuse resistance

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

Requirement

AI applications MUST maintain a threat model addressing prompt injection, data poisoning, model theft, extraction, insecure output handling, excessive agency, supply chain, denial of service, cross-tenant leakage, evasion, and unsafe tool use.

Purpose

Addresses AI-specific attack surfaces.

Applicability

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

Implementation guidance

- Test direct and indirect injection.
- Treat model output as untrusted input.

Required evidence

- Threat model
- Red-team results
- Mitigations

Assessment procedure

- **Examine:** Execute representative abuse cases.
- **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

- OWASP Top 10 for LLM Applications 2025
- NIST SP 800-218A

NORMATIVE CONTROL

MYTHOS-FND-AIA-14 – Privacy-preserving AI operation

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

Requirement

AI applications MUST minimize personal and sensitive data, enforce purpose and access boundaries, prevent unauthorized retention or provider use, support applicable rights, and evaluate memorization, inference, reidentification, and disclosure risk.

Purpose

Controls privacy risks unique to model workflows.

Applicability

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

Implementation guidance

- Prefer local or protected processing where justified.
- Redact before prompts when feasible.

Required evidence

- Privacy assessment
- Provider terms
- Leakage tests

Assessment procedure

- **Examine:** Submit canary secrets and deletion requests.
- **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 Privacy Framework 1.0
- NIST AI 600-1

NORMATIVE CONTROL

MYTHOS-FND-AIA-15 – Fallback, abstention, and degraded mode

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

Requirement

AI capabilities MUST define confidence or validity checks, abstention behavior, fallback modes, provider or model failure behavior, stale-context limits, timeout budgets, and safe recovery for material workflows.

Purpose

Maintains safe service when AI is uncertain or unavailable.

Applicability

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

Implementation guidance

- Prefer explicit unavailable state over fabricated completion.

Required evidence

- Fallback design
- Failure tests
- Operational playbook

Assessment procedure

- **Examine:** Disable model and retrieval dependencies.
- **Interview:** Force low-confidence 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

- ISO/IEC 25010:2023

NORMATIVE CONTROL

MYTHOS-FND-AIA-16 – Model, prompt, and provider change control

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

Requirement

Changes to models, providers, routing, prompts, retrieval, safety settings, data, tools, or decoding that may affect behavior MUST trigger impact analysis, regression evaluation, approval, staged release, and rollback according to risk.

Purpose

Prevents silent behavioral drift.

Applicability

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

Implementation guidance

- Treat provider aliases as mutable dependencies.
- Pin versions where possible.

Required evidence

- Change records
- Regression results
- Deployment evidence

Assessment procedure

- **Examine:** Introduce a model alias change.
- **Interview:** Verify gate and rollback.
- **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 800-218A

NORMATIVE CONTROL

MYTHOS-FND-AIA-17 – Production performance and harm monitoring

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

Requirement

Production AI systems MUST monitor task outcomes, quality proxies, drift, refusals, unsafe outputs, policy denials, latency, cost, provider changes, data quality, user feedback, and incidents with privacy-preserving sampling and escalation.

Purpose

Detects failures not captured before release.

Applicability

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

Implementation guidance

- Define leading and lagging indicators.
- Avoid treating model self-evaluation as sole evidence.

Required evidence

- Monitoring plan
- Dashboards
- Alerts and incident records

Assessment procedure

- **Examine:** Inject monitored failures.
- **Interview:** Review false negatives.
- **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 AI RMF 1.0

NORMATIVE CONTROL

MYTHOS-FND-AIA-18 – AI incident response and shutdown

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

Requirement

AI applications MUST support rapid containment, model or feature disablement, routing changes, evidence preservation, user and stakeholder notification, correction, rollback, and post-incident review.

Purpose

Limits harm from emergent or provider-driven failures.

Applicability

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

Implementation guidance

- Predefine kill switches that do not depend on the affected model.

Required evidence

- Incident plan
- Drill results
- Disablement evidence

Assessment procedure

- **Examine:** Run unsafe-output and provider-compromise exercises.
- **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-AIA-19 – Retirement, replacement, and record retention

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

Requirement

AI capabilities MUST define end-of-support, replacement, migration, data and artifact retention, reproducibility, user communication, dependent-workflow handling, and deletion requirements.

Purpose

Prevents abandoned models and irreproducible decisions.

Applicability

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

Implementation guidance

- Retain evidence proportionate to consequence and law.

Required evidence

- Retirement plan
- Migration tests
- Retention records

Assessment procedure

- **Examine:** Retire a test model version and verify dependencies.
- **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	Use-case justification, impact assessment, inventory, data governance, model fitness, evaluation, grounding, prompt control, action boundary, disclosure, fallback, monitoring, incident response, and retirement.
Enterprise	Central AI inventory, provider policy, evaluation platform, prompt and model registry, continuous monitoring, human-oversight operations, source governance, and audit-ready evidence.
High Assurance	Independent validation, adversarial and red-team evaluation, strict provider placement, protected datasets, constrained decoding, external authorization, continuous harm monitoring, supervised shutdown, and regulatory evidence packages.

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

- Using AI where a deterministic control is available and adequate
- Evaluating only with hand-selected prompts
- Allowing model-generated confidence to serve as verification
- Sending sensitive context to a provider without policy approval
- Hiding AI involvement from affected users
- Changing model or prompt without regression testing
- Removing fallback because the primary model is usually available

30. Adoption Roadmap from Source Draft

- Document use case, non-AI baseline, impact, authority, data, model, and provider decisions.
- Build versioned evaluation, threat, privacy, and fallback plans before production integration.
- Deploy through policy-enforced gateways with provenance, telemetry, limits, and rollback.
- Establish continuous evaluation, incident response, model-change governance, and user recourse.
- For High Assurance, add independent validation, adversarial testing, stronger isolation, reproducibility, and formal constraints for consequential actions.

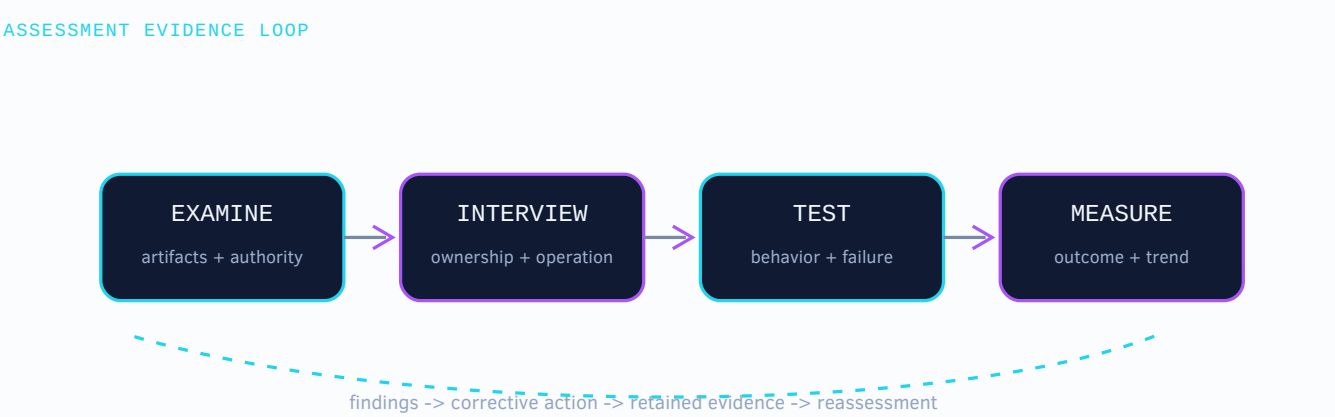
31. Limitations and Residual Risk from Source Draft

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
Evaluation coverage	Material capabilities and risk scenarios represented in versioned suites	100% of release-critical capabilities
Critical failure rate	High-consequence evaluation cases failing acceptance criteria	

Metric	Definition	Expected use or target
		0 at release unless formally accepted
Grounded-answer support	Material factual outputs supported by approved evidence when grounding is required	Target defined by use case
Unsafe action prevention	Unauthorized or policy-violating model-originated actions blocked	100% in defined tests
Drift detection latency	Time to identify material performance or risk regression	Risk-based service objective

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.

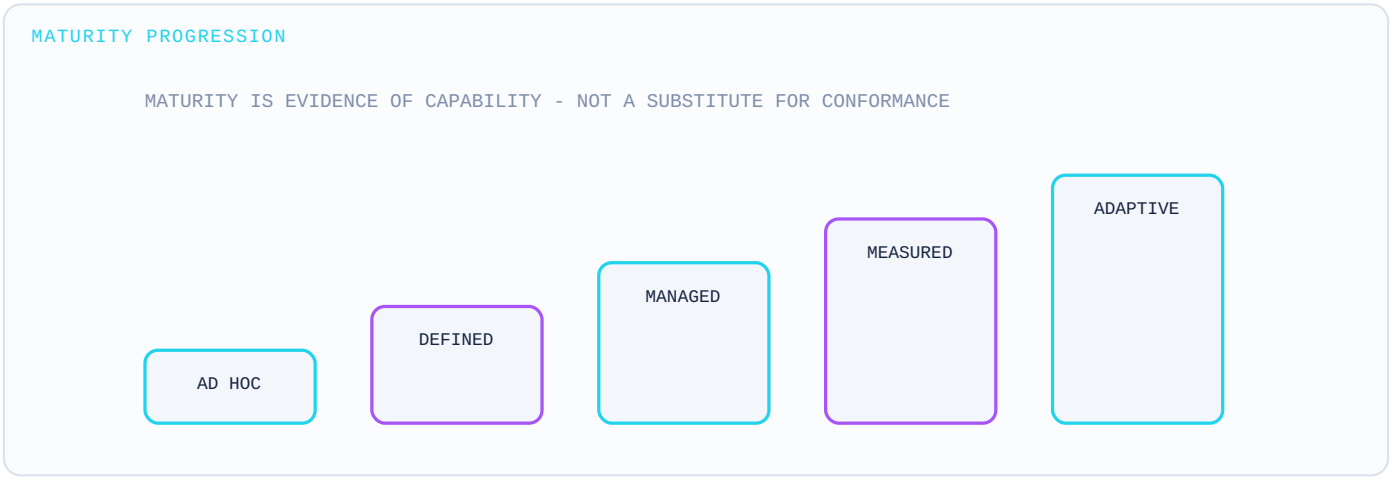
34. Exceptions and Compensating Controls

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
AI use cases without approved baseline	Defined by the adopting organization with owner, source, target, and cadence.
models and providers without current inventory	Defined by the adopting organization with owner, source, target, and cadence.
evaluation cases mapped to material risks	Defined by the adopting organization with owner, source, target, and cadence.
grounded claims with valid source support	Defined by the adopting organization with owner, source, target, and cadence.
unsupported-answer and abstention rates	Defined by the adopting organization with owner, source, target, and cadence.
high-impact actions requiring human or external authorization	Defined by the adopting organization with owner, source, target, and cadence.
production drift and harm indicators	Defined by the adopting organization with owner, source, target, and cadence.
AI incidents and shutdown exercises	Defined by the adopting organization with owner, source, target, and cadence.
users receiving required disclosure and recourse	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 AI RMF 1.0	AI risk management	https://www.nist.gov/itl/ai-risk-management-framework	Current; revision program active	2026-09-17
NIST AI 600-1	Generative AI Profile	https://www.nist.gov/publications/artificial-intelligence-risk-management-framework-generative-artificial-intelligence	Final	2026-09-17
NIST SP 800-218A	SSDF Community Profile for Generative AI and Dual-Use Foundation Models	https://csrc.nist.gov/pubs/sp/800/218/a/final	Final	2026-09-17
ISO/IEC 42001:2023	AI management systems	https://www.iso.org/standard/42001	Published	2026-09-17
ISO/IEC 23894:2023	AI risk management guidance	https://www.iso.org/standard/77304.html	Published	2026-09-17
ISO/IEC 42005:2025	AI system impact assessment	https://www.iso.org/standard/42005	Published	2026-09-17
ISO/IEC 5338:2023	AI system life cycle processes	https://www.iso.org/standard/81118.html	Published	2026-09-17
Regulation (EU) 2024/1689	Artificial Intelligence Act	https://eur-lex.europa.eu/eli/reg/2024/1689/	In force; staged application	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

- Recasts “AI-first” as disciplined product architecture rather than mandatory model use.
- Integrates current AI risk, secure development, impact assessment, and application security patterns.
- Separates AI application governance from the deeper multi-agent orchestration controls in MYTHOS-FND-0010.

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-AIA-01	Purpose	AI use-case justification and baseline	Foundational, Advanced, High Assurance	Partial	Critical
MYTHOS-FND-AIA-02	Impact	AI impact and risk assessment	Foundational, Advanced, High Assurance	Partial	Critical
MYTHOS-FND-AIA-03	Ownership	Accountability and decision rights	Foundational, Advanced, High Assurance	Low	Critical
MYTHOS-FND-AIA-04	Data	Training, retrieval, and inference data governance	Foundational, Advanced, High Assurance	Partial	Critical
MYTHOS-FND-AIA-05	Models	Model and provider inventory	Foundational, Advanced, High Assurance	High	Critical
MYTHOS-FND-AIA-06	Selection	Model selection by measured fitness	Foundational, Advanced, High Assurance	Partial	Material
MYTHOS-FND-AIA-07	Evaluation	Representative predeployment evaluation	Foundational, Advanced, High Assurance	Partial	Critical
MYTHOS-FND-AIA-08	Grounding	Grounding and source integrity	Foundational, Advanced, High Assurance	Partial	Critical
MYTHOS-FND-AIA-09	Prompts	Prompt and instruction governance	Foundational, Advanced, High Assurance	High	Critical
MYTHOS-FND-AIA-10	Authority	Action and decision boundaries	Foundational, Advanced, High Assurance	High	Critical
MYTHOS-FND-AIA-11	Human control	Meaningful human oversight and recourse	Foundational, Advanced, High Assurance	Partial	Critical

Control	Family	Title	Profiles	Automation	Impact
MYTHOS-FND-AIA-12	Transparency	User disclosure and output provenance	Foundational, Advanced, High Assurance	Partial	Material
MYTHOS-FND-AIA-13	Security	AI threat model and abuse resistance	Advanced, High Assurance	Partial	Critical
MYTHOS-FND-AIA-14	Privacy	Privacy-preserving AI operation	Foundational, Advanced, High Assurance	Partial	Critical
MYTHOS-FND-AIA-15	Reliability	Fallback, abstention, and degraded mode	Foundational, Advanced, High Assurance	Partial	Critical
MYTHOS-FND-AIA-16	Change	Model, prompt, and provider change control	Foundational, Advanced, High Assurance	High	Critical
MYTHOS-FND-AIA-17	Monitoring	Production performance and harm monitoring	Advanced, High Assurance	Partial	Critical
MYTHOS-FND-AIA-18	Incident	AI incident response and shutdown	Advanced, High Assurance	High	Critical
MYTHOS-FND-AIA-19	Lifecycle	Retirement, replacement, and record retention	Advanced, High Assurance	Partial	Material

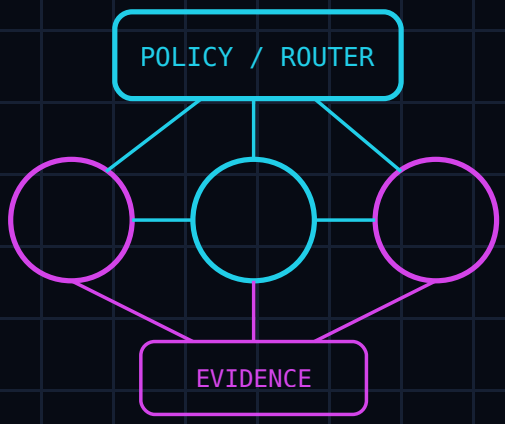
Appendix D – Minimum Conformance Claim Record

```
standard: MYTHOS-FND-0009
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



CANDIDATE STANDARD

Mythos Agentic Systems and Model Orchestration Standard

Bound delegated action with mission contracts, policy, tool controls, memory governance, budgets, evidence, verification, and containment.

PERMANENT ID
MYTHOS-FND-0010

PUBLICATION CLASS
CANDIDATE STANDARD

VERSION / STATUS
1.0.0-candidate / CANDIDATE

PERMANENT PUBLICATION IDENTITY

Mythos Agentic Systems and Model Orchestration Standard

Universal Requirements for Governed Agents, Multi-Model Routing, Tool Use, Memory, Durable Workflows, Delegation, and Autonomous Execution

Document ID
MYTHOS-FND-0010

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	23	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	Agent and AI platform architects; Software, automation, and infrastructure engineers; Security, safety, privacy, and governance teams; Operations and incident-response teams; Assessors and model-risk owners
Publisher / owner	Mythos Systems / Standards Program
Public classification	Public technical standard
Canonical route	/library/standards/foundation/mythos-fnd-0010/

Expected outcomes

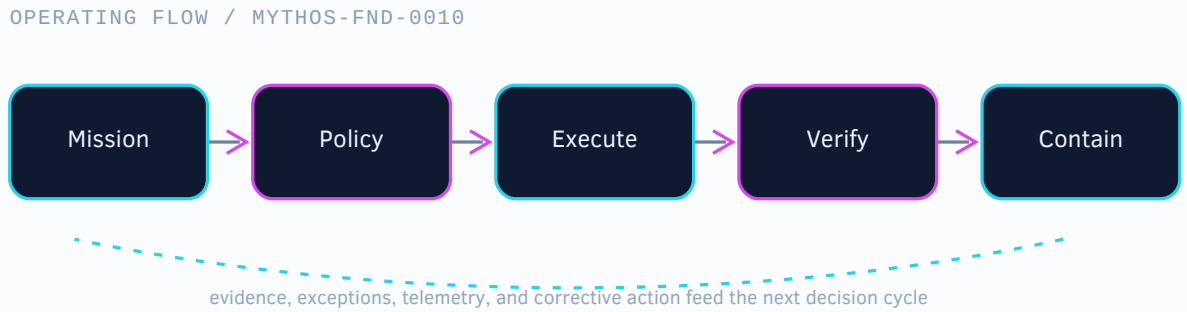
- Separate model reasoning from execution authority and policy enforcement.
- Constrain delegation, recursion, memory, tools, budgets, and cross-agent communication.
- Make every consequential action attributable, reviewable, resumable, and recoverable.
- Enable multi-model and multi-agent systems without surrendering security, reliability, or human accountability.

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.

Document Control 8

Revision Record 8

How to Use This Standard 9

Executive Reading Path 9

Engineering Reading Path 9

Assessment Reading Path 9

Normative and Informative Content 9

Part I – Executive Direction 10

1. Executive Overview 10

2. Executive Findings and Required Direction 10

3. Business and Operational Impact 10

4. Target-State Summary 11

5. Leadership Responsibilities 12

Part II – Standard Foundation 14

6. Purpose and Objectives 14

7. Scope 14

8. Intended Audience 14

9. Requirements Language and Conformance 14

10. Normative References from Source Draft 14

11. Informative References from Source Draft 15

12. Terms and Definitions 15

13. Applicability and Tailoring 16

Part III – Risk and Architecture 17

14. Enterprise Problem and Risk Landscape 17

15. Governing Principles 17

16. Reference Operating Architecture 17
17. Roles and Accountability 18
18. State, Evidence, and Decision Model 19
19. Security and Trust Considerations 19
20. Failure Modes 19
21. Cross-Functional Dependencies 19

Part IV – Normative Control System 21

22. Control-Family Overview 21
23. Normative Controls 22

Part V – Implementation and Operations 46

24. Implementation Profiles 46
25. Implementation Lifecycle 46
26. Integration Requirements 47
27. Failure Handling and Recovery 47
28. Exceptions and Compensating Controls 47
29. Prohibited Practices 47
30. Adoption Roadmap from Source Draft 48
31. Limitations and Residual Risk from Source Draft 48

Part VI – Assurance and Assessment 49

32. Assessment Methodology 49
33. Metrics and Reporting from Source Draft 49
34. Exceptions and Compensating Controls 50
35. Enterprise Metric Set 50
36. Maturity Model 51
37. Assessment Confidence 51
38. Executive Assurance Dashboard 51

Part VII – Authority and Traceability 53

39. Cross-Standard Dependencies from Source Draft 53
40. Current External Authority Register 53

41. Control Traceability 53

42. Source-Draft Preservation 54

Part VIII – Appendices **55**

Appendix A — Source-Draft Evolution Notes 55

Appendix B — Change History 55

Appendix C — Control Summary 55

Appendix D — Minimum Conformance Claim Record 56

Appendix E — Publication Review Checklist 56

NORMATIVE SYSTEM

Control index

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

MYTHOS-FND-AGT-01	Agent and mission inventory	23
MYTHOS-FND-AGT-02	Bounded mission contract	24
MYTHOS-FND-AGT-03	Workload and agent identity	25
MYTHOS-FND-AGT-04	External policy enforcement	26
MYTHOS-FND-AGT-05	Constrained delegation and lineage	27
MYTHOS-FND-AGT-06	Plan validation before execution	28
MYTHOS-FND-AGT-07	Tool contract and safety classification	29
MYTHOS-FND-AGT-08	Sandboxed and scoped execution	30
MYTHOS-FND-AGT-09	Visual and computer-use action control	31
MYTHOS-FND-AGT-10	Governed memory lifecycle	32
MYTHOS-FND-AGT-11	Context assembly and trust boundaries	33
MYTHOS-FND-AGT-12	Model routing policy	34
MYTHOS-FND-AGT-13	Resource and recursion budgets	35
MYTHOS-FND-AGT-14	Durable state and exactly-once effect strategy	36
MYTHOS-FND-AGT-15	Fan-out, fan-in, and conflict control	37
MYTHOS-FND-AGT-16	Independent approval and separation of duties	38
MYTHOS-FND-AGT-17	Governed skill creation and modification	39
MYTHOS-FND-AGT-18	End-to-end execution evidence	40
MYTHOS-FND-AGT-19	Independent result verification	41
MYTHOS-FND-AGT-20	Pause, cancel, rollback, and containment	42
MYTHOS-FND-AGT-21	Behavioral and operational monitoring	43
MYTHOS-FND-AGT-22	Agentic incident response	44
MYTHOS-FND-AGT-23	Agent, model, tool, and memory retirement	45

Document Control

Field	Value
Document ID	MYTHOS-FND-0010
Standard	Agentic Systems and Model Orchestration
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

Agentic systems turn model output into multi-step work involving memory, tools, credentials, files, browsers, terminals, infrastructure, and other agents. This creates a larger authority and failure surface than ordinary AI applications. This standard defines agentic systems as governed distributed systems: missions are bounded, identities are explicit, plans are typed, permissions are external, execution is deterministic, state is durable, results are independently verified, and the full chain is preserved as evidence.

The institutional objective is to govern bounded missions, agent and workload identity, external policy, delegation, planning, tools, sandboxing, memory, context, routing, budgets, durable execution, multi-agent coordination, approvals, skills, evidence, verification, containment, incidents, and retirement. 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
Unbounded mission authority	Agents receive broad objectives without explicit scope, budgets, targets, or stopping conditions.	Require a typed mission contract and capability requests.
Agent identity collapse	Human, agent, model, tool, and workload identities are conflated.	Use distinct identities and preserve delegation lineage.
Tool ambiguity	Natural-language tool descriptions conceal side effects and failure semantics.	Use versioned typed contracts, risk classification, validation, and post-checks.
Memory and context poisoning	Untrusted content is promoted into durable memory or treated as instructions.	Separate trust domains, source memory, require review, and support correction and deletion.
False execution guarantees	Distributed retries create duplicates or indeterminate effects while systems claim exactly-once execution.	Use idempotency, effect ledgers, reconciliation, and explicit indeterminate state.
Multi-agent consensus mistaken for truth	Several models can agree on the same unsupported conclusion.	Use independent evidence, conflict control, deterministic tests, and verification.

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.

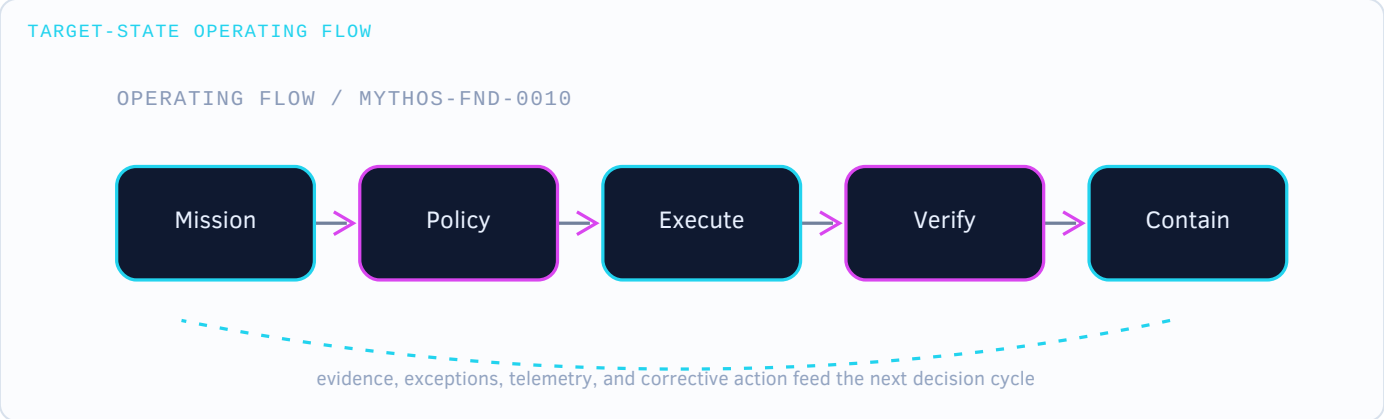
3.3 Security, Privacy, and Trust Impact

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	Agent, mission, tool, model, skill, and memory inventory
2	Bounded mission contract
3	Human, agent, workload, and tool identity
4	External policy enforcement
5	Constrained delegation and lineage
6	Plan validation and LOGOS-style typed work
7	Tool contracts and safety classes
8	Sandboxed and scoped execution
9	Visual and computer-use control
10	Governed memory lifecycle

#	Target-State Component
11	Context assembly and trust boundaries
12	Model routing policy
13	Resource, time, and recursion budgets
14	Durable workflow state and effect strategy
15	Fan-out, fan-in, and conflict resolution
16	Approvals and separation of duties
17	Governed skill lifecycle
18	End-to-end evidence
19	Independent result verification
20	Pause, cancel, rollback, and containment
21	Behavioral and operational monitoring
22	Agentic incident response
23	Retirement

```
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
Agentic-system owner	Owns the mission, agent, model, tool, and runtime architecture.
Policy authority	Owns capability, delegation, approval, and emergency policy.
Runtime owner	Owns durable state, scheduling, retries, cancellation, and effect control.
Model-routing owner	Owns model eligibility, fitness, fallback, and cost.
Tool and connector owner	Owns contracts, side effects, versioning, and verification.
Memory and knowledge owner	Owns context, memory promotion, provenance, correction, and deletion.
Independent verifier	Tests plans, outputs, effects, and failure recovery.
Incident commander	Coordinates containment, revocation, evidence, and recovery.

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

- Separate model reasoning from execution authority and policy enforcement.
- Constrain delegation, recursion, memory, tools, budgets, and cross-agent communication.
- Make every consequential action attributable, reviewable, resumable, and recoverable.
- Enable multi-model and multi-agent systems without surrendering security, reliability, or human accountability.

7. Scope

Applies to autonomous and semi-autonomous agents, copilots with tools, multi-agent systems, supervisors, planners, model routers, durable agent workflows, computer-use systems, coding agents, infrastructure agents, research agents, and agent-accessible extension ecosystems.

8. Intended Audience

- Agent and AI platform architects
- Software, automation, and infrastructure engineers
- Security, safety, privacy, and governance teams
- Operations and incident-response teams
- Assessors and model-risk owners

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 AI 100-1** — Artificial Intelligence Risk Management Framework (AI RMF 1.0). https://doi.org/10.6028/NIST.AI.100-1
- **NIST AI 600-1** — Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile. https://doi.org/10.6028/NIST.AI.600-1
- **NIST SP 800-218A** — Secure Software Development Practices for Generative AI and Dual-Use Foundation Models. https://csrc.nist.gov/pubs/sp/800/218/a/final
- **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
- **NIST SP 800-207** — Zero Trust Architecture. https://doi.org/10.6028/NIST.SP.800-207
- **OWASP Top 10 for Agentic Applications 2026** — Risk taxonomy for agentic applications. https://genai.owasp.org/
- **OWASP Top 10 for LLM Applications 2025** — Risk taxonomy for applications using large language models. https://genai.owasp.org/llm-top-10/
- **ISO/IEC 42001:2023** — Artificial intelligence — Management system. https://www.iso.org/standard/81230.html

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.
Agent	A software entity that uses one or more models or policies to select, sequence, or adapt actions toward an objective.

Term	Definition
Mission	A bounded unit of agentic work with explicit objective, authority, budget, state, checkpoints, and completion criteria.
Tool	A callable capability that can observe, transform, communicate with, or change a resource or environment.
Delegation chain	The recorded lineage by which authority, objectives, context, and constraints pass from an originator through supervisors and subagents.
Durable state	Persisted workflow state sufficient to resume, inspect, reconcile, or terminate work after interruption.

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.

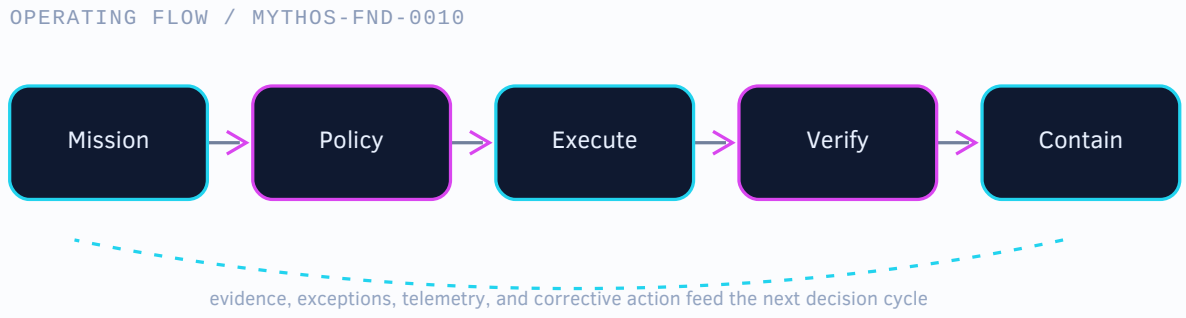
Adopting organizations SHOULD maintain a domain-specific risk register that identifies cause, affected asset or stakeholder, credible scenario, impact, existing controls, residual risk, owner, review trigger, and evidence. Risks that cross standards MUST be linked rather than copied into disconnected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

15. Governing Principles

- Probabilistic planning must execute through deterministic policy enforcement.
- Delegated authority can narrow but cannot silently expand.
- Every mission has bounded scope, budget, lifetime, and termination conditions.
- Memory is governed data, not an unquestioned source of truth.
- Parallelism and recursion require explicit fan-out, depth, cost, and convergence limits.
- Agents cannot approve their own privilege expansion, evidence sufficiency, or risk acceptance.
- Interruptibility, rollback, reconciliation, and evidence are core runtime properties.

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
Agentic-system owner	Owns the mission, agent, model, tool, and runtime architecture.
Policy authority	Owns capability, delegation, approval, and emergency policy.
Runtime owner	Owns durable state, scheduling, retries, cancellation, and effect control.
Model-routing owner	Owns model eligibility, fitness, fallback, and cost.
Tool and connector owner	Owns contracts, side effects, versioning, and verification.
Memory and knowledge owner	Owns context, memory promotion, provenance, correction, and deletion.
Independent verifier	Tests plans, outputs, effects, and failure recovery.
Incident commander	Coordinates containment, revocation, evidence, and recovery.

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
Giving agents a general shell or browser because the user asked for autonomy	Failure can create hidden risk, misleading assurance, uncontrolled cost, or unsafe operation.
Treating a skill file as permission	Failure can create hidden risk, misleading assurance, uncontrolled cost, or unsafe operation.
Allowing agents to edit their own policy or evidence	Failure can create hidden risk, misleading assurance, uncontrolled cost, or unsafe operation.
Using one giant conversation as durable state	Failure can create hidden risk, misleading assurance, uncontrolled cost, or unsafe operation.
Calling retries exactly-once execution	Failure can create hidden risk, misleading assurance, uncontrolled cost, or unsafe operation.
Accepting multi-agent agreement without tests	Failure can create hidden risk, misleading assurance, uncontrolled cost, or unsafe operation.
Allowing computer-use agents unrestricted targets	Failure can create hidden risk, misleading assurance, uncontrolled cost, or unsafe operation.
Persisting every conversation statement as memory	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.

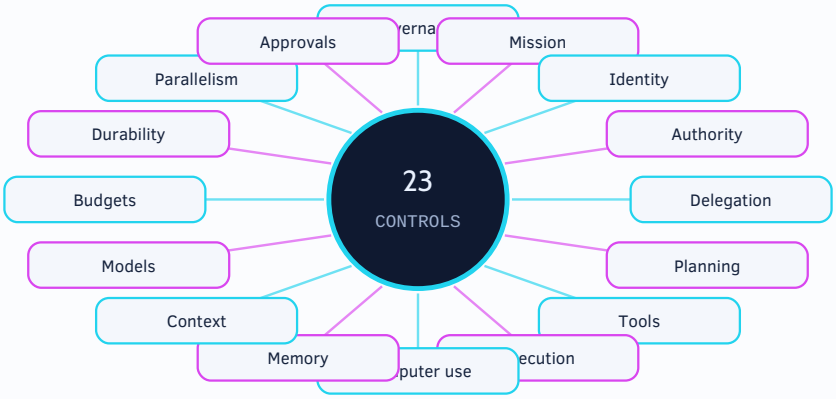
An adopting organization MUST resolve overlapping requirements through the stricter applicable control or a documented authority decision.

FOUNDATION STANDARD / STRUCTURAL PART

Part IV – Normative Control System

22. Control-Family Overview

CONTROL-FAMILY CONSTELLATION



This standard contains **23 controls** across the following families:

- Governance
- Mission
- Identity
- Authority
- Delegation
- Planning
- Tools
- Execution
- Computer use
- Memory
- Context
- Models
- Budgets
- Durability
- Parallelism
- Approvals
- Skills
- Evidence

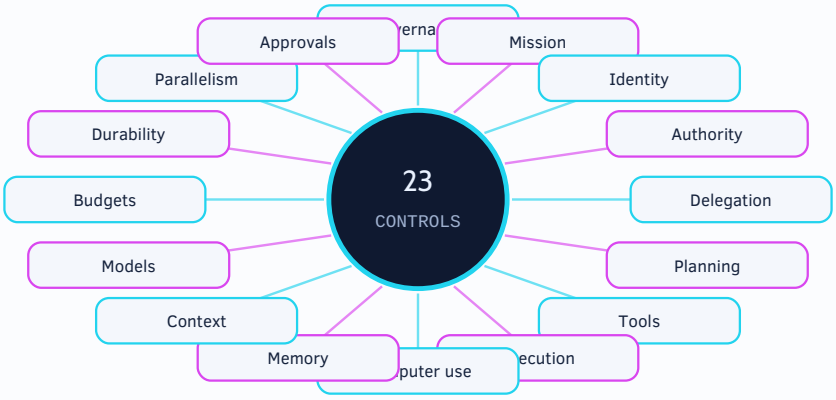
- Verification
- Interruptibility
- Monitoring
- Incident
- Lifecycle

23. Normative Controls

CONTROL SET	PROFILES	ASSESSMENT
23	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-AGT-01 – Agent and mission inventory

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

Requirement

The organization MUST inventory agent types, owners, models, tools, memories, environments, identities, permitted missions, autonomy levels, data classes, and maximum consequence.

Purpose

Creates a bounded governance surface.

Applicability

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

Implementation guidance

- Include ephemeral subagents and third-party agents.

Required evidence

- Agent registry
- Mission catalog
- Ownership records

Assessment procedure

- **Examine:** Compare runtime identities and tool calls to registry.
- **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 42001:2023

NORMATIVE CONTROL

MYTHOS-FND-AGT-02 – Bounded mission contract

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

Requirement

Every mission MUST define objective, originator, accountable owner, scope, targets, constraints, inputs, authority, budgets, completion criteria, stop conditions, evidence requirements, and expiration before consequential execution.

Purpose

Prevents open-ended or ambiguous autonomy.

Applicability

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

Implementation guidance

- Use machine-readable mission envelopes.
- Reject missing mandatory constraints.

Required evidence

- Mission record
- Schema validation
- Approval evidence

Assessment procedure

- **Examine:** Submit ambiguous and expired missions.
- **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 AI RMF 1.0

NORMATIVE CONTROL

MYTHOS-FND-AGT-03 – Workload and agent identity

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

Requirement

Agents, supervisors, runtimes, tools, and delegated workers MUST use distinguishable, authenticated identities bound to mission and trust-domain context; shared ambient identities MUST NOT authorize consequential actions.

Purpose

Enables attribution and least privilege.

Applicability

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

Implementation guidance

- Use short-lived workload credentials.
- Bind model sessions to execution identity without equating them.

Required evidence

- Identity architecture
- Credential records
- Authentication tests

Assessment procedure

- **Examine:** Replay credentials across missions or tenants.
- **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 800-207

NORMATIVE CONTROL

MYTHOS-FND-AGT-04 – External policy enforcement

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

Requirement

All consequential tool calls and state changes MUST pass through deterministic authorization and policy enforcement outside the model using current identity, mission, resource, tenant, environment, risk, and approval state.

Purpose

Prevents prompts or model output from self-authorizing.

Applicability

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

Implementation guidance

- Default deny.
- Validate arguments and preconditions.

Required evidence

- Policy rules
- Gateway logs
- Negative tests

Assessment procedure

- **Examine:** Attempt unauthorized and policy-conflicting calls.
- **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 family

NORMATIVE CONTROL

MYTHOS-FND-AGT-05 – Constrained delegation and lineage

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

Requirement

Delegation MUST preserve origin, objective, context, constraints, authority, budgets, data classification, and evidence lineage; a delegate MUST NOT expand authority, lifetime, scope, or approval rights beyond the delegator's grant.

Purpose

Contains authority through agent hierarchies.

Applicability

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

Implementation guidance

- Use capability attenuation.
- Record fan-out and delegated sub-budgets.

Required evidence

- Delegation graph
- Grant records
- Tests

Assessment procedure

- **Examine:** Attempt privilege amplification and hidden subagents.
- **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-AGT-06 – Plan validation before execution

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

Requirement

Plans for consequential work MUST be validated for scope, dependencies, ordering, preconditions, conflicts, policy, expected effects, rollback, and evidence before execution; validation MUST be independent of the proposing model where risk warrants.

Purpose

Catches unsafe reasoning before action.

Applicability

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

Implementation guidance

- Compile plans to typed operations.
- Use simulation or dry run.

Required evidence

- Plan schema
- Validation output
- Approval records

Assessment procedure

- **Examine:** Insert unsafe or contradictory step.
- **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 AI RMF 1.0

NORMATIVE CONTROL

MYTHOS-FND-AGT-07 – Tool contract and safety classification

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

Requirement

Each tool MUST have a versioned contract defining identity, inputs, outputs, side effects, authorization, idempotency, limits, secrets, failure semantics, observability, reversibility, and risk classification.

Purpose

Makes tool behavior enforceable.

Applicability

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

Implementation guidance

- Separate read from mutate.
- Reject unstructured shell access for routine operations where narrower tools exist.

Required evidence

- Tool registry
- Schemas
- Conformance tests

Assessment procedure

- **Examine:** Call with malformed, excessive, and unauthorized arguments.
- **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 800-218A

NORMATIVE CONTROL

MYTHOS-FND-AGT-08 – Sandboxed and scoped execution

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

Requirement

Agent-generated code, commands, browser actions, files, and workloads MUST execute in an isolated, resource-bounded, policy-controlled environment appropriate to consequence, with explicit promotion gates to shared or production systems.

Purpose

Contains malicious or defective execution.

Applicability

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

Implementation guidance

- Use disposable environments where practical.
- Control network and filesystem mounts.

Required evidence

- Sandbox design
- Policy
- Escape tests

Assessment procedure

- **Examine:** Attempt host, network, secret, and tenant boundary escape.
- **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-AGT-09 – Visual and computer-use action control

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

Requirement

Agents operating graphical interfaces or remote computers MUST anchor actions to verified target state, detect unexpected UI changes, avoid hidden or ambiguous elements, limit sensitive capture, and require stronger confirmation for consequential interactions.

Purpose

Addresses brittle and spoofable visual automation.

Applicability

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

Implementation guidance

- Prefer semantic APIs over pixels when available.
- Revalidate after navigation or modal changes.

Required evidence

- Computer-use policy
- Session recordings or event logs
- Adversarial tests

Assessment procedure

- **Examine:** Introduce overlays, shifted controls, and deceptive prompts.
- **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 AI 600-1

NORMATIVE CONTROL

MYTHOS-FND-AGT-10 – Governed memory lifecycle

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

Requirement

Agent memory MUST have defined purpose, source, provenance, confidence, scope, tenancy, sensitivity, retention, update, conflict, correction, retrieval, and deletion rules and MUST NOT be treated as authoritative without validation.

Purpose

Prevents stale, poisoned, or cross-context memory from controlling behavior.

Applicability

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

Implementation guidance

- Separate episodic, semantic, procedural, and user-controlled memory.
- Protect shared memory writes.

Required evidence

- Memory schema
- Access policy
- Poisoning and deletion tests

Assessment procedure

- **Examine:** Insert conflicting and malicious memory.
- **Interview:** Test tenant isolation.
- **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 AI 600-1

NORMATIVE CONTROL

MYTHOS-FND-AGT-11 – Context assembly and trust boundaries

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

Requirement

The runtime MUST label and preserve trust, source, freshness, sensitivity, and instruction status across prompts, retrieved content, memory, tool output, user input, and system policy, and MUST prevent untrusted content from silently becoming higher-priority instruction.

Purpose

Mitigates context confusion and indirect prompt injection.

Applicability

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

Implementation guidance

- Use typed context segments.
- Apply least-context and access filtering.

Required evidence

- Context schema
- Assembly traces
- Injection tests

Assessment procedure

- **Examine:** Embed instructions in documents and tool output.
- **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

- OWASP Top 10 for Agentic Applications 2026

NORMATIVE CONTROL

MYTHOS-FND-AGT-12 – Model routing policy

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

Requirement

Model selection and routing MUST follow versioned policy based on task, data sensitivity, capability, risk, latency, cost, availability, jurisdiction, evaluation evidence, and provider terms, with logged rationale and bounded fallback.

Purpose

Prevents arbitrary or unsafe provider switching.

Applicability

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

Implementation guidance

- Never route sensitive context to an unapproved provider.
- Evaluate fallbacks independently.

Required evidence

- Routing policy
- Model registry
- Routing logs

Assessment procedure

- **Examine:** Force provider outage and sensitive task.
- **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 AI RMF 1.0

NORMATIVE CONTROL

MYTHOS-FND-AGT-13 – Resource and recursion budgets

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

Requirement

Missions MUST enforce approved limits for time, tokens, cost, tool calls, concurrency, subagents, recursion depth, storage, network, and changed resources, with deterministic stop or escalation behavior.

Purpose

Prevents runaway consumption and uncontrolled scope growth.

Applicability

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

Implementation guidance

- Allocate sub-budgets rather than duplicating parent budget.

Required evidence

- Budget policy
- Runtime counters
- Limit tests

Assessment procedure

- **Examine:** Trigger each budget limit and race conditions.
- **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 AI 600-1

NORMATIVE CONTROL

MYTHOS-FND-AGT-14 – Durable state and exactly-once effect strategy

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

Requirement

Consequential workflows MUST persist authoritative state, action identifiers, approvals, checkpoints, tool outcomes, retries, and compensation status sufficient to resume or reconcile without unintended repeated effects.

Purpose

Controls interruption and uncertain outcomes.

Applicability

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

Implementation guidance

- Separate workflow state from model transcript.
- Use idempotency and deduplication.

Required evidence

- State model
- Execution journal
- Recovery tests

Assessment procedure

- **Examine:** Crash between request and acknowledgment.
- **Interview:** Resume and reconcile.
- **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 25010:2023 — reliability

NORMATIVE CONTROL

MYTHOS-FND-AGT-15 – Fan-out, fan-in, and conflict control

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

Requirement

Parallel agents and tasks MUST have explicit partitioning, authority, shared-state rules, synchronization, conflict detection, result validation, convergence criteria, and bounded fan-out.

Purpose

Prevents duplicated effects and inconsistent synthesis.

Applicability

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

Implementation guidance

- Use immutable inputs where possible.
- Do not allow competing writers without coordination.

Required evidence

- Concurrency design
- Task graph
- Conflict tests

Assessment procedure

- **Examine:** Run duplicate and conflicting agents.
- **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 25010:2023

NORMATIVE CONTROL

MYTHOS-FND-AGT-16 – Independent approval and separation of duties

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

Requirement

Agents MUST NOT approve their own privilege expansion, production promotion, evidence sufficiency, policy exception, risk acceptance, or irreversible high-consequence action; required approval MUST come from an authorized independent principal or deterministic policy.

Purpose

Preserves accountability and prevents self-authorization.

Applicability

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

Implementation guidance

- Define quorum or dual control for highest risk.

Required evidence

- Approval policy
- Decision records
- Bypass tests

Assessment procedure

- **Examine:** Attempt self-approval and approval replay.
- **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-5

NORMATIVE CONTROL

MYTHOS-FND-AGT-17 – Governed skill creation and modification

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

Requirement

Agent-created or modified skills, prompts, policies, code, and tools MUST be sandboxed, versioned, evaluated, provenance-tracked, permission-scoped, reviewed, and rollback-capable before broader use; creation MUST NOT imply publication or privilege.

Purpose

Allows learning without silent self-modification.

Applicability

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

Implementation guidance

- Separate propose, test, approve, publish, and execute.

Required evidence

- Skill registry
- Provenance
- Evaluation and review records

Assessment procedure

- **Examine:** Create a skill requesting new privilege.
- **Interview:** Attempt silent replacement.
- **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 800-218A
- SLSA 1.2

NORMATIVE CONTROL

MYTHOS-FND-AGT-18 – End-to-end execution evidence

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

Requirement

Consequential missions MUST produce tamper-evident evidence linking objective, inputs, context sources, plan, models, prompts or policy versions, delegation, approvals, tool calls, diffs, outputs, verification, exceptions, and final state.

Purpose

Supports audit and trustworthy completion claims.

Applicability

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

Implementation guidance

- Store hashes or references instead of unnecessary sensitive payloads.

Required evidence

- Evidence bundle
- Integrity validation
- Reconstruction report

Assessment procedure

- **Examine:** Reconstruct a sampled mission and detect tampering.
- **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 — AU family

NORMATIVE CONTROL

MYTHOS-FND-AGT-19 – Independent result verification

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

Requirement

Agents MUST verify consequential outcomes against explicit acceptance criteria using authoritative observations, tests, reconciliation, or independent evaluators before declaring completion.

Purpose

Prevents self-reported success from substituting for reality.

Applicability

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

Implementation guidance

- Use different evidence paths than the action path where possible.

Required evidence

- Acceptance criteria
- Verification results
- Completion decision

Assessment procedure

- **Examine:** Cause partial failure and misleading tool output.
- **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 AI RMF 1.0

NORMATIVE CONTROL

MYTHOS-FND-AGT-20 – Pause, cancel, rollback, and containment

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

Requirement

The runtime MUST support authorized pause, cancellation, kill, isolation, rollback or compensation, and evidence preservation for active missions, including cascaded subagents and pending tool work.

Purpose

Enables human and automated containment.

Applicability

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

Implementation guidance

- Kill controls must not depend solely on the affected agent.

Required evidence

- Control design
- Drill results
- State reconciliation

Assessment procedure

- **Examine:** Cancel during fan-out and partial execution.
- **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-AGT-21 – Behavioral and operational monitoring

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

Requirement

Agent runtimes MUST monitor policy denials, novel tool sequences, authority use, budget consumption, recursion, delegation, errors, drift, unsafe content, anomalous data access, and outcome quality with actionable escalation.

Purpose

Detects emergent and compromised behavior.

Applicability

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

Implementation guidance

- Baseline by agent and mission type.
- Avoid relying on model self-report.

Required evidence

- Telemetry plan
- Detections
- Incident records

Assessment procedure

- **Examine:** Generate anomalous sequences and confirm alerting.
- **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 — SI-4

NORMATIVE CONTROL

MYTHOS-FND-AGT-22 – Agentic incident response

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

Requirement

The organization MUST maintain incident procedures for compromised agents, poisoned memory or context, malicious tools, provider failure, runaway missions, unauthorized actions, evidence compromise, and cross-tenant exposure.

Purpose

Addresses the distinctive failure modes of agentic systems.

Applicability

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

Implementation guidance

- Support global and scoped revocation.
- Preserve mission state.

Required evidence

- Incident plan
- Exercises
- Corrective actions

Assessment procedure

- **Examine:** Run a memory-poisoning or runaway-agent 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-AGT-23 – Agent, model, tool, and memory retirement

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

Requirement

Retirement MUST revoke identities and capabilities, terminate schedules and missions, migrate or delete governed state and memory, preserve required evidence, update dependents, and verify no residual execution path remains.

Purpose

Prevents orphaned autonomous authority.

Applicability

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

Implementation guidance

- Search for hidden schedules, webhooks, and credentials.

Required evidence

- Retirement plan
- Revocation evidence
- Dependency report

Assessment procedure

- **Examine:** Retire a test agent and attempt delayed execution.
- **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	Inventory, bounded mission, distinct identity, external policy, validated plan, typed tools, scoped execution, governed memory and context, routing, budgets, durable state, approval, evidence, verification, cancellation, monitoring, incident response, and retirement.
Enterprise	Central agent registry, multi-agent runtime, policy-as-code, worker attestation, context compiler, model routing service, skill governance, continuous observability, evidence graph, and enterprise incident operations.
High Assurance	Formally constrained missions, capability-secure execution, microVM or equivalent isolation, independent plan review, two-person approval for high-risk actions, deterministic effect ledger, continuous verification, adversarial agent testing, and cryptographically protected evidence.

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

- Giving agents a general shell or browser because the user asked for autonomy
- Treating a skill file as permission
- Allowing agents to edit their own policy or evidence
- Using one giant conversation as durable state
- Calling retries exactly-once execution
- Accepting multi-agent agreement without tests
- Allowing computer-use agents unrestricted targets
- Persisting every conversation statement as memory

30. Adoption Roadmap from Source Draft

- Define mission, agent, tool, policy, identity, budget, state, and evidence schemas.
- Route all tool use through an authenticated, policy-enforced execution gateway.
- Add durable orchestration, checkpoints, approvals, cancellation, reconciliation, and audit.
- Govern memory, delegation, multi-model routing, skills, and extension access.
- For High Assurance, add independent supervisors, formal policy constraints, isolated execution ranges, adversarial simulation, and continuous verification.

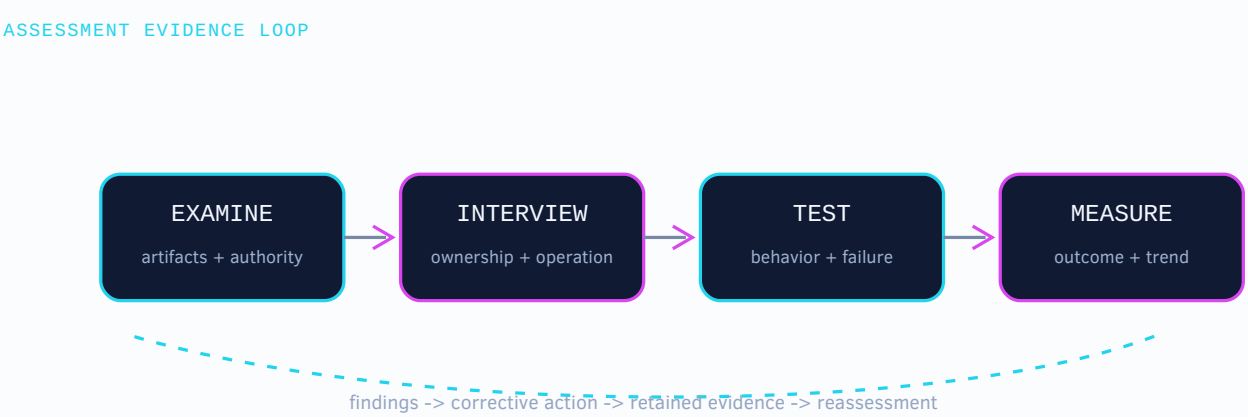
31. Limitations and Residual Risk from Source Draft

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
Attributed action coverage	Consequential actions linked to mission, actor, model, policy, tool, and evidence	100%
	Actions outside granted authority reaching execution	

Metric	Definition	Expected use or target
Unauthorized action rate		0 in defined tests and production
Mission reconciliation	Interrupted missions reconciled to known state	100% of consequential missions
Budget enforcement	Missions exceeding approved cost, time, token, tool, or concurrency budgets without approval	0
Evaluation pass rate	Release-critical agent scenarios meeting deterministic acceptance rules	100% of MUST scenarios

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.

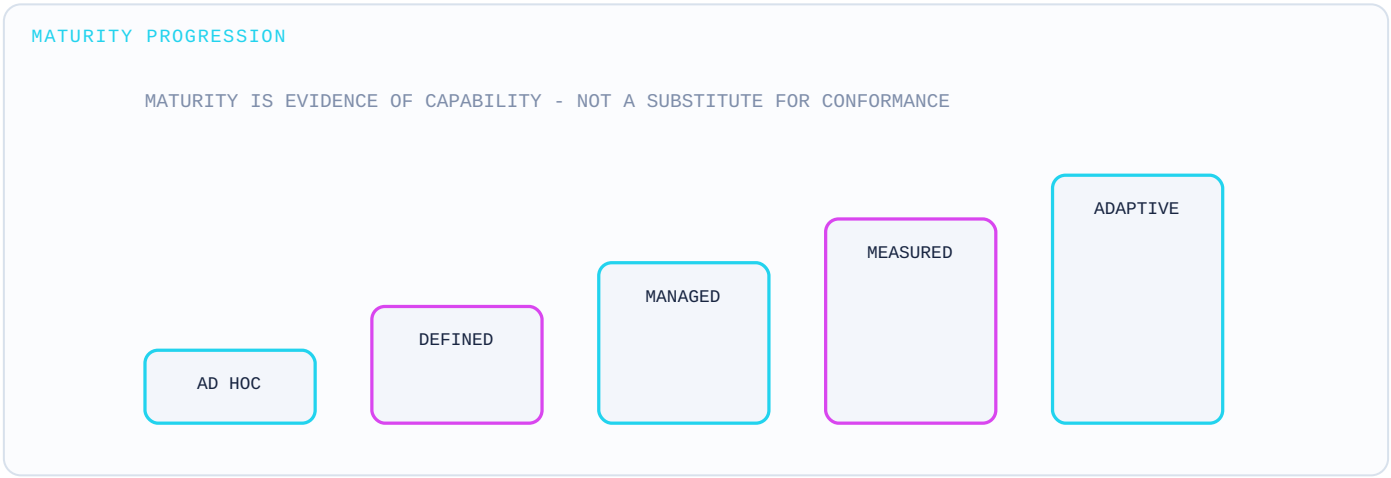
34. Exceptions and Compensating Controls

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
missions without bounded contract	Defined by the adopting organization with owner, source, target, and cadence.
agents without distinct workload identity	Defined by the adopting organization with owner, source, target, and cadence.
tool calls outside declared contract	Defined by the adopting organization with owner, source, target, and cadence.
delegation depth and unresolved lineage	Defined by the adopting organization with owner, source, target, and cadence.
context sources without trust classification	Defined by the adopting organization with owner, source, target, and cadence.
memory proposals accepted without review	Defined by the adopting organization with owner, source, target, and cadence.
model and tool calls beyond budget	Defined by the adopting organization with owner, source, target, and cadence.
indeterminate effects awaiting reconciliation	Defined by the adopting organization with owner, source, target, and cadence.
high-risk actions without independent approval	Defined by the adopting organization with owner, source, target, and cadence.
results lacking independent verification	Defined by the adopting organization with owner, source, target, and cadence.
time to revoke and contain compromised agent	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 AI RMF 1.0	AI risk management	https://www.nist.gov/itl/ai-risk-management-framework	Current; revision program active	2026-09-17
NIST AI 600-1	Generative AI Profile	https://www.nist.gov/publications/artificial-intelligence-risk-management-framework-generative-artificial-intelligence	Final	2026-09-17
NIST SP 800-218A	Secure development for generative AI and dual-use foundation models	https://csrc.nist.gov/pubs/sp/800/218/a/final	Final	2026-09-17
NIST SP 800-207	Zero Trust Architecture	https://csrc.nist.gov/pubs/sp/800/207/final	Final	2026-09-17
ISO/IEC 42001:2023	AI management systems	https://www.iso.org/standard/42001	Published	2026-09-17
ISO/IEC 23894:2023	AI risk management	https://www.iso.org/standard/77304.html	Published	2026-09-17
ISO/IEC 5338:2023	AI system life cycle processes	https://www.iso.org/standard/81118.html	Published	2026-09-17
Regulation (EU) 2024/1689	Artificial Intelligence Act	https://eur-lex.europa.eu/eli/reg/2024/1689/	In force; staged application	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

- Preserves the source draft's model-independent harness, hierarchy, memory, fan-out/fan-in, skills, budgets, and evidence concepts.
- Reframes product-specific names as universal runtime roles and control points.
- Adds explicit identity, delegation lineage, durable-state reconciliation, computer-use, and autonomous-change 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-AGT-01	Governance	Agent and mission inventory	Foundational, Advanced, High Assurance	High	Critical
MYTHOS-FND-AGT-02	Mission	Bounded mission contract	Foundational, Advanced, High Assurance	High	Critical
MYTHOS-FND-AGT-03	Identity	Workload and agent identity	Foundational, Advanced, High Assurance	High	Critical
MYTHOS-FND-AGT-04	Authority	External policy enforcement	Foundational, Advanced, High Assurance	High	Critical
MYTHOS-FND-AGT-05	Delegation	Constrained delegation and lineage	Advanced, High Assurance	High	Critical
MYTHOS-FND-AGT-06	Planning	Plan validation before execution	Foundational, Advanced, High Assurance	Partial	Critical
MYTHOS-FND-AGT-07	Tools	Tool contract and safety classification	Foundational, Advanced, High Assurance	High	Critical
MYTHOS-FND-AGT-08	Execution	Sandboxed and scoped execution	Advanced, High Assurance	High	Critical
MYTHOS-FND-AGT-09	Computer use	Visual and computer-use action control	Advanced, High Assurance	Partial	Critical
MYTHOS-FND-AGT-10	Memory	Governed memory lifecycle	Foundational, Advanced, High Assurance	Partial	Critical
	Context			Partial	Critical

Control	Family	Title	Profiles	Automation	Impact
MYTHOS-FND-AGT-11		Context assembly and trust boundaries	Foundational, Advanced, High Assurance		
MYTHOS-FND-AGT-12	Models	Model routing policy	Advanced, High Assurance	High	Critical
MYTHOS-FND-AGT-13	Budgets	Resource and recursion budgets	Foundational, Advanced, High Assurance	High	Critical
MYTHOS-FND-AGT-14	Durability	Durable state and exactly-once effect strategy	Advanced, High Assurance	High	Critical
MYTHOS-FND-AGT-15	Parallelism	Fan-out, fan-in, and conflict control	Advanced, High Assurance	Partial	Critical
MYTHOS-FND-AGT-16	Approvals	Independent approval and separation of duties	Foundational, Advanced, High Assurance	High	Critical
MYTHOS-FND-AGT-17	Skills	Governed skill creation and modification	Advanced, High Assurance	Partial	Critical
MYTHOS-FND-AGT-18	Evidence	End-to-end execution evidence	Advanced, High Assurance	High	Critical
MYTHOS-FND-AGT-19	Verification	Independent result verification	Foundational, Advanced, High Assurance	Partial	Critical
MYTHOS-FND-AGT-20	Interruptibility	Pause, cancel, rollback, and containment	Advanced, High Assurance	High	Critical
MYTHOS-FND-AGT-21	Monitoring	Behavioral and operational monitoring	Advanced, High Assurance	Partial	Critical
MYTHOS-FND-AGT-22	Incident	Agentic incident response	Advanced, High Assurance	Partial	Critical
MYTHOS-FND-AGT-23	Lifecycle	Agent, model, tool, and memory retirement	Advanced, High Assurance	High	Critical

Appendix D – Minimum Conformance Claim Record

```
standard: MYTHOS-FND-0010
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