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

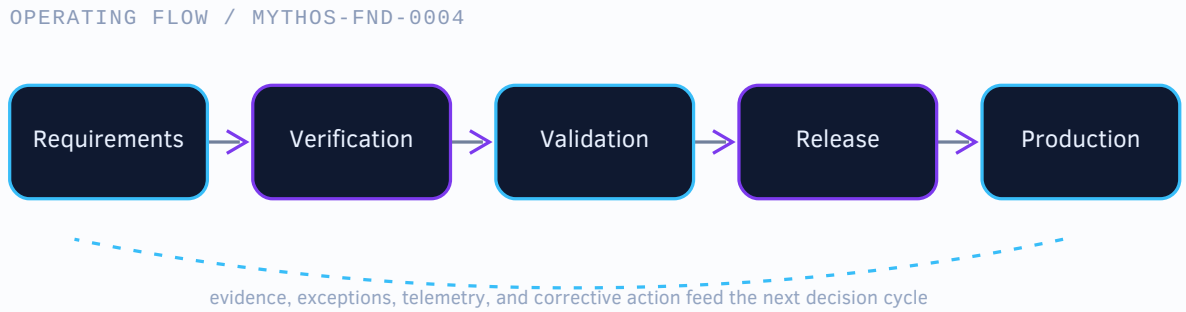
- Establish measurable quality models and risk-based validation depth.
- Create reproducible evidence across static, dynamic, operational, human, security, and AI evaluation methods.
- Prevent test quantity, code coverage, or pipeline success from substituting for meaningful assurance.
- Continuously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

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-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.

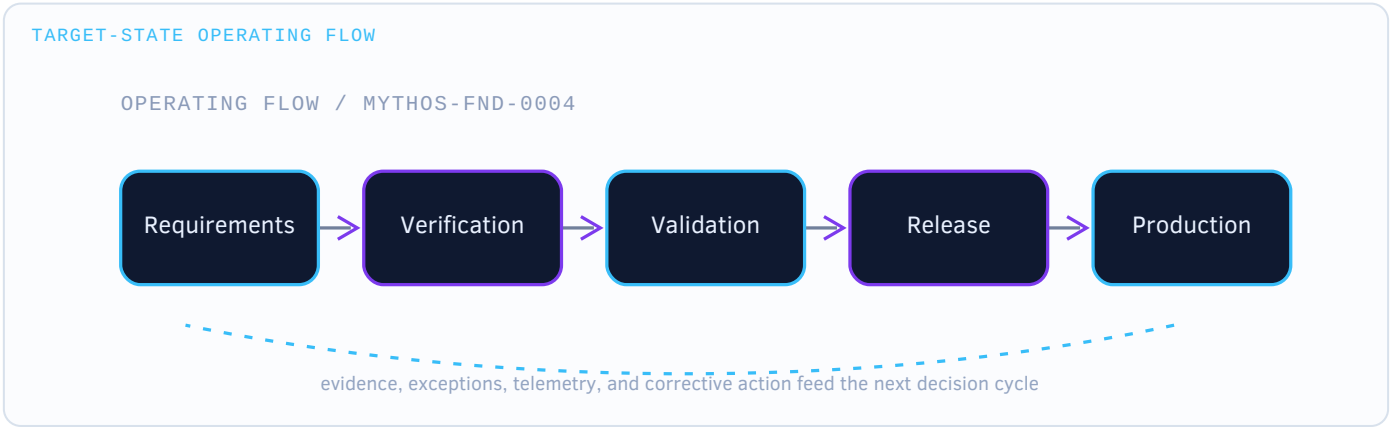
3.3 Security, Privacy, and Trust Impact

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.

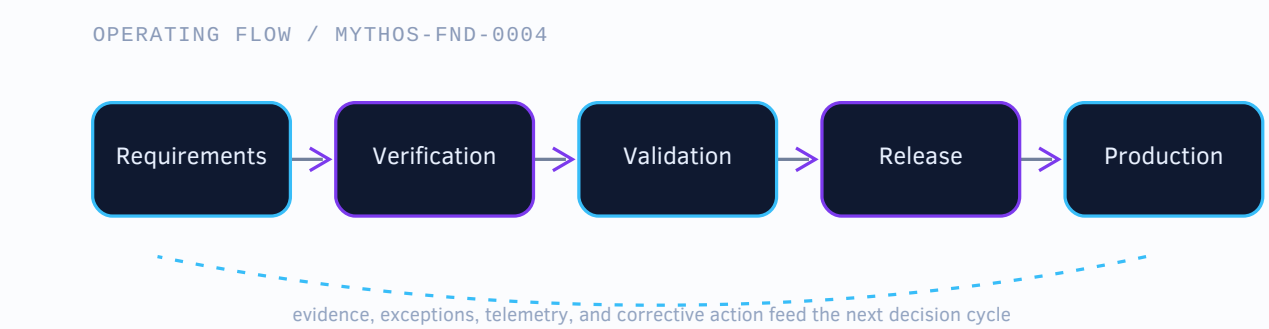
Adopting organizations SHOULD maintain a domain-specific risk register that identifies cause, affected asset or stakeholder, credible scenario, impact, existing controls, residual risk, owner, review trigger, and evidence. Risks that cross standards MUST be linked rather than copied into disconnected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

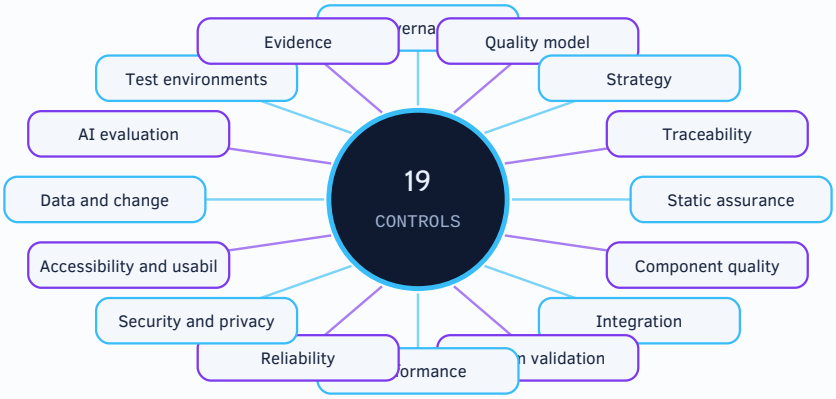
This Foundation standard depends on the remaining MYTHOS-FND standards for documentation, security and trust, quality, operations, data and integration, interfaces, extensions, AI-first behavior, and agentic orchestration. An adopting organization MUST resolve overlapping requirements through the stricter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

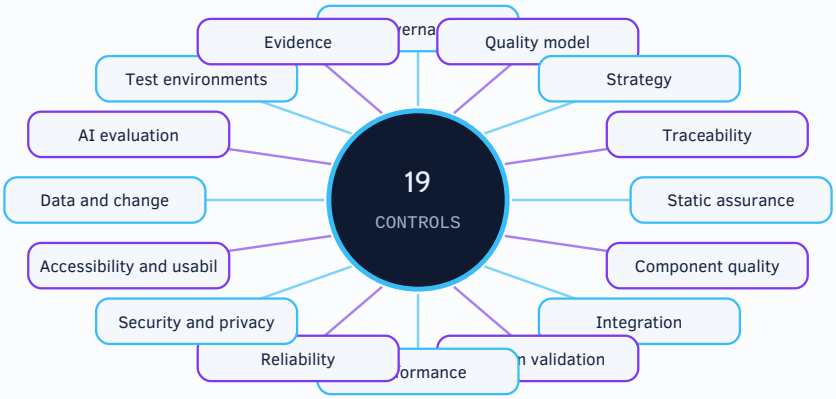
- Production validation

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.

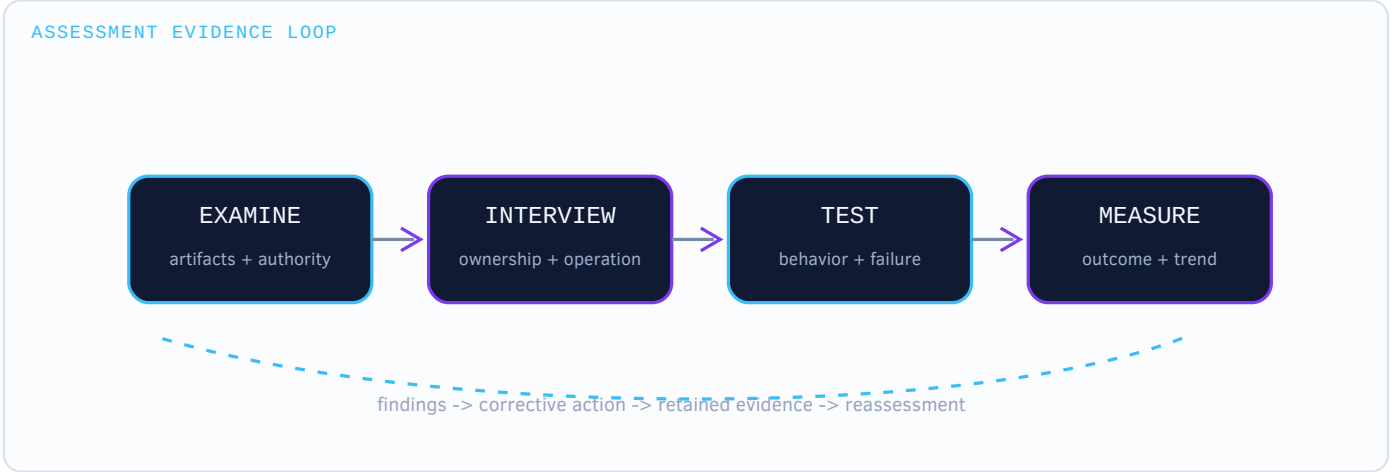
31. Limitations and Residual Risk from Source Draft

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.

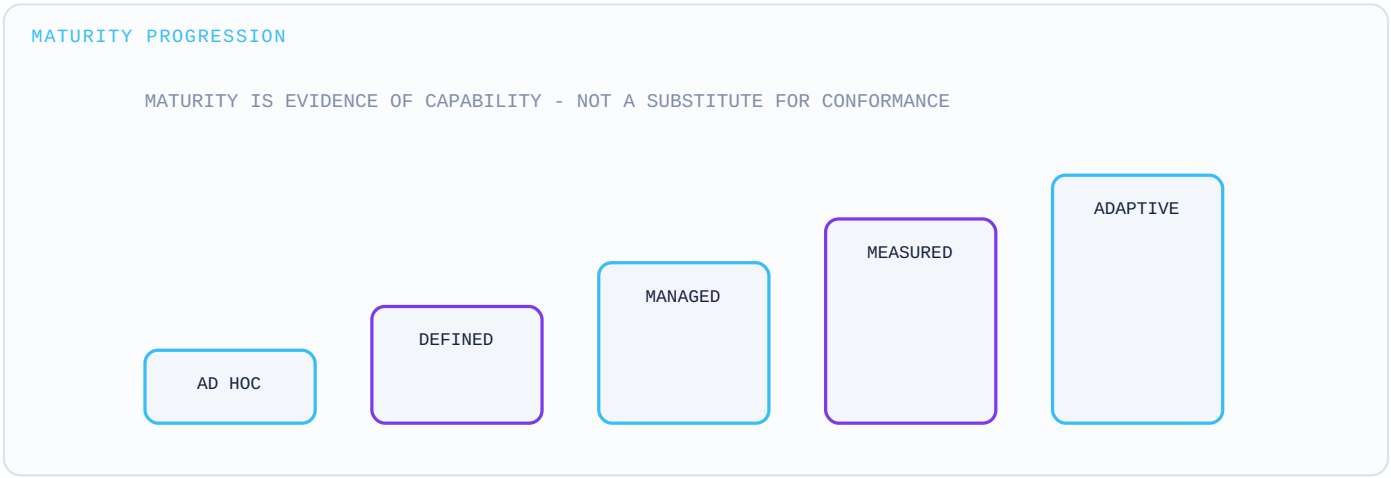
34. Exceptions and Compensating Controls

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