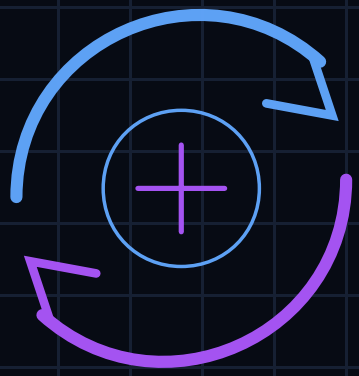


CANDIDATE STANDARD

# Mythos Operations, Release, and Lifecycle Standard

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

PERMANENT ID
MYTHOS-FND-0005

PUBLICATION CLASS
CANDIDATE STANDARD

VERSION / STATUS
1.0.0-candidate / CANDIDATE

PERMANENT PUBLICATION IDENTITY

# Mythos Operations, Release, and Lifecycle Standard

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

Document ID
MYTHOS-FND-0005

Version
1.0.0-candidate

Status
Candidate Standard

Review date
2027-09-17

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

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

## Reader orientation

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

## Expected outcomes

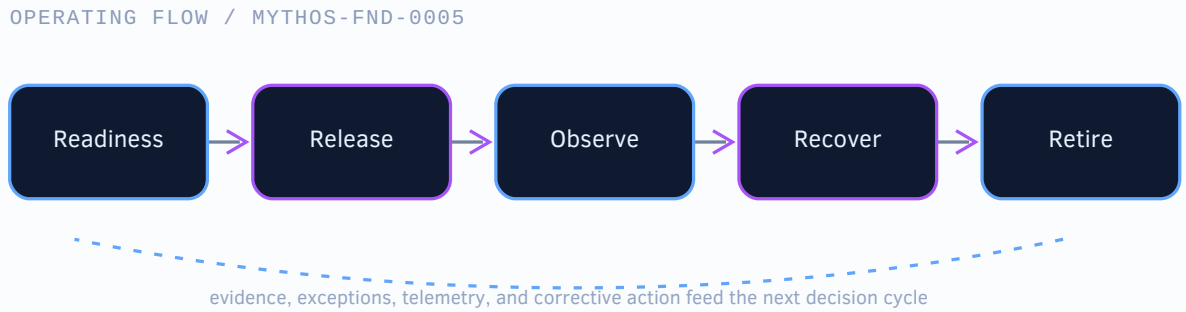
- Ensure every production capability has ownership, objectives, observable health, and operational procedures.
- Make changes controlled, progressive, reversible, and supported by immutable release evidence.
- Reduce incident impact through preparation, rapid containment, reliable recovery, and systemic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

SOURCE / FRESHNESS POSITION

# Authority and source posture

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

FOUNDATION OPERATING DOCTRINE




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

NAVIGATION

# Contents

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

**Document Control** 8

Revision Record 8

**How to Use This Standard** 9

Executive Reading Path 9

Engineering Reading Path 9

Assessment Reading Path 9

Normative and Informative Content 9

**Part I – Executive Direction** 10

1. Executive Overview 10

2. Executive Findings and Required Direction 10

3. Business and Operational Impact 10

4. Target-State Summary 11

5. Leadership Responsibilities 12

**Part II – Standard Foundation** 13

6. Purpose and Objectives 13

7. Scope 13

8. Intended Audience 13

9. Requirements Language and Conformance 13

10. Normative References from Source Draft 13

11. Informative References from Source Draft 14

12. Terms and Definitions 14

13. Applicability and Tailoring 15

**Part III – Risk and Architecture** 16

14. Enterprise Problem and Risk Landscape 16

15. Governing Principles 16

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

**Part IV – Normative Control System 19**

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

**Part V – Implementation and Operations 40**

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

**Part VI – Assurance and Assessment 43**

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

**Part VII – Authority and Traceability 47**

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

41. Control Traceability 47

42. Source-Draft Preservation 48

**Part VIII – Appendices** **49**

Appendix A — Source-Draft Evolution Notes 49

Appendix B — Change History 49

Appendix C — Control Summary 49

Appendix D — Minimum Conformance Claim Record 50

Appendix E — Publication Review Checklist 50

NORMATIVE SYSTEM

# Control index

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


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

# Document Control

| Field | Value |
|---|---|
| Document ID | MYTHOS-FND-0005 |
| Standard | Operations, Release, and Lifecycle |
| Version | 1.0.0-candidate |
| Status | Candidate Standard |
| Classification | Public |
| Publisher | Mythos Systems |
| Program | Mythos Engineering Standards Program |
| Accountable Owner | Mythos Systems Standards Program |
| Technical Review | Required |
| Source and Citation Review | Required |
| Assessment Review | Required |
| Accessibility and Publication Review | Required |
| Supersedes | No published edition; evolves source draft 0.2.0 |
| Next Review | 2027-09-17 or earlier on trigger |

## Revision Record

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

# How to Use This Standard

## Executive Reading Path

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

## Engineering Reading Path

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

## Assessment Reading Path

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

## Normative and Informative Content

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

FOUNDATION STANDARD / STRUCTURAL PART

# Part I – Executive Direction

## 1. Executive Overview

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

The institutional objective is to govern service ownership, observability, change, release, deployment, recovery, incident response, capacity, maintenance, deprecation, and retirement across the operating lifecycle. Adoption should produce a controlled operating state in which leadership can understand the material risks, engineering teams can act on explicit requirements, assessors can test implementation and operating effectiveness, and the organization can support every conformance or trust claim with current evidence.

## 2. Executive Findings and Required Direction

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

## 3. Business and Operational Impact

### 3.1 Strategic Impact

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

### 3.2 Delivery and Cost Impact

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

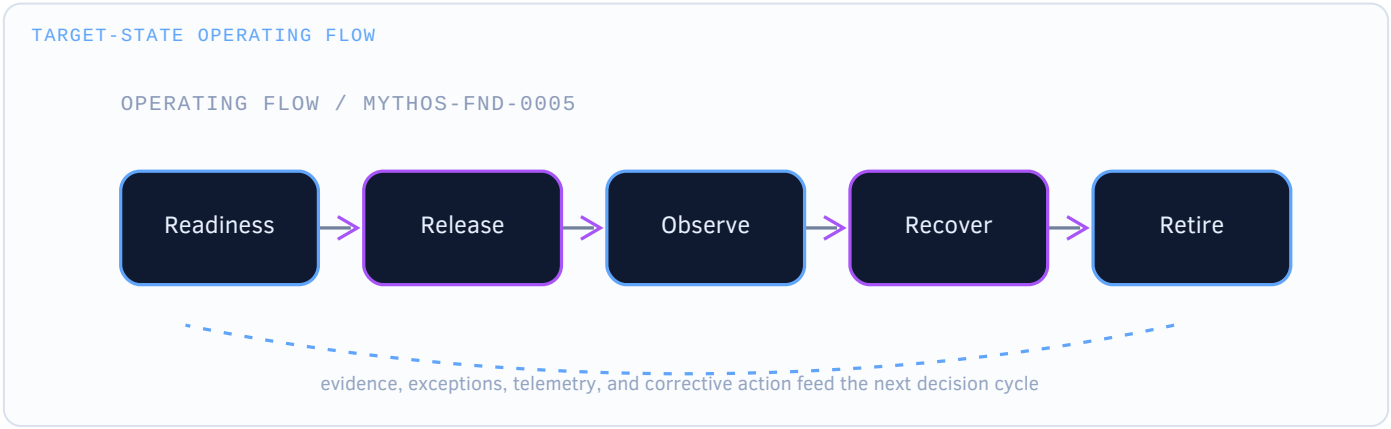
### 3.3 Security, Privacy, and Trust Impact

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

### 3.4 Workforce and Organizational Impact

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

## 4. Target-State Summary




The target state contains the following institutional components:

| # | Target-State Component |
|---|---|
| 1 | Service catalog and ownership |
| 2 | SLIs, SLOs, and error budgets |
| 3 | Operational telemetry and state model |
| 4 | Operational readiness review |
| 5 | Change and release governance |
| 6 | Progressive deployment and canary |
| 7 | Configuration and desired-state authority |
| 8 | Rollback and forward recovery |
| 9 | Runbooks and operational automation |
| 10 | Incident command and communication |
| 11 | Problem management and learning |
| 12 | Capacity and performance |
| 13 | Backup, restore, and continuity |
| 14 | Patch and dependency lifecycle |

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

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

## 5. Leadership Responsibilities

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

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

FOUNDATION STANDARD / STRUCTURAL PART

# Part II – Standard Foundation

## 6. Purpose and Objectives

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

## 7. Scope

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

## 8. Intended Audience

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

## 9. Requirements Language and Conformance

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

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

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

## 10. Normative References from Source Draft

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

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

## 11. Informative References from Source Draft

- **ISO/IEC/IEEE 15288:2023** — Systems and software engineering — System life cycle processes. https://www.iso.org/standard/81702.html
- **NIST CSWP 29** — The NIST Cybersecurity Framework (CSF) 2.0. https://doi.org/10.6028/NIST.CSWP.29
- **NIST SP 800-53 Rev. 5, Release 5.2.0** — Security and Privacy Controls for Information Systems and Organizations. https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final
- **NIST SP 800-61 Rev. 3** — Incident Response Recommendations and Considerations for Cybersecurity Risk Management. https://csrc.nist.gov/pubs/sp/800/61/r3/final
- **CISA CPG 2.0** — Cross-Sector Cybersecurity Performance Goals 2.0. https://www.cisa.gov/cybersecurity-performance-goals-2-0-cpg-2-0
- **CIS Controls v8.1** — CIS Critical Security Controls. https://www.cisecurity.org/controls/v8-1
- **NIST SP 800-218 v1.1** — Secure Software Development Framework (SSDF). https://csrc.nist.gov/pubs/sp/800/218/final

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

## 12. Terms and Definitions

| Term | Definition |
|---|---|
| Accountable owner | The person or formally delegated role that accepts responsibility for an outcome, decision, control, or risk. |
| Assessment object | The system, process, component, artifact, team, service, or organizational scope being evaluated. |
| Compensating control | An alternative safeguard that provides comparable risk reduction when the specified control cannot be implemented as written. |
| Conformance claim | A bounded statement that an identified scope satisfies the applicable requirements of a named standard version and assurance profile. |
| Evidence | Reviewable information that supports a conclusion about design, implementation, operation, or control effectiveness. |
| High Assurance | The cumulative profile requiring stronger independence, adversarial testing, continuous verification, or formal evidence where risk warrants it. |
| Residual risk | Risk remaining after controls, mitigations, and compensating measures are applied. |
| System | A product, service, application, platform, workflow, integration, operational capability, or combined socio-technical environment. |
| Tailoring | A documented decision to include, strengthen, parameterize, or mark a control not applicable based on scope and risk. |
| Service objective | A measurable target for user- or mission-relevant service behavior over a defined interval. |
| Error budget | The tolerated amount of objective nonconformance used to govern risk and change velocity. |
| Progressive delivery | Controlled exposure of a change to increasing scope while observing defined guardrails. |
| Operational readiness | Evidence that a capability can be deployed, observed, supported, secured, recovered, and retired safely. |
| Retirement | The controlled removal of a capability, dependency, interface, data set, credential, and supporting obligation. |

## 13. Applicability and Tailoring

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

FOUNDATION STANDARD / STRUCTURAL PART

# Part III – Risk and Architecture

## 14. Enterprise Problem and Risk Landscape

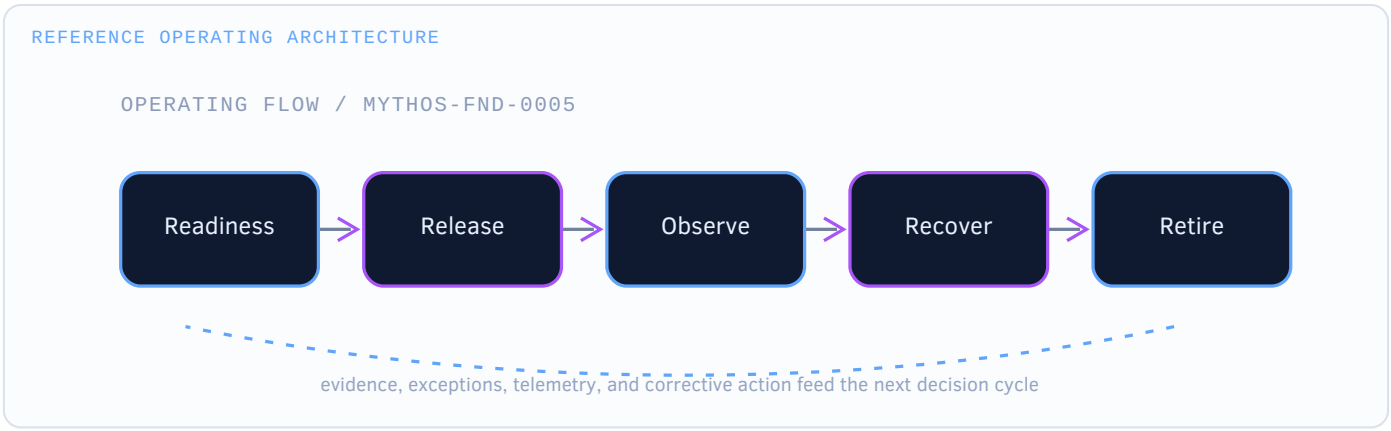
The principal enterprise risks addressed by this standard include inconsistent ownership, undocumented authority, uncontrolled change, local optimization, evidence gaps, stale assumptions, supplier dependence, false assurance, and the inability to determine whether the operating system still matches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

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

## 15. Governing Principles

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

## 16. Reference Operating Architecture



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

### 16.1 Control Plane

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

### 16.2 Delivery and Enforcement Plane

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

### 16.3 Evidence and Assurance Plane

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

### 16.4 Feedback Plane

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

## 17. Roles and Accountability

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

## 18. State, Evidence, and Decision Model

The adopting organization MUST distinguish:

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

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

## 19. Security and Trust Considerations

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

## 20. Failure Modes

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

## 21. Cross-Functional Dependencies

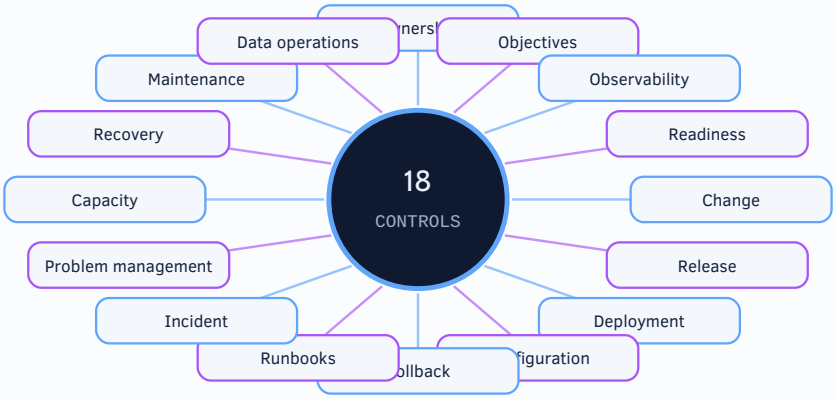
This Foundation standard depends on the remaining MYTHOS-FND standards for documentation, security and trust, quality, operations, data and integration, interfaces, extensions, AI-first behavior, and agentic orchestration. An adopting organization MUST resolve overlapping requirements through the stricter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

FOUNDATION STANDARD / STRUCTURAL PART

# Part IV – Normative Control System

## 22. Control-Family Overview

CONTROL-FAMILY CONSTELLATION




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

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

# 23. Normative Controls

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

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

NORMATIVE CONTROL CONSTELLATION

NORMATIVE CONTROL

# MYTHOS-FND-ORL-01 – Service ownership and catalog

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

## Requirement

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

### Purpose

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

### Applicability

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

### Implementation guidance

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

### Required evidence

- Service catalog
- Ownership attestations
- Escalation records

### Assessment procedure

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

### Exceptions and compensating controls

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

### External mappings

- NIST CSF 2.0 — GV.RR and ID.AM

NORMATIVE CONTROL

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

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

## Requirement

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

## Purpose

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

## Applicability

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

## Implementation guidance

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

## Required evidence

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

## Assessment procedure

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

## Exceptions and compensating controls

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

## External mappings

- NIST CSF 2.0 — ID.IM and PR.IR

NORMATIVE CONTROL

# MYTHOS-FND-ORL-03 – Observable operational state

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

## Requirement

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

## Purpose

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

## Applicability

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

## Implementation guidance

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

## Required evidence

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

## Assessment procedure

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

## Exceptions and compensating controls

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

## External mappings

- NIST SP 800-53 — AU, SI-4
- CISA CPG 2.0 — logging

NORMATIVE CONTROL

# MYTHOS-FND-ORL-04 – Operational readiness review

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

## Requirement

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

## Purpose

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

## Applicability

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

## Implementation guidance

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

## Required evidence

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

## Assessment procedure

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

## Exceptions and compensating controls

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

## External mappings

- ISO/IEC/IEEE 15288:2023 — transition and operation

NORMATIVE CONTROL

# MYTHOS-FND-ORL-05 – Controlled change management

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

## Requirement

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

## Purpose

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

## Applicability

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

## Implementation guidance

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

## Required evidence

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

## Assessment procedure

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

## Exceptions and compensating controls

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

## External mappings

- NIST SP 800-53 — CM-3
- NIST CSF 2.0 — PR.PS

NORMATIVE CONTROL

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

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

## Requirement

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

## Purpose

Prevents version ambiguity and promotion without reviewable evidence.

## Applicability

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

## Implementation guidance

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

## Required evidence

- Release manifest
- Gate results
- Approval and artifact identity

## Assessment procedure

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

## Exceptions and compensating controls

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

## External mappings

- NIST SSDF v1.1 — PS.2 and PW.9

NORMATIVE CONTROL

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

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

## Requirement

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

## Purpose

Limits blast radius and creates early production evidence.

## Applicability

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

## Implementation guidance

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

## Required evidence

- Deployment strategy
- Exposure and guardrail records
- Promotion history

## Assessment procedure

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

## Exceptions and compensating controls

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

## External mappings

- NIST SP 800-53 — SI-2 and CM-3

NORMATIVE CONTROL

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

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

## Requirement

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

### Purpose

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

### Applicability

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

### Implementation guidance

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

### Required evidence

- Configuration inventory
- Drift reports
- Override and recovery records

### Assessment procedure

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

### Exceptions and compensating controls

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

### External mappings

- NIST SP 800-53 — CM family

NORMATIVE CONTROL

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

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

## Requirement

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

## Purpose

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

## Applicability

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

## Implementation guidance

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

## Required evidence

- Rollback plan
- Exercise results
- Irreversibility assessment

## Assessment procedure

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

## Exceptions and compensating controls

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

## External mappings

- NIST CSF 2.0 — RC.RP

NORMATIVE CONTROL

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

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

## Requirement

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

### Purpose

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

### Applicability

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

### Implementation guidance

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

### Required evidence

- Runbooks or automation definitions
- Exercise logs
- Change history

### Assessment procedure

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

### Exceptions and compensating controls

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

### External mappings

- NIST SP 800-61 Rev. 3

NORMATIVE CONTROL

# MYTHOS-FND-ORL-11 – Incident command, containment, and communication

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

## Requirement

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

### Purpose

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

### Applicability

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

### Implementation guidance

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

### Required evidence

- Incident plan
- Exercise and incident timelines
- Communication records

### Assessment procedure

- **Examine:** Run a cross-functional exercise.
- **Interview:** Review a sampled incident for role clarity and evidence.
- **Test:** Test after-hours escalation.

### Exceptions and compensating controls

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

### External mappings

- NIST SP 800-61 Rev. 3
- NIST CSF 2.0 — Respond

NORMATIVE CONTROL

# MYTHOS-FND-ORL-12 – Systemic problem management and learning

| FAMILY | PROFILES | FAILURE IMPACT | AUTOMATION POTENTIAL |
|---|---|---|---|
| Problem management | Foundational, Advanced, High Assurance | Material | Partial |

## Requirement

Significant incidents, recurring defects, near misses, and objective breaches MUST receive causal analysis that identifies contributing system conditions and produces owned, prioritized, verifiable corrective actions.

### Purpose

Prevents recurrence and avoids reducing complex failures to individual error.

### Applicability

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

### Implementation guidance

- Separate trigger from systemic contributors.
- Examine design, process, incentives, capacity, telemetry, dependencies, and documentation.
- Validate that corrective actions reduce the identified risk.

### Required evidence

- Post-incident review
- Corrective action register
- Effectiveness evidence

### Assessment procedure

- **Examine:** Trace corrective actions to closure.
- **Interview:** Look for repeated causal patterns.
- **Test:** Verify lessons changed tests, controls, or architecture.

### Exceptions and compensating controls

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

### External mappings

- NIST CSF 2.0 — ID.IM

NORMATIVE CONTROL

# MYTHOS-FND-ORL-13 – Capacity, performance, and demand management

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

## Requirement

Critical services MUST forecast and monitor demand, saturation, quotas, dependency limits, cost, and failure thresholds and maintain tested responses for overload and abnormal demand.

### Purpose

Prevents predictable exhaustion and unsafe scaling behavior.

### Applicability

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

### Implementation guidance

- Define headroom by lead time and consequence.
- Include human, network, storage, queue, rate, model, and supplier capacity.
- Use admission control, prioritization, and graceful degradation.

### Required evidence

- Capacity model
- Forecast and saturation dashboard
- Load-shedding tests

### Assessment procedure

- **Examine:** Compare forecast to actual demand.
- **Interview:** Drive a test environment to saturation.
- **Test:** Verify critical traffic remains prioritized.

### Exceptions and compensating controls

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

### External mappings

- ISO/IEC 25010:2023 — performance efficiency

NORMATIVE CONTROL

# MYTHOS-FND-ORL-14 – Backup, restore, and continuity

| FAMILY | PROFILES | FAILURE IMPACT | AUTOMATION POTENTIAL |
|---|---|---|---|
| Recovery | Foundational, Advanced, High Assurance | Critical | Partial |

## Requirement

Critical data and services MUST have documented and exercised backup, restoration, continuity, and disaster-recovery controls that meet approved recovery objectives and verify confidentiality, authorization, integrity, and completeness after recovery.

## Purpose

Ensures recoverability rather than backup-job completion.

## Applicability

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

## Implementation guidance

- Protect backups from common compromise.
- Test regional, supplier, identity, key, and control-plane loss as applicable.
- Record gaps between objectives and observed results.

## Required evidence

- Backup inventory
- Restore and continuity exercises
- Recovery validation

## Assessment procedure

- **Examine:** Restore sampled data and services.
- **Interview:** Test recovery without a key dependency.
- **Test:** Review recovery objective exceptions.

## Exceptions and compensating controls

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

## External mappings

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

NORMATIVE CONTROL

# MYTHOS-FND-ORL-15 – Vulnerability, patch, and dependency lifecycle

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

## Requirement

The organization MUST monitor, prioritize, test, deploy, verify, and, when necessary, roll back security patches, defect fixes, certificates, firmware, models, dependencies, and supplier changes according to risk and support status.

## Purpose

Reduces exposure while controlling update-induced failure.

## Applicability

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

## Implementation guidance

- Maintain supported-version inventory and end-of-life dates.
- Use emergency pathways for active exploitation.
- Test updates against critical workflows and compatibility.
- Plan replacement before support expiry.

## Required evidence

- Lifecycle inventory
- Patch and update records
- Verification and exception records

## Assessment procedure

- **Examine:** Sample aged dependencies and critical updates.
- **Interview:** Verify deployment and remediation.
- **Test:** Review end-of-life exposure.

## Exceptions and compensating controls

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

## External mappings

- NIST SP 800-53 Release 5.2.0 — SI-2
- CISA CPG 2.0

NORMATIVE CONTROL

# MYTHOS-FND-ORL-16 – Operational data integrity and maintenance

| FAMILY | PROFILES | FAILURE IMPACT | AUTOMATION POTENTIAL |
|---|---|---|---|
| Data operations | Foundational, Advanced, High Assurance | Critical | High |

## Requirement

Operational data jobs, retention processes, reconciliation, reindexing, compaction, replication, archival, and deletion MUST be observable, recoverable, authorization-controlled, and validated for correctness and privacy impact.

### Purpose

Prevents maintenance operations from silently corrupting or over-retaining data.

### Applicability

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

### Implementation guidance

- Use checkpoints and idempotency for long-running jobs.
- Reconcile totals and invariants.
- Separate operator authority from application authority for high-impact actions.

### Required evidence

- Job definitions
- Reconciliation reports
- Authorization and recovery tests

### Assessment procedure

- **Examine:** Interrupt and resume a maintenance job.
- **Interview:** Verify duplicate execution is safe.
- **Test:** Review deletion and archival outcomes.

### Exceptions and compensating controls

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

### External mappings

- NIST SP 800-53 — SI-7, SI-12

NORMATIVE CONTROL

# MYTHOS-FND-ORL-17 – Operational access and emergency controls

| FAMILY | PROFILES | FAILURE IMPACT | AUTOMATION POTENTIAL |
|---|---|---|---|
| Security operations | Foundational, Advanced, High Assurance | Critical | High |

## Requirement

Operational and support access MUST use distinct identities, least privilege, approved channels, time-bounded elevation, complete audit, and post-use review for high-impact or break-glass activity.

## Purpose

Constrains powerful operational authority and supports accountability.

## Applicability

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

## Implementation guidance

- Disallow shared administrative credentials.
- Broker sessions and record commands or actions where justified.
- Test emergency access without weakening ordinary controls.

## Required evidence

- Privileged access policy
- Elevation and session records
- Break-glass exercise

## Assessment procedure

- **Examine:** Review sampled privileged sessions.
- **Interview:** Attempt expired elevation.
- **Test:** Verify break-glass use triggers review.

## Exceptions and compensating controls

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

## External mappings

- NIST SP 800-53 — AC-2, AC-6, AU-12

NORMATIVE CONTROL

# MYTHOS-FND-ORL-18 – Controlled deprecation and retirement

| FAMILY | PROFILES | FAILURE IMPACT | AUTOMATION POTENTIAL |
|---|---|---|---|
| Retirement | Foundational, Advanced, High Assurance | Critical | Partial |

## Requirement

Services, interfaces, data stores, models, extensions, credentials, infrastructure, and operational obligations MUST be retired through a controlled plan that addresses consumers, migration, communication, data disposition, access revocation, dependency removal, evidence retention, and post-retirement verification.

## Purpose

Prevents abandoned systems, orphan data, lingering credentials, and hidden dependencies.

## Applicability

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

## Implementation guidance

- Define deprecation windows and compatibility support.
- Discover consumers rather than relying only on registration.
- Remove monitoring and cost only after verifying absence of required use.

## Required evidence

- Retirement plan
- Consumer and migration records
- Post-retirement verification

## Assessment procedure

- **Examine:** Search for remaining traffic, credentials, data, and dependencies.
- **Interview:** Verify user communication and migration.
- **Test:** Review rollback or contingency for failed retirement.

## Exceptions and compensating controls

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

## External mappings

- ISO/IEC/IEEE 15288:2023 — disposal

FOUNDATION STANDARD / STRUCTURAL PART

# Part V – Implementation and Operations

## 24. Implementation Profiles

| Profile | Required Operating State |
|---|---|
| Baseline | Service owner, catalog, SLIs/SLOs, telemetry, readiness review, controlled release, rollback, runbooks, incident response, backups, patching, and retirement. |
| Enterprise | Central service management, progressive delivery, automated evidence, error budgets, configuration reconciliation, capacity forecasting, problem analytics, and regular recovery exercises. |
| High Assurance | Independent release authorization, multi-region or equivalent resilience, continuous verification, immutable evidence, strict change windows, proven failover, cryptographic artifact admission, and supervised emergency authority. |

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

## 25. Implementation Lifecycle

### 25.1 Establish

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

### 25.2 Baseline

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

### 25.3 Implement

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

### 25.4 Assure

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

### 25.5 Operate and Improve

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

## 26. Integration Requirements

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

## 27. Failure Handling and Recovery

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

## 28. Exceptions and Compensating Controls

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

## 29. Prohibited Practices

- Declaring success when deployment completes without post-checks
- Using dashboards without defined service objectives
- Treating backup completion as proof of recovery
- Allowing emergency access to become permanent
- Running high-risk changes without verified rollback
- Retiring services without data, identity, dependency, and customer migration

## 30. Adoption Roadmap from Source Draft

- Create service ownership, catalog, criticality, objectives, telemetry, and operational-readiness criteria.

- Standardize change, release, deployment, rollback, configuration, and runbook controls.
- Implement incident, problem, vulnerability, capacity, backup, recovery, and continuity practices.
- Add progressive delivery, automated gates, lifecycle intelligence, and dependency health monitoring.
- For High Assurance, continuously verify controls, exercise severe scenarios, preserve tamper-evident evidence, and test retirement and recovery end to end.

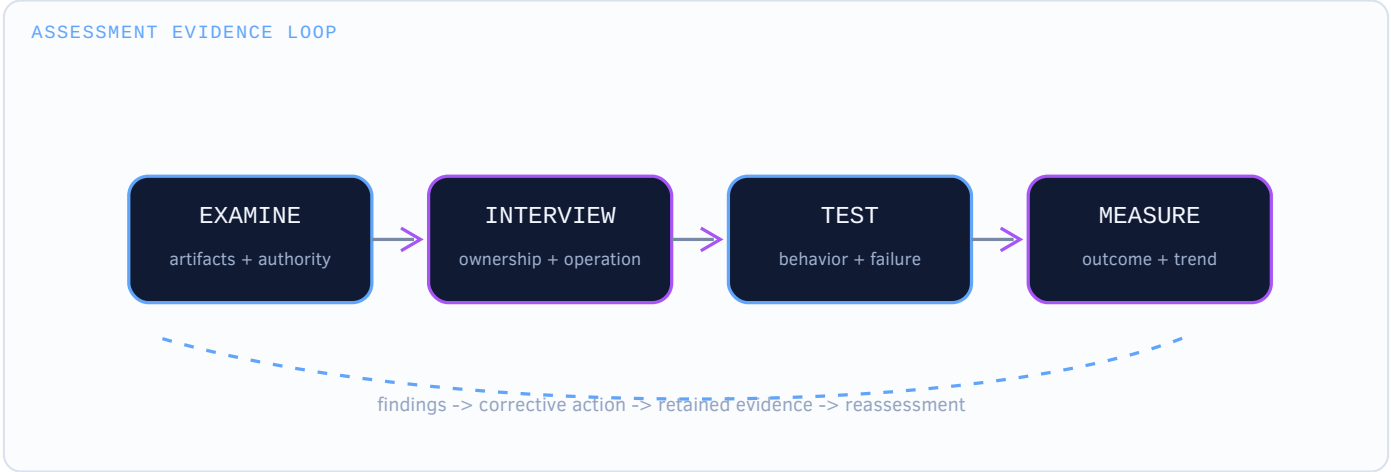
## 31. Limitations and Residual Risk from Source Draft

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

FOUNDATION STANDARD / STRUCTURAL PART

# Part VI – Assurance and Assessment

## 32. Assessment Methodology




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

### 12.1 Finding States

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

### 12.2 Conformance

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

## 33. Metrics and Reporting from Source Draft

| Metric | Definition | Expected use or target |
|---|---|---|
| Objective attainment | Time and request volume meeting defined service objectives | Within approved error budget |
| Change failure rate | Changes causing rollback, incident, hotfix, or objective breach | Tracked by service and risk class; declining trend |

| Metric | Definition | Expected use or target |
|---|---|---|
| Recovery performance | Observed recovery time and point versus objectives | Meets objective in exercises and incidents |
| Detection and containment time | Elapsed time from impact to detection and containment | Risk-defined; trend reviewed |
| Operational-readiness coverage | Production capabilities with current owners, SLOs, runbooks, telemetry, rollback, and recovery evidence | 100% |

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

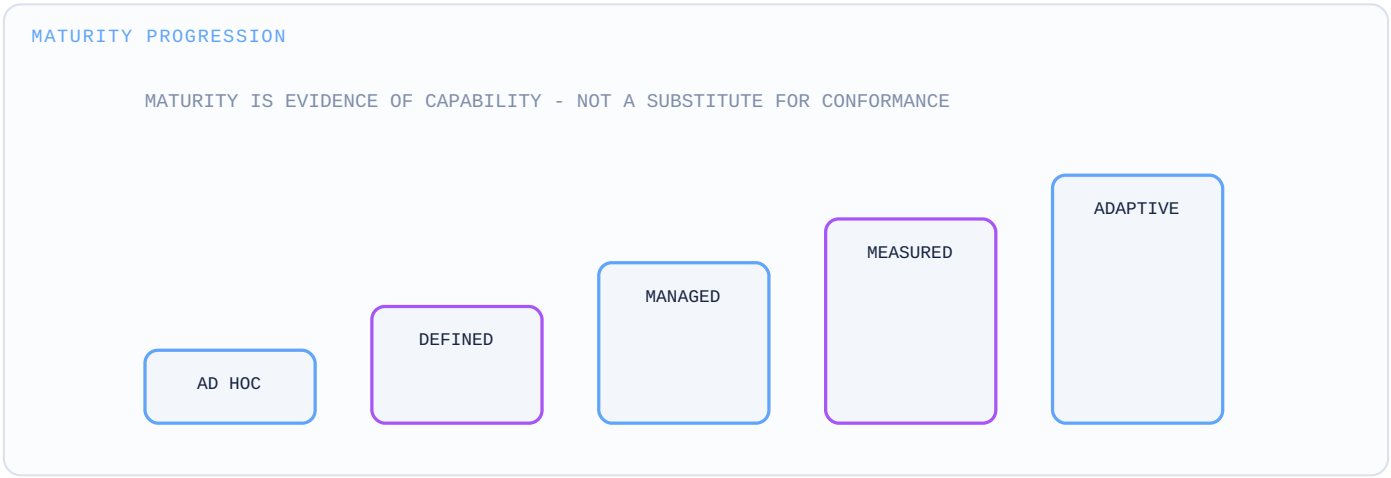
## 34. Exceptions and Compensating Controls

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

## 35. Enterprise Metric Set

| Metric | Measurement Requirement |
|---|---|
| services without current owner | Defined by the adopting organization with owner, source, target, and cadence. |
| SLO attainment and error-budget consumption | Defined by the adopting organization with owner, source, target, and cadence. |
| changes causing incident or rollback | Defined by the adopting organization with owner, source, target, and cadence. |
| release gate overrides | Defined by the adopting organization with owner, source, target, and cadence. |
| mean time to detect, contain, restore, and learn | Defined by the adopting organization with owner, source, target, and cadence. |
| restore tests meeting objectives | Defined by the adopting organization with owner, source, target, and cadence. |
| critical dependencies beyond patch target | Defined by the adopting organization with owner, source, target, and cadence. |
| deprecated interfaces past retirement date | Defined by the adopting organization with owner, source, target, and cadence. |

# 36. Maturity Model




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

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

# 37. Assessment Confidence

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

# 38. Executive Assurance Dashboard

The executive report SHOULD present:

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

- corrective-action status.

FOUNDATION STANDARD / STRUCTURAL PART

# Part VII – Authority and Traceability

## 39. Cross-Standard Dependencies from Source Draft

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

## 40. Current External Authority Register

| Authority | Relevance | Official Location | Status | Validated |
|---|---|---|---|---|
| ISO/IEC 20000-1:2018 | Service management system requirements | https://www.iso.org/standard/70636.html | Published | 2026-09-17 |
| ISO 22301:2019 | Business continuity management systems | https://www.iso.org/standard/75106.html | Published | 2026-09-17 |
| ISO/IEC/IEEE 15288:2023 | System life cycle processes | https://www.iso.org/standard/81702.html | Published | 2026-09-17 |
| NIST CSF 2.0 | Cybersecurity governance and recovery | https://www.nist.gov/cyberframework | Current | 2026-09-17 |
| NIST SP 800-53 Rev. 5 | Contingency, configuration, incident, maintenance, and audit controls | https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final | Final update 1 | 2026-09-17 |

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

## 41. Control Traceability

Each control MUST remain traceable to:

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

## 42. Source-Draft Preservation

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

FOUNDATION STANDARD / STRUCTURAL PART

# Part VIII – Appendices

## Appendix A – Source-Draft Evolution Notes

- Preserves the source draft's release gates, evidence folders, runbooks, rollback discipline, observability, incident management, and current-state lifecycle control.
- Generalizes tool-specific operational recommendations into outcome-based requirements.
- Strengthens service objectives, progressive delivery, configuration authority, dependency retirement, and operational evidence.
- Separates emergency change flexibility from ungoverned bypass.

## Appendix B – Change History

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

## Appendix C – Control Summary

| Control | Family | Title | Profiles | Automation | Impact |
|---|---|---|---|---|---|
| MYTHOS-FND-ORL-01 | Ownership | Service ownership and catalog | Foundational, Advanced, High Assurance | High | Critical |
| MYTHOS-FND-ORL-02 | Objectives | Service-level indicators and objectives | Foundational, Advanced, High Assurance | High | Critical |
| MYTHOS-FND-ORL-03 | Observability | Observable operational state | Foundational, Advanced, High Assurance | High | Critical |
| MYTHOS-FND-ORL-04 | Readiness | Operational readiness review | Foundational, Advanced, High Assurance | Partial | Critical |
| MYTHOS-FND-ORL-05 | Change | Controlled change management | Foundational, Advanced, High Assurance | High | Critical |
| MYTHOS-FND-ORL-06 | Release | Release authorization and evidence | Foundational, Advanced, High Assurance | High | Critical |
| MYTHOS-FND-ORL-07 | Deployment | Progressive and safe deployment | Advanced, High Assurance | High | Critical |
| MYTHOS-FND-ORL-08 | Configuration | Authoritative configuration and state management | Foundational, Advanced, High Assurance | High | Critical |
| MYTHOS-FND-ORL-09 | Rollback | Rollback and forward-recovery capability | Foundational, Advanced, High Assurance | Partial | Critical |
| MYTHOS-FND-ORL-10 | Runbooks | Operational runbooks and automation | Foundational, Advanced, High Assurance | Partial | Critical |

| Control | Family | Title | Profiles | Automation | Impact |
|---|---|---|---|---|---|
| MYTHOS-FND-ORL-11 | Incident | Incident command, containment, and communication | Foundational, Advanced, High Assurance | Partial | Critical |
| MYTHOS-FND-ORL-12 | Problem management | Systemic problem management and learning | Foundational, Advanced, High Assurance | Partial | Material |
| MYTHOS-FND-ORL-13 | Capacity | Capacity, performance, and demand management | Foundational, Advanced, High Assurance | High | Critical |
| MYTHOS-FND-ORL-14 | Recovery | Backup, restore, and continuity | Foundational, Advanced, High Assurance | Partial | Critical |
| MYTHOS-FND-ORL-15 | Maintenance | Vulnerability, patch, and dependency lifecycle | Foundational, Advanced, High Assurance | High | Critical |
| MYTHOS-FND-ORL-16 | Data operations | Operational data integrity and maintenance | Foundational, Advanced, High Assurance | High | Critical |
| MYTHOS-FND-ORL-17 | Security operations | Operational access and emergency controls | Foundational, Advanced, High Assurance | High | Critical |
| MYTHOS-FND-ORL-18 | Retirement | Controlled deprecation and retirement | Foundational, Advanced, High Assurance | Partial | Critical |

## Appendix D – Minimum Conformance Claim Record

```
standard: MYTHOS-FND-0005
version: 0.2.0
profile: foundational | advanced | high_assurance
scope: <bounded systems, teams, environments, and processes>
assessment_period: <start/end>
assessor: <person or independent body>
tailoring_decisions: []
exceptions: []
findings_summary:
  satisfied: 0
  partially_satisfied: 0
  not_satisfied: 0
  not_applicable: 0
  not_assessed: 0
residual_risk_owner: <accountable role>
approval: <record reference>
```

## Appendix E – Publication Review Checklist

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

- [ ] Accessibility and publication quality verified
- [ ] Machine-readable control catalog validated
- [ ] Change and review record complete
- [ ] Formal approval recorded