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

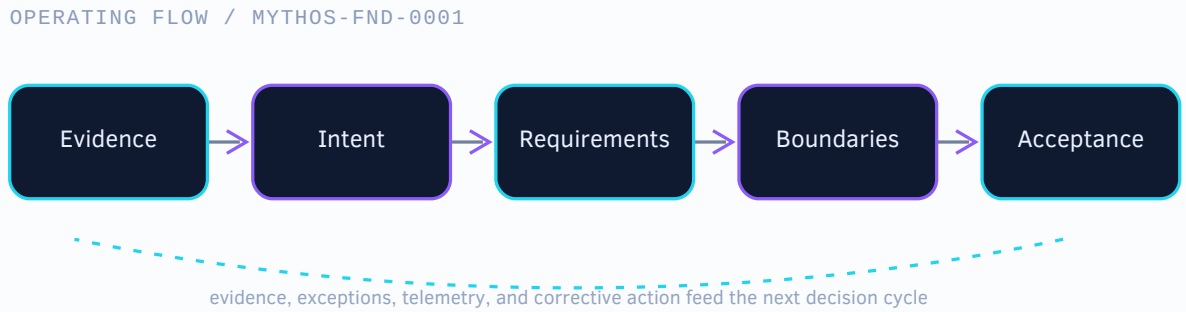
- Create a stable chain from validated problem evidence to released product outcomes.
- Prevent premature implementation, unbounded scope, hidden assumptions, and architecture-by-accident.
- Make product decisions reviewable, reversible where practical, and traceable to evidence.
- Integrate security, 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.

NORMATIVE SYSTEM

Control index

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

Document Control

Field	Value
Document ID	MYTHOS-FND-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.

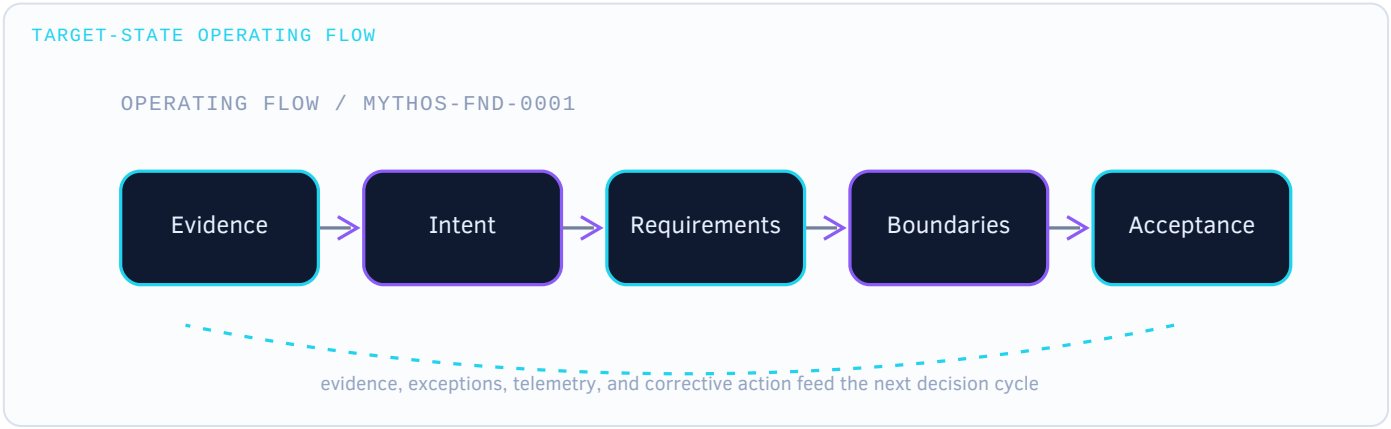
3.3 Security, Privacy, and Trust Impact

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

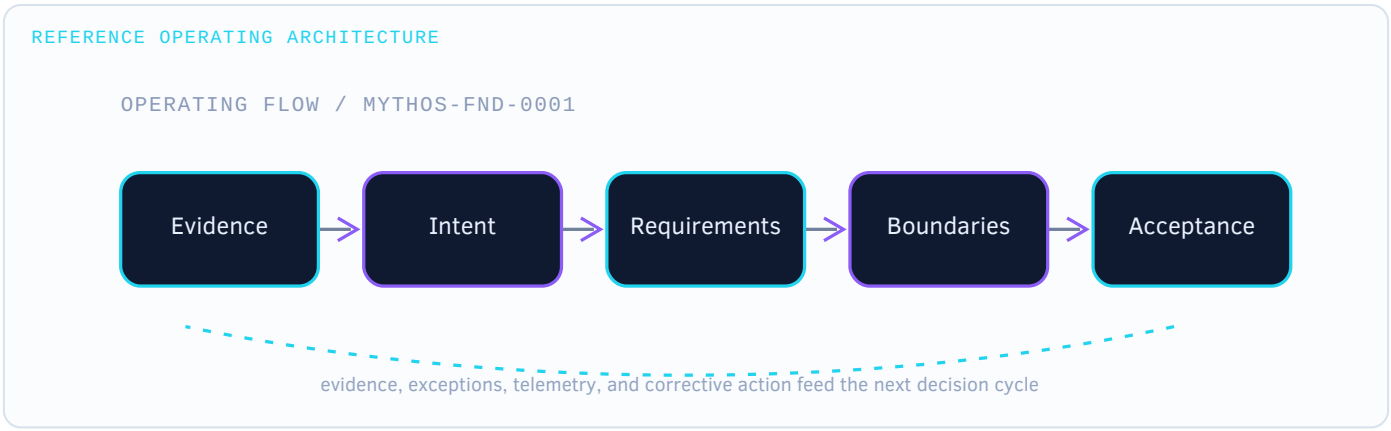
The principal enterprise risks addressed by this standard include inconsistent ownership, undocumented authority, uncontrolled change, local optimization, evidence gaps, stale assumptions, supplier dependence, false assurance, and the inability to determine whether the operating system still matches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

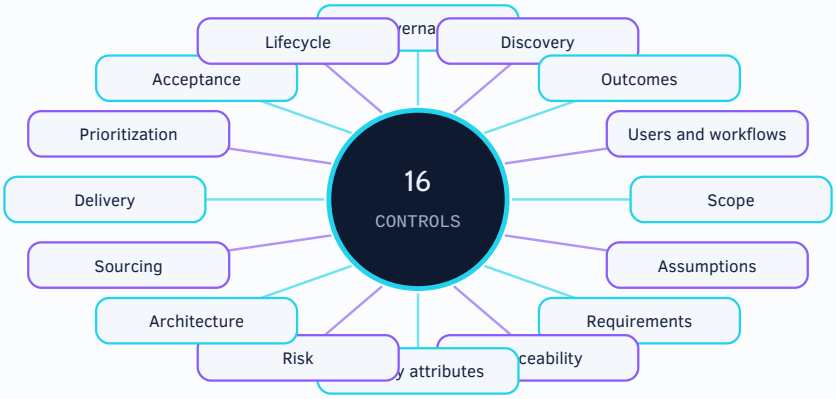
This Foundation standard depends on the remaining MYTHOS-FND standards for documentation, security and trust, quality, operations, data and integration, interfaces, extensions, AI-first behavior, and agentic orchestration. An adopting organization MUST resolve overlapping requirements through the stricter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

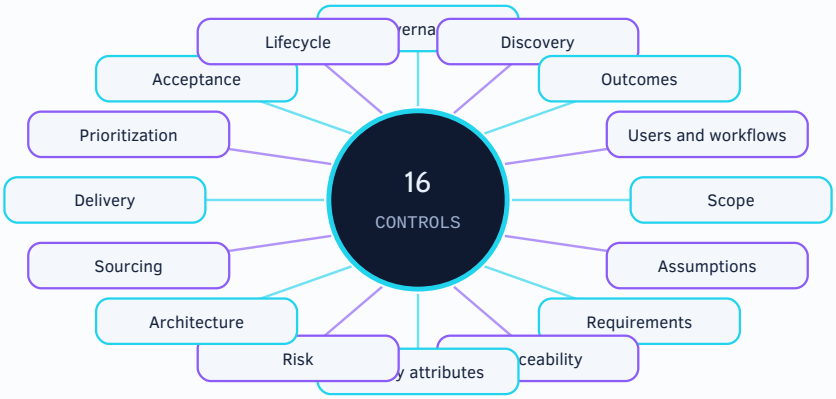
- Governance
- Discovery
- Outcomes
- Users and workflows
- Scope
- Assumptions
- Requirements
- Traceability
- Quality attributes
- Risk
- Architecture
- Sourcing
- Delivery
- Prioritization
- Acceptance
- Lifecycle

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.

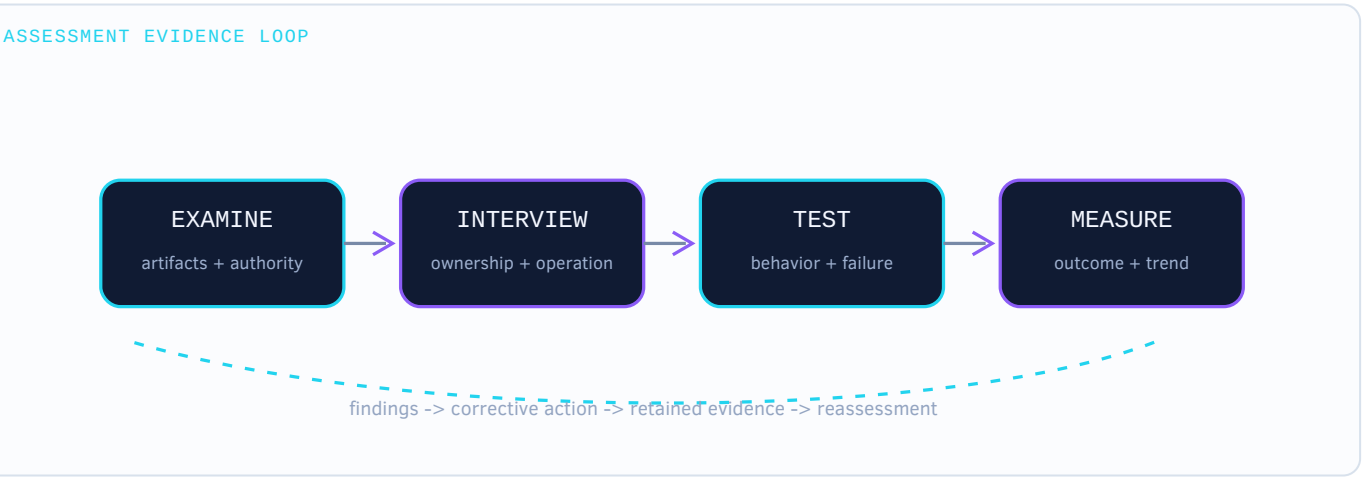
31. Limitations and Residual Risk from Source Draft

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.

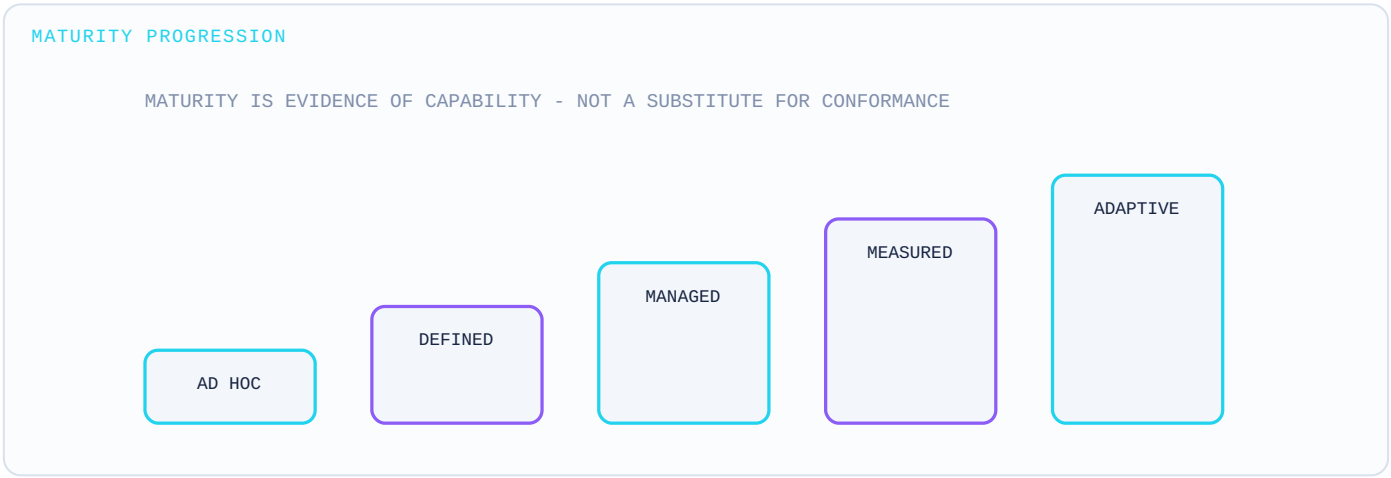
34. Exceptions and Compensating Controls

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