CANDIDATE STANDARD

Mythos Data, API, and Integration Standard

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

PERMANENT ID
MYTHOS-FND-0006

PUBLICATION CLASS
CANDIDATE STANDARD

VERSION / STATUS
1.0.0-candidate / CANDIDATE

PERMANENT PUBLICATION IDENTITY

Mythos Data, API, and Integration Standard

Universal Requirements for Data Governance, Contracts, APIs, Events, Reliability, Security, Lineage, Compatibility, and Integration Operations

Document ID
MYTHOS-FND-0006

Version
1.0.0-candidate

Status
Candidate Standard

Review date
2027-09-17

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

PROFILE	CONTROLS	CADENCE	EVIDENCE
3 LEVELS	19	TRIGGERED	ASSESSABLE
Foundational / Advanced / High Assurance	Atomic normative controls	Annual plus material-change review	Examine / Interview / Test / Measure

Reader orientation

Dimension	Engineering position
Primary domain	Foundation and Governance
Audience	Data, API, integration, and platform engineers; Application and infrastructure architects; Security, privacy, and governance teams; Product and service owners; Operations and reliability engineers
Publisher / owner	Mythos Systems / Standards Program
Public classification	Public technical standard
Canonical route	/library/standards/foundation/mythos-fnd-0006/

Expected outcomes

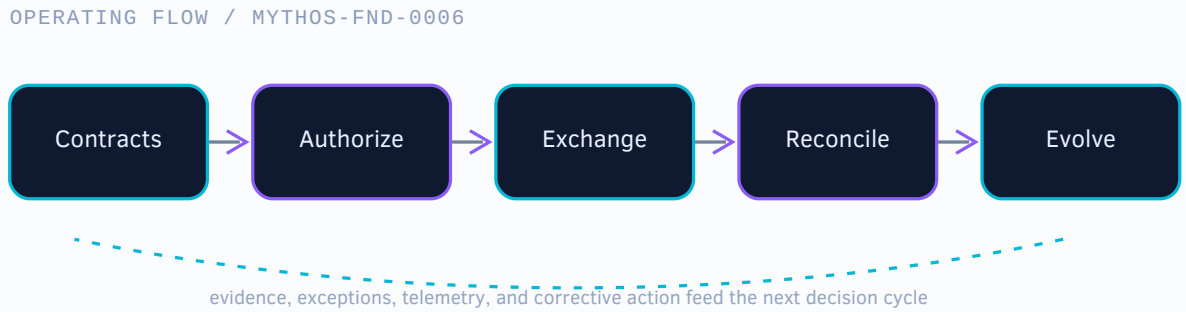
- Make data meaning, ownership, quality, sensitivity, and lifecycle explicit.
- Create stable, testable, evolvable contracts for synchronous and asynchronous integration.
- Prevent distributed failure, duplicate effects, unauthorized access, and silent data corruption.
- Provide evidence for compatibility, lineage, operational health, and deprecation decisions.

SOURCE / FRESHNESS POSITION

Authority and source posture

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

FOUNDATION OPERATING DOCTRINE



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

NAVIGATION

Contents

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

Document Control 8

Revision Record 8

How to Use This Standard 9

Executive Reading Path 9

Engineering Reading Path 9

Assessment Reading Path 9

Normative and Informative Content 9

Part I – Executive Direction 10

1. Executive Overview 10

2. Executive Findings and Required Direction 10

3. Business and Operational Impact 10

4. Target-State Summary 11

5. Leadership Responsibilities 12

Part II – Standard Foundation 13

6. Purpose and Objectives 13

7. Scope 13

8. Intended Audience 13

9. Requirements Language and Conformance 13

10. Normative References from Source Draft 13

11. Informative References from Source Draft 14

12. Terms and Definitions 14

13. Applicability and Tailoring 15

Part III – Risk and Architecture 16

14. Enterprise Problem and Risk Landscape 16

15. Governing Principles 16

16. Reference Operating Architecture 16

17. Roles and Accountability 17

18. State, Evidence, and Decision Model 18

19. Security and Trust Considerations 18

20. Failure Modes 18

21. Cross-Functional Dependencies 18

Part IV – Normative Control System **19**

22. Control-Family Overview 19

23. Normative Controls 20

Part V – Implementation and Operations **40**

24. Implementation Profiles 40

25. Implementation Lifecycle 40

26. Integration Requirements 41

27. Failure Handling and Recovery 41

28. Exceptions and Compensating Controls 41

29. Prohibited Practices 41

30. Adoption Roadmap from Source Draft 42

31. Limitations and Residual Risk from Source Draft 42

Part VI – Assurance and Assessment **43**

32. Assessment Methodology 43

33. Metrics and Reporting from Source Draft 43

34. Exceptions and Compensating Controls 44

35. Enterprise Metric Set 44

36. Maturity Model 45

37. Assessment Confidence 45

38. Executive Assurance Dashboard 45

Part VII – Authority and Traceability **47**

39. Cross-Standard Dependencies from Source Draft 47

40. Current External Authority Register 47

41. Control Traceability 47

42. Source-Draft Preservation 48

Part VIII – Appendices **49**

Appendix A — Source-Draft Evolution Notes 49

Appendix B — Change History 49

Appendix C — Control Summary 49

Appendix D — Minimum Conformance Claim Record 50

Appendix E — Publication Review Checklist 50

NORMATIVE SYSTEM

Control index

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

MYTHOS-FND-DAI-01	Data and integration ownership	21
MYTHOS-FND-DAI-02	Data classification and permitted use	22
MYTHOS-FND-DAI-03	Versioned data contracts	23
MYTHOS-FND-DAI-04	Consistent resource and operation design	24
MYTHOS-FND-DAI-05	Identity, authorization, and tenant context	25
MYTHOS-FND-DAI-06	Idempotency and duplicate-effect control	26
MYTHOS-FND-DAI-07	Concurrency, ordering, and consistency	27
MYTHOS-FND-DAI-08	Structured errors and failure semantics	28
MYTHOS-FND-DAI-09	Rate limits, quotas, backpressure, and admission control	29
MYTHOS-FND-DAI-10	Event and messaging semantics	30
MYTHOS-FND-DAI-11	Data quality objectives and controls	31
MYTHOS-FND-DAI-12	Lineage, provenance, and transformation accountability	32
MYTHOS-FND-DAI-13	Integration observability and reconciliation	33
MYTHOS-FND-DAI-14	Dependency failure and retry control	34
MYTHOS-FND-DAI-15	Schema and data migration safety	35
MYTHOS-FND-DAI-16	Versioning, compatibility, and deprecation	36
MYTHOS-FND-DAI-17	Third-party integration boundary control	37
MYTHOS-FND-DAI-18	Contract, compatibility, and failure testing	38
MYTHOS-FND-DAI-19	Discoverable interface documentation	39

Document Control

Field	Value
Document ID	MYTHOS-FND-0006
Standard	Data, API, and Integration
Version	1.0.0-candidate
Status	Candidate Standard
Classification	Public
Publisher	Mythos Systems
Program	Mythos Engineering Standards Program
Accountable Owner	Mythos Systems Standards Program
Technical Review	Required
Source and Citation Review	Required
Assessment Review	Required
Accessibility and Publication Review	Required
Supersedes	No published edition; evolves source draft 0.2.0
Next Review	2027-09-17 or earlier on trigger

Revision Record

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

How to Use This Standard

Executive Reading Path

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

Engineering Reading Path

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

Assessment Reading Path

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

Normative and Informative Content

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

FOUNDATION STANDARD / STRUCTURAL PART

Part I – Executive Direction

1. Executive Overview

Enterprise systems fail at boundaries. Data changes meaning, requests are duplicated, events arrive out of order, dependencies throttle or disappear, and undocumented compatibility assumptions become production outages. This standard defines the contract and operating discipline required for data, APIs, events, and integrations to remain secure, observable, evolvable, and accountable.

The institutional objective is to establish durable contracts, data authority, identity context, failure semantics, lineage, observability, compatibility, and lifecycle controls for data exchange and system integration. Adoption should produce a controlled operating state in which leadership can understand the material risks, engineering teams can act on explicit requirements, assessors can test implementation and operating effectiveness, and the organization can support every conformance or trust claim with current evidence.

2. Executive Findings and Required Direction

Finding	Enterprise Exposure	Required Direction
Contract ambiguity	Consumers infer behavior from examples or implementation rather than versioned contracts.	Use explicit schemas, operation semantics, compatibility rules, and ownership.
Duplicate and concurrent effects	Retries and concurrent updates create unintended repeated or lost actions.	Define idempotency, concurrency, ordering, and conflict semantics.
Identity and tenant leakage	Integration context is lost or inconsistently enforced across boundaries.	Propagate authenticated identity, authorization, purpose, and tenant context.
Failure hidden as success	Unstructured errors and partial outcomes prevent reliable recovery.	Define machine-readable errors, indeterminate outcomes, retries, and reconciliation.
Third-party dependency opacity	External service limits, changes, and outages are not governed as product risk.	Maintain dependency contracts, quotas, health, fallback, exit, and evidence.

3. Business and Operational Impact

3.1 Strategic Impact

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

3.2 Delivery and Cost Impact

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

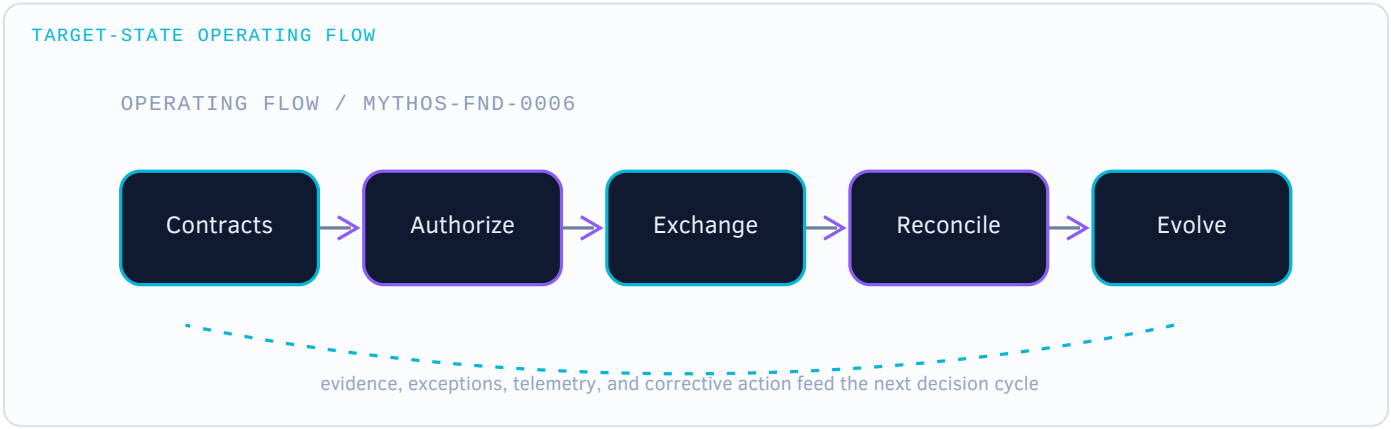
3.3 Security, Privacy, and Trust Impact

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

3.4 Workforce and Organizational Impact

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

4. Target-State Summary



The target state contains the following institutional components:

#	Target-State Component
1	Data and integration ownership
2	Classification and permitted use
3	Versioned schemas and contracts
4	Resource and operation design
5	Identity and tenant context
6	Idempotency and duplicate-effect control
7	Concurrency, ordering, and consistency
8	Structured errors and failure states
9	Rate limits, quotas, backpressure, and admission
10	Events and messaging
11	Data quality and lineage
12	Observability and reconciliation
13	Retry and dependency failure
14	Migration and compatibility

#	Target-State Component
15	Third-party boundary control
16	Contract and failure testing
17	Discoverable documentation

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

5. Leadership Responsibilities

Role	Accountability
Data owner	Owns meaning, permitted use, quality, retention, and authority.
API or integration owner	Owns contract, compatibility, operations, and support.
Domain architect	Defines resource, event, and consistency boundaries.
Security and privacy lead	Approves identity, authorization, data movement, and retention.
Platform engineering	Provides gateways, schemas, messaging, telemetry, and policy enforcement.
Consumer owner	Validates use and migration obligations.
Reliability owner	Defines retry, backpressure, failure, and reconciliation.
Independent assessor	Tests contract and operational behavior.

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

FOUNDATION STANDARD / STRUCTURAL PART

Part II – Standard Foundation

6. Purpose and Objectives

- Make data meaning, ownership, quality, sensitivity, and lifecycle explicit.
- Create stable, testable, evolvable contracts for synchronous and asynchronous integration.
- Prevent distributed failure, duplicate effects, unauthorized access, and silent data corruption.
- Provide evidence for compatibility, lineage, operational health, and deprecation decisions.

7. Scope

Applies to databases, files, messages, event streams, APIs, webhooks, batch transfers, device protocols, data pipelines, caches, search indexes, analytics, model data paths, and third-party integrations.

8. Intended Audience

- Data, API, integration, and platform engineers
- Application and infrastructure architects
- Security, privacy, and governance teams
- Product and service owners
- Operations and reliability engineers

9. Requirements Language and Conformance

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

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

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

10. Normative References from Source Draft

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

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

11. Informative References from Source Draft

- **OpenAPI Specification 3.2.1** — OpenAPI Initiative specification. https://spec.openapis.org/oas/v3.2.1.html
- **JSON Schema Draft 2020-12** — JSON Schema Core and Validation. https://json-schema.org/draft/2020-12
- **AsyncAPI Specification 3.1.0** — AsyncAPI Initiative specification. https://www.asyncapi.com/docs/reference/specification/v3.1.0
- **CloudEvents 1.0.2** — Cloud Native Computing Foundation event format. https://github.com/cloudevents/spec/tree/v1.0.2
- **NIST SP 800-53 Rev. 5, Release 5.2.0** — Security and Privacy Controls for Information Systems and Organizations. https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final
- **NIST Privacy Framework 1.0** — A Tool for Improving Privacy through Enterprise Risk Management. https://www.nist.gov/privacy-framework/privacy-framework
- **ISO/IEC 25010:2023** — Systems and software Quality Requirements and Evaluation — Product quality model. https://www.iso.org/standard/78176.html
- **NIST SP 800-218 v1.1** — Secure Software Development Framework (SSDF). https://csrc.nist.gov/pubs/sp/800/218/final

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

12. Terms and Definitions

Term	Definition
Accountable owner	The person or formally delegated role that accepts responsibility for an outcome, decision, control, or risk.
Assessment object	The system, process, component, artifact, team, service, or organizational scope being evaluated.
Compensating control	An alternative safeguard that provides comparable risk reduction when the specified control cannot be implemented as written.
Conformance claim	A bounded statement that an identified scope satisfies the applicable requirements of a named standard version and assurance profile.
Evidence	Reviewable information that supports a conclusion about design, implementation, operation, or control effectiveness.
High Assurance	The cumulative profile requiring stronger independence, adversarial testing, continuous verification, or formal evidence where risk warrants it.
Residual risk	Risk remaining after controls, mitigations, and compensating measures are applied.
System	A product, service, application, platform, workflow, integration, operational capability, or combined socio-technical environment.
Tailoring	A documented decision to include, strengthen, parameterize, or mark a control not applicable based on scope and risk.
Data contract	A versioned agreement defining data semantics, schema, quality, ownership, access, lifecycle, and compatibility expectations.
Idempotency	The property that repeated processing of the same logical request or event does not create unintended additional effects.
Lineage	The recorded origin, transformations, movement, and use of data or derived artifacts.

Term	Definition
Compatibility window	The period and version range during which producers and consumers are expected to interoperate.
Integration boundary	A change in ownership, trust, protocol, data semantics, availability, or operational responsibility.

13. Applicability and Tailoring

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

FOUNDATION STANDARD / STRUCTURAL PART

Part III – Risk and Architecture

14. Enterprise Problem and Risk Landscape

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

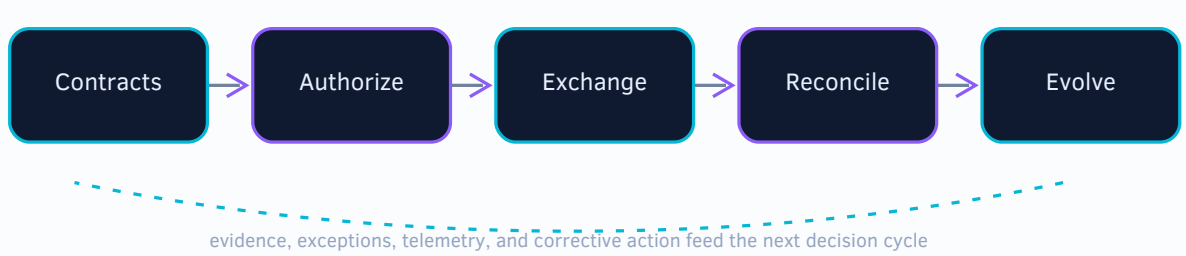
Adopting organizations SHOULD maintain a domain-specific risk register that identifies cause, affected asset or stakeholder, credible scenario, impact, existing controls, residual risk, owner, review trigger, and evidence. Risks that cross standards MUST be linked rather than copied into disconnected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

15. Governing Principles

- Data and interfaces have accountable owners and explicit contracts.
- Compatibility is designed and tested, not assumed.
- At-least-once delivery and partial failure are normal distributed-system conditions.
- Authorization is enforced at the authoritative boundary and at the resource level.
- Data quality, lineage, retention, and privacy follow derived data and secondary stores.
- Third-party integration failures must be contained and observable.

16. Reference Operating Architecture

REFERENCE OPERATING ARCHITECTURE



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

16.1 Control Plane

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

16.2 Delivery and Enforcement Plane

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

16.3 Evidence and Assurance Plane

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

16.4 Feedback Plane

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

17. Roles and Accountability

Role	Accountability
Data owner	Owns meaning, permitted use, quality, retention, and authority.
API or integration owner	Owns contract, compatibility, operations, and support.
Domain architect	Defines resource, event, and consistency boundaries.
Security and privacy lead	Approves identity, authorization, data movement, and retention.
Platform engineering	Provides gateways, schemas, messaging, telemetry, and policy enforcement.
Consumer owner	Validates use and migration obligations.
Reliability owner	Defines retry, backpressure, failure, and reconciliation.
Independent assessor	Tests contract and operational behavior.

18. State, Evidence, and Decision Model

The adopting organization MUST distinguish:

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

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

19. Security and Trust Considerations

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

20. Failure Modes

Failure or Anti-Pattern	Enterprise Consequence
Using documentation examples as the only contract	Failure can create hidden risk, misleading assurance, uncontrolled cost, or unsafe operation.
Retries without idempotency analysis	Failure can create hidden risk, misleading assurance, uncontrolled cost, or unsafe operation.
Returning generic errors without machine-readable cause	Failure can create hidden risk, misleading assurance, uncontrolled cost, or unsafe operation.
Assuming exactly-once delivery without an effect strategy	Failure can create hidden risk, misleading assurance, uncontrolled cost, or unsafe operation.
Embedding tenant identity only in request payload	Failure can create hidden risk, misleading assurance, uncontrolled cost, or unsafe operation.
Changing schemas in place without compatibility testing	Failure can create hidden risk, misleading assurance, uncontrolled cost, or unsafe operation.
Integrating third parties without exit or degraded-mode design	Failure can create hidden risk, misleading assurance, uncontrolled cost, or unsafe operation.

21. Cross-Functional Dependencies

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

FOUNDATION STANDARD / STRUCTURAL PART

Part IV – Normative Control System

22. Control-Family Overview

CONTROL-FAMILY CONSTELLATION

This standard contains **19 controls** across the following families:

- Governance
- Classification
- Contracts
- API design
- Authorization
- Reliability
- Concurrency
- Errors
- Flow control
- Events
- Quality
- Lineage
- Observability
- Resilience
- Migrations
- Lifecycle
- Third parties
- Testing

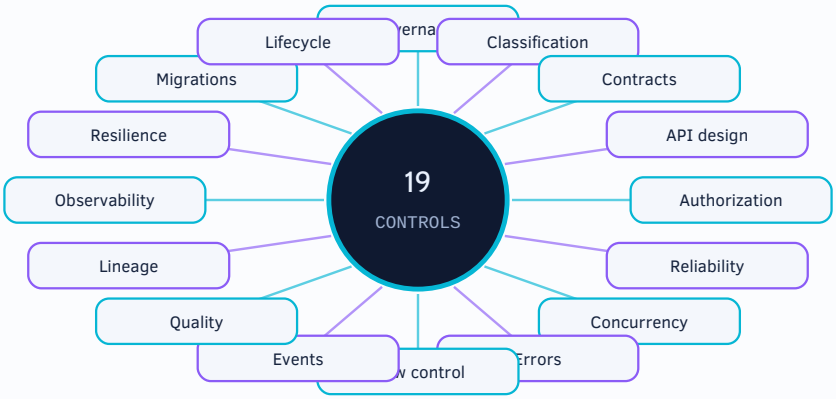
- Documentation

23. Normative Controls

CONTROL SET	PROFILES	ASSESSMENT
19	3	4
atomic requirements	cumulative assurance levels	Examine / Interview / Test / Measure

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

NORMATIVE CONTROL CONSTELLATION



NORMATIVE CONTROL

MYTHOS-FND-DAI-01 – Data and integration ownership

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

Requirement

Every material data domain, data product, API, event channel, pipeline, and external integration MUST have accountable ownership for semantics, access, quality, lifecycle, compatibility, and operational support.

Purpose

Prevents ownerless interfaces and ambiguous responsibility for data defects or breaking changes.

Applicability

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

Implementation guidance

- Separate producer, consumer, platform, and business ownership where useful.
- Record criticality, support expectations, and escalation.
- Review ownership after organizational or supplier change.

Required evidence

- Data and interface catalog
- Ownership records
- Escalation tests

Assessment procedure

- **Examine:** Sample catalog entries against deployed systems.
- **Interview:** Interview owners and consumers.
- **Test:** Review unowned or stale entries.

Exceptions and compensating controls

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

External mappings

- NIST CSF 2.0 — ID.AM and GV.RR

NORMATIVE CONTROL

MYTHOS-FND-DAI-02 – Data classification and permitted use

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

Requirement

Data fields, records, streams, files, embeddings, indexes, logs, and derived outputs MUST inherit or receive classification, purpose, access, residency, retention, integrity, and privacy handling requirements.

Purpose

Ensures protections follow data across transformations and secondary stores.

Applicability

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

Implementation guidance

- Classify unknown or mixed data conservatively.
- Record sensitive-field semantics in schemas.
- Prevent lower-classification outputs when transformations do not reliably remove sensitivity.

Required evidence

- Classification map
- Schema annotations
- Handling-policy tests

Assessment procedure

- **Examine:** Trace sensitive data through a pipeline.
- **Interview:** Inspect caches and logs.
- **Test:** Test enforcement of residency or export restrictions.

Exceptions and compensating controls

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

External mappings

- NIST SP 800-53 — RA-2, MP family
- NIST Privacy Framework

NORMATIVE CONTROL

MYTHOS-FND-DAI-03 – Versioned data contracts

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

Requirement

Material data exchanges MUST have versioned contracts defining semantics, schema, required and optional fields, identifiers, units, nullability, quality expectations, ownership, security, lifecycle, and compatibility rules.

Purpose

Prevents syntactically valid but semantically incompatible integration.

Applicability

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

Implementation guidance

- Use machine-readable schemas where practical.
- Define examples and counterexamples.
- Treat semantic changes as potentially breaking even when syntax is unchanged.

Required evidence

- Data contracts
- Schema repository
- Contract review records

Assessment procedure

- **Examine:** Validate samples and counterexamples.
- **Interview:** Interview producer and consumer about field meaning.
- **Test:** Detect an undeclared semantic change in a test workflow.

Exceptions and compensating controls

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

External mappings

- JSON Schema 2020-12
- OpenAPI 3.2.1

NORMATIVE CONTROL

MYTHOS-FND-DAI-04 – Consistent resource and operation design

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

Requirement

APIs MUST define stable resource or operation semantics, authentication, authorization, request and response schemas, status and error behavior, limits, idempotency expectations, versioning, and lifecycle status in an authoritative specification.

Purpose

Creates predictable, testable interfaces and reduces consumer-specific behavior.

Applicability

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

Implementation guidance

- Use nouns and commands consistently.
- Model asynchronous operations explicitly.
- Document partial success, long-running operations, and cancellation.
- Avoid exposing internal implementation structures as accidental contracts.

Required evidence

- API specification
- Design review
- Conformance tests

Assessment procedure

- **Examine:** Validate implementation against specification.
- **Interview:** Test undocumented fields and behavior.
- **Test:** Review consistency across similar APIs.

Exceptions and compensating controls

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

External mappings

- OpenAPI Specification 3.2.1

NORMATIVE CONTROL

MYTHOS-FND-DAI-05 – Identity, authorization, and tenant context

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

Requirement

Every integration request, event publication, subscription, data operation, and administrative action MUST be authorized at an authoritative enforcement point using current identity, scope, resource, tenant or trust-domain context, and policy.

Purpose

Prevents confused-deputy, cross-tenant, frontend-only, and overly broad service access.

Applicability

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

Implementation guidance

- Use workload identities and narrow scopes.
- Propagate context through asynchronous paths with integrity protection.
- Do not trust caller-supplied tenant identifiers without binding to identity and policy.

Required evidence

- Authorization policy
- Identity and scope inventory
- Negative tests

Assessment procedure

- **Examine:** Attempt direct unauthorized access.
- **Interview:** Replay an event under a different tenant.
- **Test:** Test revoked scopes.

Exceptions and compensating controls

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

External mappings

- NIST SP 800-53 — AC and IA families

NORMATIVE CONTROL

MYTHOS-FND-DAI-06 – Idempotency and duplicate-effect control

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

Requirement

Operations that may be retried, replayed, duplicated, or resumed MUST define idempotency or duplicate-detection behavior and preserve enough state to prevent unintended repeated effects.

Purpose

Addresses normal distributed-system delivery behavior and uncertain outcomes.

Applicability

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

Implementation guidance

- Use client or server idempotency keys for consequential commands.
- Define retention and conflict behavior.
- Make consumers resilient to duplicate events.
- Distinguish safe reads from mutating actions.

Required evidence

- Idempotency design
- Duplicate and replay tests
- State records

Assessment procedure

- **Examine:** Submit duplicate and concurrent requests.
- **Interview:** Replay events after restart.
- **Test:** Verify conflicting keys fail safely.

Exceptions and compensating controls

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

External mappings

- CloudEvents 1.0.2 — event identity

NORMATIVE CONTROL

MYTHOS-FND-DAI-07 – Concurrency, ordering, and consistency

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

Requirement

Data and integration designs MUST state and enforce concurrency, ordering, transactional, consistency, conflict, and stale-read semantics for operations where competing actions can affect correctness.

Purpose

Prevents lost updates, double execution, inconsistent decisions, and hidden assumptions about distributed state.

Applicability

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

Implementation guidance

- Use optimistic concurrency, leases, sequencing, partition keys, or transactions as appropriate.
- Document where eventual consistency is acceptable.
- Define reconciliation and conflict resolution.

Required evidence

- Consistency model
- Concurrency tests
- Reconciliation procedures

Assessment procedure

- **Examine:** Run concurrent conflicting operations.
- **Interview:** Reorder events.
- **Test:** Verify conflict evidence and recovery.

Exceptions and compensating controls

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

External mappings

- ISO/IEC 25010:2023 — reliability and functional correctness

NORMATIVE CONTROL

MYTHOS-FND-DAI-08 – Structured errors and failure semantics

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

Requirement

Interfaces MUST return structured, stable, non-sensitive error information that distinguishes caller errors, authorization denial, conflicts, throttling, dependency failure, transient unavailability, and internal failure and provides correlation for support.

Purpose

Enables safe recovery without leaking secrets or forcing consumers to parse human text.

Applicability

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

Implementation guidance

- Use stable machine codes and human-readable messages.
- Define retryability and backoff hints.
- Preserve root-cause detail in protected telemetry rather than public responses.

Required evidence

- Error catalog
- Contract tests
- Redaction review

Assessment procedure

- **Examine:** Trigger each major error class.
- **Interview:** Verify clients do not retry permanent failures.
- **Test:** Inspect responses for sensitive content.

Exceptions and compensating controls

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

External mappings

- OpenAPI 3.2.1

NORMATIVE CONTROL

MYTHOS-FND-DAI-09 – Rate limits, quotas, backpressure, and admission control

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

Requirement

APIs, event systems, pipelines, and integrations MUST define and enforce capacity limits, quotas, backpressure, queue bounds, timeout budgets, and overload behavior proportionate to service and tenant risk.

Purpose

Prevents cascading failure, unfair resource capture, and unbounded queues.

Applicability

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

Implementation guidance

- Expose limits and reset behavior.
- Prioritize critical workloads.
- Bound retries and concurrency.
- Use dead-letter or quarantine paths with operational ownership.

Required evidence

- Limit policy
- Load and overload tests
- Queue and retry telemetry

Assessment procedure

- **Examine:** Exceed quotas and capacity.
- **Interview:** Verify graceful degradation.
- **Test:** Inspect unbounded or ownerless queues.

Exceptions and compensating controls

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

External mappings

- ISO/IEC 25010:2023 — performance efficiency and reliability

NORMATIVE CONTROL

MYTHOS-FND-DAI-10 – Event and messaging semantics

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

Requirement

Event channels MUST define event identity, source, type, time semantics, subject, schema, ordering scope, delivery guarantee, retention, replay, consumer ownership, sensitive-data handling, and evolution policy.

Purpose

Makes asynchronous behavior explicit and operable.

Applicability

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

Implementation guidance

- Use a standard envelope such as CloudEvents where appropriate.
- Separate facts from commands.
- Define poison-message handling and replay authorization.
- Avoid embedding mutable external state without version or reference.

Required evidence

- Event catalog
- AsyncAPI or equivalent specification
- Replay and poison-message tests

Assessment procedure

- **Examine:** Inspect sampled events.
- **Interview:** Replay across schema versions.
- **Test:** Test unauthorized subscription or replay.

Exceptions and compensating controls

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

External mappings

- AsyncAPI 3.1.0
- CloudEvents 1.0.2

NORMATIVE CONTROL

MYTHOS-FND-DAI-11 – Data quality objectives and controls

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

Requirement

Critical data products and fields MUST have defined and monitored quality objectives for accuracy, completeness, validity, consistency, timeliness, uniqueness, lineage, and fitness for intended use.

Purpose

Prevents technically available but misleading or unsafe data from being treated as trustworthy.

Applicability

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

Implementation guidance

- Define ownership and thresholds by use case.
- Quarantine, annotate, or block data that fails critical constraints.
- Distinguish observed quality from inferred confidence.

Required evidence

- Data quality specification
- Quality dashboard
- Exception and remediation records

Assessment procedure

- **Examine:** Recalculate selected metrics.
- **Interview:** Inject invalid data.
- **Test:** Review downstream behavior when quality falls below threshold.

Exceptions and compensating controls

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

External mappings

- ISO/IEC 25010:2023 — data-related quality characteristics

NORMATIVE CONTROL

MYTHOS-FND-DAI-12 – Lineage, provenance, and transformation accountability

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

Requirement

Critical data and derived artifacts MUST record source, collection or creation context, transformations, responsible process, versions, timestamps, and integrity information sufficient to reproduce or explain material outputs.

Purpose

Supports audit, debugging, privacy, model governance, and correction of upstream defects.

Applicability

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

Implementation guidance

- Capture field-level lineage where consequence warrants.
- Include manual edits and external enrichments.
- Preserve provenance across exports and model inputs.

Required evidence

- Lineage graph
- Transformation manifests
- Reproduction records

Assessment procedure

- **Examine:** Trace an output to original sources.
- **Interview:** Change an upstream record and identify affected derivatives.
- **Test:** Verify provenance survives export or handoff.

Exceptions and compensating controls

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

External mappings

- NIST AI 600-1 — provenance
- NIST SP 800-53 — AU family

NORMATIVE CONTROL

MYTHOS-FND-DAI-13 – Integration observability and reconciliation

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

Requirement

Integrations MUST expose end-to-end correlation, success and failure outcomes, latency, retry, queue, freshness, volume, schema, and reconciliation signals sufficient to detect silent loss, duplication, delay, or corruption.

Purpose

Makes distributed data movement diagnosable and measurable.

Applicability

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

Implementation guidance

- Use business reconciliation in addition to transport metrics.
- Monitor expected absence and stale data.
- Correlate across asynchronous boundaries without leaking sensitive payloads.

Required evidence

- Telemetry specification
- Reconciliation reports
- Alert tests

Assessment procedure

- **Examine:** Trace a transaction or batch end to end.
- **Interview:** Drop or duplicate a message in a test environment.
- **Test:** Verify alerts and reconciliation identify the issue.

Exceptions and compensating controls

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

External mappings

- NIST SP 800-53 — AU-12, SI-4

NORMATIVE CONTROL

MYTHOS-FND-DAI-14 – Dependency failure and retry control

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

Requirement

Integrations MUST define timeout, retry, backoff, circuit breaking, fallback, cache, compensation, and manual reconciliation behavior based on operation semantics and dependency failure modes.

Purpose

Prevents retry storms, cascading failure, stale authority, and duplicate side effects.

Applicability

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

Implementation guidance

- Use deadline budgets across call chains.
- Do not retry non-idempotent actions without protection.
- Define stale-data limits and user-visible degraded state.
- Test provider throttling and partial response.

Required evidence

- Resilience policy
- Failure-injection results
- Fallback and reconciliation procedures

Assessment procedure

- **Examine:** Disable or slow a dependency.
- **Interview:** Verify retries are bounded.
- **Test:** Inspect correctness under stale or partial data.

Exceptions and compensating controls

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

External mappings

- ISO/IEC 25010:2023 — reliability

NORMATIVE CONTROL

MYTHOS-FND-DAI-15 – Schema and data migration safety

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

Requirement

Schema and data migrations MUST be versioned, reviewed, tested at representative scale, observable, resumable or safely restartable, compatible with deployment sequence, backed by recovery points, and verified through reconciliation.

Purpose

Controls one of the most common sources of irreversible production failure.

Applicability

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

Implementation guidance

- Prefer expand-and-contract changes.
- Avoid long blocking operations without explicit impact control.
- Test mixed-version clients.
- Record irreversible transformations.

Required evidence

- Migration plan and scripts
- Scale and compatibility tests
- Reconciliation and rollback evidence

Assessment procedure

- **Examine:** Interrupt and resume a migration.
- **Interview:** Run old and new clients concurrently.
- **Test:** Verify data invariants.

Exceptions and compensating controls

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

External mappings

- NIST SP 800-53 — CM-3 and SI-7

NORMATIVE CONTROL

MYTHOS-FND-DAI-16 – Versioning, compatibility, and deprecation

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

Requirement

Interfaces and schemas MUST have a documented versioning and compatibility policy, supported-version window, deprecation notice, migration path, consumer discovery, and retirement verification.

Purpose

Allows evolution without surprise breakage or indefinite support burden.

Applicability

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

Implementation guidance

- Differentiate additive, behavior-changing, and breaking changes.
- Measure actual use before retirement.
- Keep security fixes possible within support windows.

Required evidence

- Version policy
- Consumer and usage records
- Deprecation and retirement evidence

Assessment procedure

- **Examine:** Test a compatibility claim.
- **Interview:** Identify unknown consumers.
- **Test:** Verify retired versions no longer receive traffic.

Exceptions and compensating controls

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

External mappings

- OpenAPI 3.2.1
- AsyncAPI 3.1.0

NORMATIVE CONTROL

MYTHOS-FND-DAI-17 – Third-party integration boundary control

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

Requirement

Third-party integrations MUST be treated as untrusted and failure-prone boundaries with explicit data disclosure, identity, rate, retention, contract, security, privacy, availability, observability, incident, and exit requirements.

Purpose

Contains external risk and prevents supplier behavior from becoming implicit system policy.

Applicability

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

Implementation guidance

- Use provider adapters or anti-corruption layers for critical dependencies.
- Validate responses and signatures.
- Document provider data use and subprocessor implications.
- Maintain replacement or degraded-mode plans.

Required evidence

- Provider assessment
- Integration boundary design
- Exit and failure tests

Assessment procedure

- **Examine:** Return malformed or malicious provider data.
- **Interview:** Disable the provider.
- **Test:** Verify data disclosure matches approval.

Exceptions and compensating controls

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

External mappings

- NIST SP 800-161 Rev. 1

NORMATIVE CONTROL

MYTHOS-FND-DAI-18 – Contract, compatibility, and failure testing

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

Requirement

Data and integration changes MUST pass automated contract, schema, authorization, compatibility, idempotency, concurrency, performance, and failure-path tests appropriate to risk before promotion.

Purpose

Turns interface expectations into enforceable evidence.

Applicability

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

Implementation guidance

- Run provider and consumer tests.
- Use malformed, boundary, delayed, duplicated, and out-of-order inputs.
- Preserve representative fixtures without exposing sensitive data.

Required evidence

- Test suites
- Compatibility matrix
- Failure evidence

Assessment procedure

- **Examine:** Introduce a breaking schema change.
- **Interview:** Replay duplicate and reordered messages.
- **Test:** Attempt unauthorized resource access.

Exceptions and compensating controls

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

External mappings

- NIST SSDF v1.1
- OpenAPI 3.2.1

NORMATIVE CONTROL

MYTHOS-FND-DAI-19 – Discoverable interface documentation

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

Requirement

Consumers MUST have access to current interface and data documentation covering purpose, authentication, authorization, contracts, examples, limits, errors, operational expectations, versioning, deprecation, support, and known limitations.

Purpose

Reduces unsafe reverse engineering and inconsistent consumer behavior.

Applicability

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

Implementation guidance

- Generate documentation from authoritative contracts where practical.
- Validate examples.
- Separate public, partner, and internal access while preserving required operational knowledge.

Required evidence

- Developer portal or documentation
- Example validation results
- Support and change records

Assessment procedure

- **Examine:** Complete a representative integration from documentation.
- **Interview:** Verify examples compile or validate.
- **Test:** Check superseded versions are clearly labeled.

Exceptions and compensating controls

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

External mappings

- ISO/IEC/IEEE 26514:2022

FOUNDATION STANDARD / STRUCTURAL PART

Part V – Implementation and Operations

24. Implementation Profiles

Profile	Required Operating State
Baseline	Owned data and APIs, classification, versioned contracts, identity, idempotency, errors, limits, observability, migration, compatibility, and documentation.
Enterprise	Central schema registry, automated contract testing, event governance, lineage, policy enforcement, reconciliation, consumer analytics, and managed third-party gateways.
High Assurance	Cryptographic message integrity, formal compatibility analysis, deterministic replay, independently tested failure semantics, strict tenant isolation, signed contracts, and continuous reconciliation.

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

25. Implementation Lifecycle

25.1 Establish

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

25.2 Baseline

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

25.3 Implement

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

25.4 Assure

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

25.5 Operate and Improve

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

26. Integration Requirements

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

27. Failure Handling and Recovery

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

28. Exceptions and Compensating Controls

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

29. Prohibited Practices

- Using documentation examples as the only contract
- Retries without idempotency analysis
- Returning generic errors without machine-readable cause
- Assuming exactly-once delivery without an effect strategy
- Embedding tenant identity only in request payload
- Changing schemas in place without compatibility testing
- Integrating third parties without exit or degraded-mode design

30. Adoption Roadmap from Source Draft

- Establish ownership, classification, data contracts, interface inventory, and authoritative schemas.
- Standardize API, event, error, authorization, versioning, and reliability behaviors.
- Add lineage, quality objectives, observability, migration, retention, and third-party resilience.
- Automate contract generation, validation, compatibility testing, policy enforcement, and deprecation monitoring.
- For High Assurance, add integrity protection, replay testing, fault injection, independent contract review, and continuous data reconciliation.

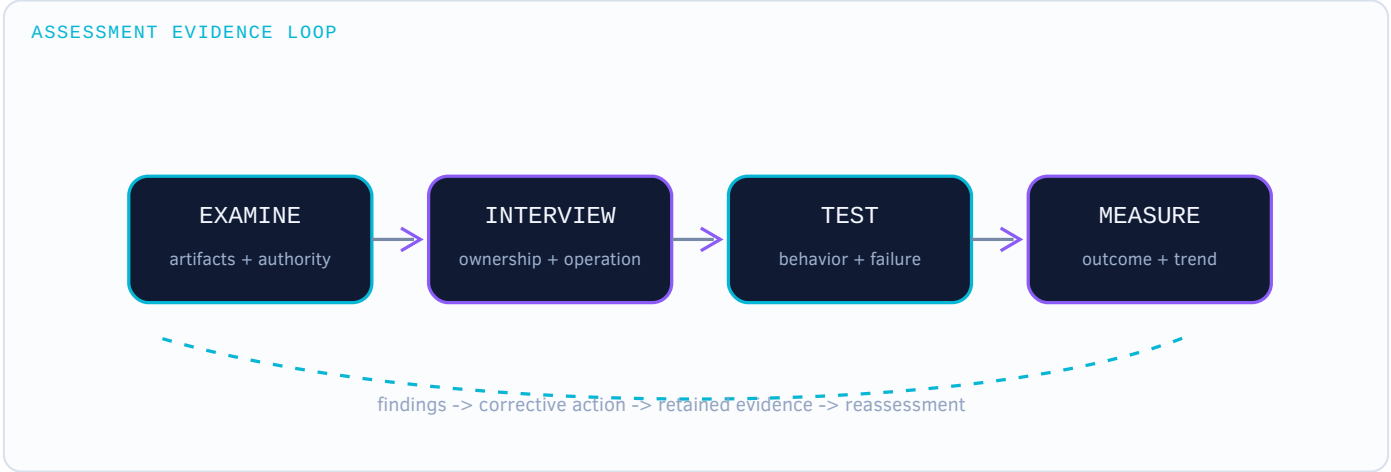
31. Limitations and Residual Risk from Source Draft

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

FOUNDATION STANDARD / STRUCTURAL PART

Part VI – Assurance and Assessment

32. Assessment Methodology



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

12.1 Finding States

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

12.2 Conformance

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

33. Metrics and Reporting from Source Draft

Metric	Definition	Expected use or target
Contract coverage	Production integrations represented by current versioned contracts	100% material integrations
	Undeclared incompatible changes reaching consumers	0

Metric	Definition	Expected use or target
Breaking-change escape rate		
Data quality objective attainment	Critical data products meeting defined quality objectives	Within approved thresholds
Integration recovery rate	Failed operations safely retried, reconciled, or compensated	Risk-defined; all critical paths tested
Lineage completeness	Critical fields and derived artifacts with source and transformation lineage	>= 95% Advanced; 100% selected High Assurance scope

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

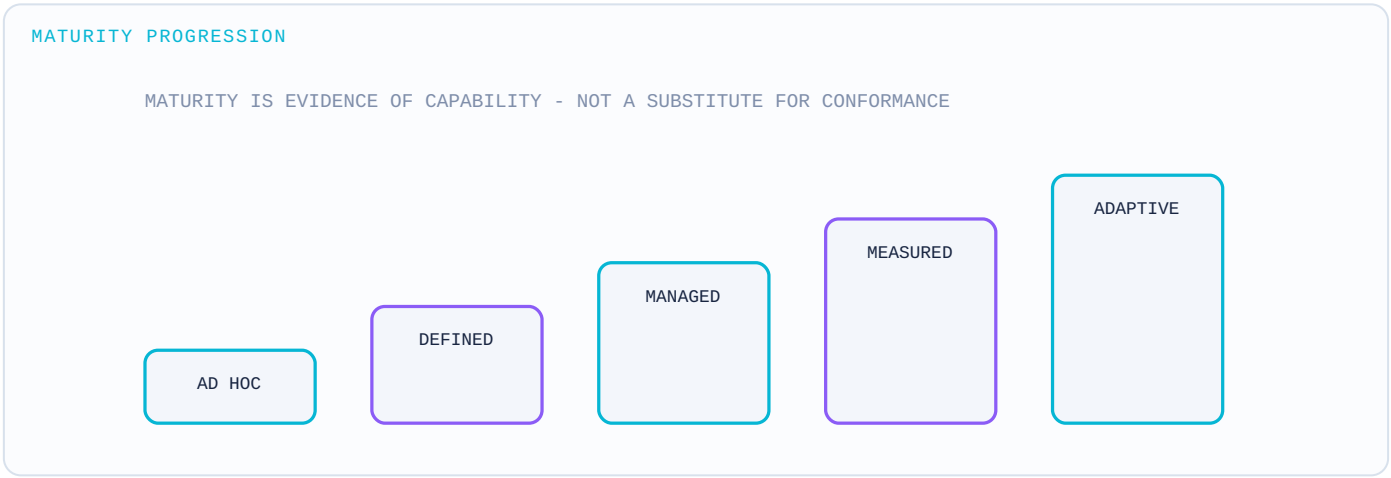
34. Exceptions and Compensating Controls

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

35. Enterprise Metric Set

Metric	Measurement Requirement
interfaces with current owner and contract	Defined by the adopting organization with owner, source, target, and cadence.
breaking changes without approved migration	Defined by the adopting organization with owner, source, target, and cadence.
duplicate-effect incidents	Defined by the adopting organization with owner, source, target, and cadence.
requests ending indeterminate without reconciliation	Defined by the adopting organization with owner, source, target, and cadence.
schema validation failures	Defined by the adopting organization with owner, source, target, and cadence.
consumer versions beyond support window	Defined by the adopting organization with owner, source, target, and cadence.
third-party errors and quota saturation	Defined by the adopting organization with owner, source, target, and cadence.
data quality objectives outside target	Defined by the adopting organization with owner, source, target, and cadence.
events without lineage or correlation	Defined by the adopting organization with owner, source, target, and cadence.

36. Maturity Model



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

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

37. Assessment Confidence

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

38. Executive Assurance Dashboard

The executive report SHOULD present:

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

- corrective-action status.

FOUNDATION STANDARD / STRUCTURAL PART

Part VII – Authority and Traceability

39. Cross-Standard Dependencies from Source Draft

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

40. Current External Authority Register

Authority	Relevance	Official Location	Status	Validated
OpenAPI Specification 3.2.1	Language-agnostic HTTP API description	https://spec.openapis.org/oas/v3.2.1.html	Current 3.2 patch release	2026-09-17
JSON Schema 2020-12	JSON structure and validation	https://json-schema.org/draft/2020-12	Current published dialect	2026-09-17
RFC 9110	HTTP Semantics	https://www.rfc-editor.org/rfc/rfc9110	Internet Standard	2026-09-17
RFC 9457	Problem Details for HTTP APIs	https://www.rfc-editor.org/info/rfc9457/	Proposed Standard	2026-09-17
RFC 9421	HTTP Message Signatures	https://www.rfc-editor.org/info/rfc9421/	Proposed Standard	2026-09-17
RFC 9530	Digest Fields	https://www.rfc-editor.org/info/rfc9530/	Proposed Standard	2026-09-17
CloudEvents 1.0.2	Event envelope specification	https://github.com/cloudevents/spec/blob/v1.0.2/cloudevents/spec.md	Released	2026-09-17

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

41. Control Traceability

Each control MUST remain traceable to:

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

- related Foundation controls.

42. Source-Draft Preservation

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

FOUNDATION STANDARD / STRUCTURAL PART

Part VIII – Appendices

Appendix A – Source-Draft Evolution Notes

- Preserves the source draft's contract-first approach, provider abstraction, repository and data-store guidance, migration safety, and explicit integration boundaries.
- Generalizes database- and framework-specific prescriptions into outcome-based controls.
- Adds event semantics, idempotency, backpressure, lineage, deprecation telemetry, and third-party containment.
- Aligns API documentation with current OpenAPI, JSON Schema, AsyncAPI, and CloudEvents specifications.

Appendix B – Change History

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

Appendix C – Control Summary

Control	Family	Title	Profiles	Automation	Impact
MYTHOS-FND-DAI-01	Governance	Data and integration ownership	Foundational, Advanced, High Assurance	High	Critical
MYTHOS-FND-DAI-02	Classification	Data classification and permitted use	Foundational, Advanced, High Assurance	High	Critical
MYTHOS-FND-DAI-03	Contracts	Versioned data contracts	Foundational, Advanced, High Assurance	High	Critical
MYTHOS-FND-DAI-04	API design	Consistent resource and operation design	Foundational, Advanced, High Assurance	High	Critical
MYTHOS-FND-DAI-05	Authorization	Identity, authorization, and tenant context	Foundational, Advanced, High Assurance	High	Critical
MYTHOS-FND-DAI-06	Reliability	Idempotency and duplicate-effect control	Foundational, Advanced, High Assurance	High	Critical
MYTHOS-FND-DAI-07	Concurrency	Concurrency, ordering, and consistency	Foundational, Advanced, High Assurance	Partial	Critical
MYTHOS-FND-DAI-08	Errors	Structured errors and failure semantics	Foundational, Advanced, High Assurance	High	Material
MYTHOS-FND-DAI-09	Flow control	Rate limits, quotas, backpressure, and admission control	Foundational, Advanced, High Assurance	High	Critical
MYTHOS-FND-DAI-10	Events	Event and messaging semantics	Foundational, Advanced, High Assurance	High	Critical

Control	Family	Title	Profiles	Automation	Impact
MYTHOS-FND-DAI-11	Quality	Data quality objectives and controls	Foundational, Advanced, High Assurance	High	Critical
MYTHOS-FND-DAI-12	Lineage	Lineage, provenance, and transformation accountability	Advanced, High Assurance	High	Critical
MYTHOS-FND-DAI-13	Observability	Integration observability and reconciliation	Foundational, Advanced, High Assurance	High	Critical
MYTHOS-FND-DAI-14	Resilience	Dependency failure and retry control	Foundational, Advanced, High Assurance	Partial	Critical
MYTHOS-FND-DAI-15	Migrations	Schema and data migration safety	Foundational, Advanced, High Assurance	High	Critical
MYTHOS-FND-DAI-16	Lifecycle	Versioning, compatibility, and deprecation	Foundational, Advanced, High Assurance	High	Critical
MYTHOS-FND-DAI-17	Third parties	Third-party integration boundary control	Foundational, Advanced, High Assurance	Partial	Critical
MYTHOS-FND-DAI-18	Testing	Contract, compatibility, and failure testing	Foundational, Advanced, High Assurance	High	Critical
MYTHOS-FND-DAI-19	Documentation	Discoverable interface documentation	Foundational, Advanced, High Assurance	Partial	Material

Appendix D – Minimum Conformance Claim Record

```
standard: MYTHOS-FND-0006
version: 0.2.0
profile: foundational | advanced | high_assurance
scope: <bounded systems, teams, environments, and processes>
assessment_period: <start/end>
assessor: <person or independent body>
tailoring_decisions: []
exceptions: []
findings_summary:
  satisfied: 0
  partially_satisfied: 0
  not_satisfied: 0
  not_applicable: 0
  not_assessed: 0
residual_risk_owner: <accountable role>
approval: <record reference>
```

Appendix E – Publication Review Checklist

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

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