CANDIDATE STANDARD

Mythos Interface Standards

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

PERMANENT ID
MYTHOS-FND-0007

PUBLICATION CLASS
CANDIDATE STANDARD

VERSION / STATUS
1.0.0-candidate / CANDIDATE

PERMANENT PUBLICATION IDENTITY

Mythos Interface Standards

Universal Requirements for Human Interfaces, Administrative Surfaces, Accessibility, Safety, Feedback, and Trustworthy Interaction

Document ID
MYTHOS-FND-0007

Version
1.0.0-candidate

Status
Candidate Standard

Review date
2027-09-17

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

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

Reader orientation

Dimension	Engineering position
Primary domain	Foundation and Governance
Audience	Product and interface designers; Frontend and platform engineers; Accessibility and quality specialists; Security and privacy teams; Operators, administrators, and assessors
Publisher / owner	Mythos Systems / Standards Program
Public classification	Public technical standard
Canonical route	/library/standards/foundation/mythos-fnd-0007/

Expected outcomes

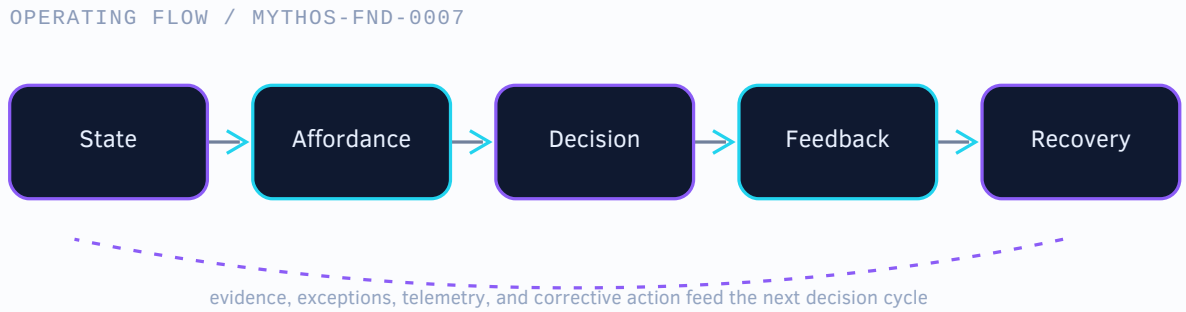
- Make interfaces understandable, accessible, predictable, and safe.
- Prevent visual design from obscuring authority, risk, system state, or irreversible consequences.
- Establish assessable requirements for administrative, operational, consumer, and AI-mediated interfaces.
- Ensure interaction design remains effective under failure, latency, degraded connectivity, and assistive technology.

SOURCE / FRESHNESS POSITION

Authority and source posture

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

FOUNDATION OPERATING DOCTRINE



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

NAVIGATION

Contents

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

NORMATIVE SYSTEM

Control index

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

Document Control

Field	Value
Document ID	MYTHOS-FND-0007
Standard	Interface Standards
Version	1.0.0-candidate
Status	Candidate Standard
Classification	Public
Publisher	Mythos Systems
Program	Mythos Engineering Standards Program
Accountable Owner	Mythos Systems Standards Program
Technical Review	Required
Source and Citation Review	Required
Assessment Review	Required
Accessibility and Publication Review	Required
Supersedes	No published edition; evolves source draft 0.2.0
Next Review	2027-09-17 or earlier on trigger

Revision Record

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

How to Use This Standard

Executive Reading Path

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

Engineering Reading Path

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

Assessment Reading Path

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

Normative and Informative Content

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

FOUNDATION STANDARD / STRUCTURAL PART

Part I – Executive Direction

1. Executive Overview

Interfaces are operational control surfaces. Ambiguous state, hidden scope, inaccessible interaction, unsafe confirmation, or misleading AI presentation can cause the same level of harm as backend defects. This standard defines interfaces as part of the system safety and trust architecture, with particular attention to critical actions, state authority, recovery, accessibility, privacy, degraded behavior, and AI-generated content.

The institutional objective is to establish safe, accessible, comprehensible, responsive, privacy-respecting, and auditable human-system interfaces across ordinary, degraded, critical, and AI-assisted workflows. Adoption should produce a controlled operating state in which leadership can understand the material risks, engineering teams can act on explicit requirements, assessors can test implementation and operating effectiveness, and the organization can support every conformance or trust claim with current evidence.

2. Executive Findings and Required Direction

Finding	Enterprise Exposure	Required Direction
Ambiguous state	Users cannot tell whether work is proposed, approved, executing, verified, failed, or unknown.	Present authoritative state and its source without relying on color alone.
Unsafe critical actions	Generic confirmation and hidden scope cause destructive mistakes.	Show identity, environment, target, effect, reversibility, and exact action.
Accessibility deferred	Interfaces exclude users and create operational risk when accessibility is treated as polish.	Apply accessibility requirements from design through representative validation.
Recovery omitted	Users cannot cancel, undo, resume, or understand partial completion.	Design cancellation, undo, recovery, and indeterminate states explicitly.
AI presented as authority	Generated suggestions are visually indistinguishable from system facts or executed outcomes.	Label AI content, sources, uncertainty, action boundaries, and verification.

3. Business and Operational Impact

3.1 Strategic Impact

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

3.2 Delivery and Cost Impact

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

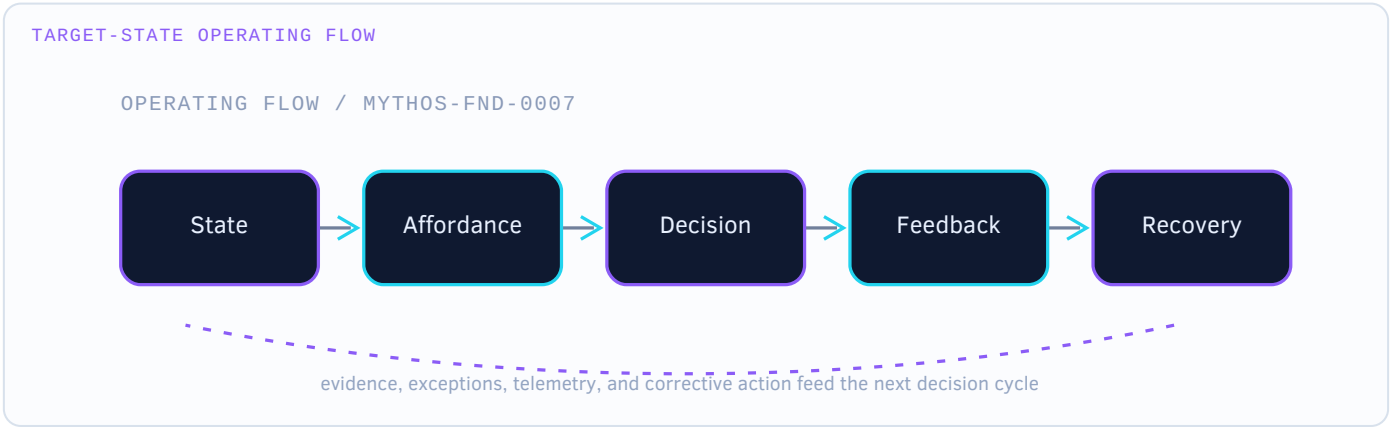
3.3 Security, Privacy, and Trust Impact

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

3.4 Workforce and Organizational Impact

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

4. Target-State Summary



The target state contains the following institutional components:

#	Target-State Component
1	Interface ownership and critical-flow inventory
2	Authoritative state model
3	Identity, scope, and environment context
4	Critical-action safety
5	Undo, cancellation, and recovery
6	Accessibility baseline
7	Validation and constraints
8	Feedback and progress
9	Safe error communication
10	Privacy and sensitive-data handling
11	Consistent interaction semantics
12	Performance and responsiveness
13	Degraded and offline behavior
14	AI output and action boundaries

#	Target-State Component
15	Locale, language, time, and units
16	Interaction auditability
17	Representative validation

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

5. Leadership Responsibilities

Role	Accountability
Product owner	Owns user outcomes and critical workflow inventory.
Design authority	Owns interaction principles, consistency, and design system.
Accessibility lead	Defines accessibility requirements and representative evaluation.
Security and privacy lead	Reviews critical actions, sensitive data, identity, and disclosure.
Frontend engineering	Implements state, performance, keyboard, assistive technology, and error behavior.
Operations representative	Validates operational and degraded workflows.
User research lead	Validates with representative users and contexts.
Independent assessor	Tests accessibility, safety, and evidence.

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

FOUNDATION STANDARD / STRUCTURAL PART

Part II – Standard Foundation

6. Purpose and Objectives

- Make interfaces understandable, accessible, predictable, and safe.
- Prevent visual design from obscuring authority, risk, system state, or irreversible consequences.
- Establish assessable requirements for administrative, operational, consumer, and AI-mediated interfaces.
- Ensure interaction design remains effective under failure, latency, degraded connectivity, and assistive technology.

7. Scope

Applies to graphical, command-line, conversational, voice, immersive, embedded, mobile, desktop, web, and machine-assisted human interfaces. It includes setup, operations, administration, approval, recovery, support, and decommissioning workflows.

8. Intended Audience

- Product and interface designers
- Frontend and platform engineers
- Accessibility and quality specialists
- Security and privacy teams
- Operators, administrators, and assessors

9. Requirements Language and Conformance

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

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

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

10. Normative References from Source Draft

- **RFC 2119** — Key words for use in RFCs to Indicate Requirement Levels. https://www.rfc-editor.org/rfc/rfc2119

- **RFC 8174** — Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words. https://www.rfc-editor.org/rfc/rfc8174
- **MYTHOS-GOV-0001** — Mythos Engineering Standards Authoring and Benchmark Framework, Version 0.1.0. ../governance/01_MYTHOS_STANDARDS_AUTHORING_AND_BENCHMARK_FRAMEWORK.md

11. Informative References from Source Draft

- **W3C WCAG 2.2** — Web Content Accessibility Guidelines 2.2. https://www.w3.org/TR/WCAG22/
- **W3C WAI-ARIA 1.2** — Accessible Rich Internet Applications 1.2. https://www.w3.org/TR/wai-aria-1.2/
- **ISO/IEC 25010:2023** — Systems and software Quality Requirements and Evaluation — Product quality model. https://www.iso.org/standard/78176.html
- **NIST SP 800-53 Rev. 5, Release 5.2.0** — Security and Privacy Controls for Information Systems and Organizations. https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final
- **NIST Privacy Framework 1.0** — A Tool for Improving Privacy through Enterprise Risk Management. https://www.nist.gov/privacy-framework/privacy-framework

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

12. Terms and Definitions

Term	Definition
Accountable owner	The person or formally delegated role that accepts responsibility for an outcome, decision, control, or risk.
Assessment object	The system, process, component, artifact, team, service, or organizational scope being evaluated.
Compensating control	An alternative safeguard that provides comparable risk reduction when the specified control cannot be implemented as written.
Conformance claim	A bounded statement that an identified scope satisfies the applicable requirements of a named standard version and assurance profile.
Evidence	Reviewable information that supports a conclusion about design, implementation, operation, or control effectiveness.
High Assurance	The cumulative profile requiring stronger independence, adversarial testing, continuous verification, or formal evidence where risk warrants it.
Residual risk	Risk remaining after controls, mitigations, and compensating measures are applied.
System	A product, service, application, platform, workflow, integration, operational capability, or combined socio-technical environment.
Tailoring	A documented decision to include, strengthen, parameterize, or mark a control not applicable based on scope and risk.
Critical action	An action that can cause material loss, exposure, outage, irreversible change, legal effect, or significant user harm.
System state	The authoritative condition of a system, operation, resource, or workflow at a point in time.
Progressive disclosure	Presentation of essential information first, with additional complexity available when needed.
Interaction evidence	Records demonstrating that a user was shown relevant information, possessed required authority, and completed or declined an action.

13. Applicability and Tailoring

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

FOUNDATION STANDARD / STRUCTURAL PART

Part III – Risk and Architecture

14. Enterprise Problem and Risk Landscape

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

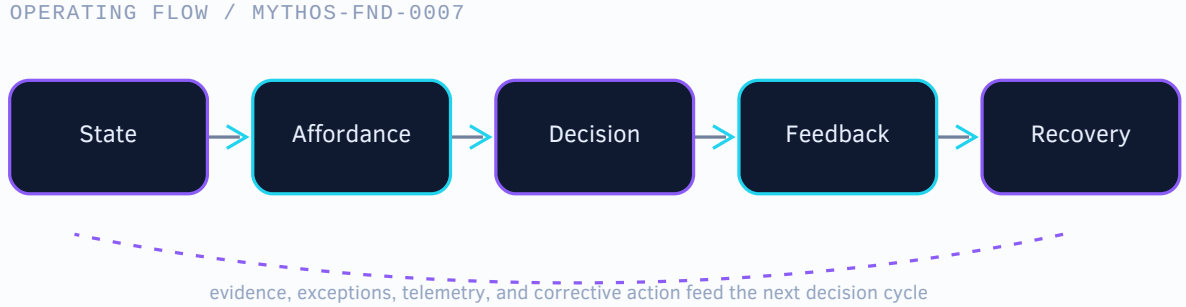
Adopting organizations SHOULD maintain a domain-specific risk register that identifies cause, affected asset or stakeholder, credible scenario, impact, existing controls, residual risk, owner, review trigger, and evidence. Risks that cross standards MUST be linked rather than copied into disconnected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

15. Governing Principles

- Clarity outranks ornament when consequences are material.
- State, authority, scope, and consequence must be visible before commitment.
- Accessibility is a design constraint, not a post-release accommodation.
- Errors should be prevented where practical and recoverable where prevention is impossible.
- The interface must not claim success before authoritative completion.
- High-consequence automation requires meaningful human control or explicitly approved autonomous authority.

16. Reference Operating Architecture

REFERENCE OPERATING ARCHITECTURE



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

16.1 Control Plane

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

16.2 Delivery and Enforcement Plane

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

16.3 Evidence and Assurance Plane

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

16.4 Feedback Plane

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

17. Roles and Accountability

Role	Accountability
Product owner	Owns user outcomes and critical workflow inventory.
Design authority	Owns interaction principles, consistency, and design system.
Accessibility lead	Defines accessibility requirements and representative evaluation.
Security and privacy lead	Reviews critical actions, sensitive data, identity, and disclosure.
Frontend engineering	Implements state, performance, keyboard, assistive technology, and error behavior.
Operations representative	Validates operational and degraded workflows.
User research lead	Validates with representative users and contexts.
Independent assessor	Tests accessibility, safety, and evidence.

18. State, Evidence, and Decision Model

The adopting organization MUST distinguish:

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

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

19. Security and Trust Considerations

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

20. Failure Modes

Failure or Anti-Pattern	Enterprise Consequence
Generic approve or delete buttons without scope	Failure can create hidden risk, misleading assurance, uncontrolled cost, or unsafe operation.
Using color as the only status signal	Failure can create hidden risk, misleading assurance, uncontrolled cost, or unsafe operation.
Hiding errors behind friendly but non-actionable language	Failure can create hidden risk, misleading assurance, uncontrolled cost, or unsafe operation.
Automatic destructive actions from AI suggestions	Failure can create hidden risk, misleading assurance, uncontrolled cost, or unsafe operation.
Modal confirmations that repeat no new information	Failure can create hidden risk, misleading assurance, uncontrolled cost, or unsafe operation.
Inaccessible custom controls	Failure can create hidden risk, misleading assurance, uncontrolled cost, or unsafe operation.
Infinite loading states without timeout or recovery	Failure can create hidden risk, misleading assurance, uncontrolled cost, or unsafe operation.

21. Cross-Functional Dependencies

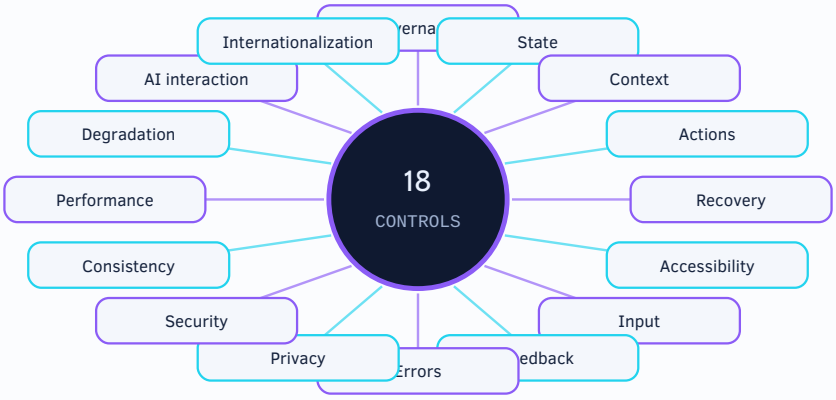
This Foundation standard depends on the remaining MYTHOS-FND standards for documentation, security and trust, quality, operations, data and integration, interfaces, extensions, AI-first behavior, and agentic orchestration. An adopting organization MUST resolve overlapping requirements through the stricter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

FOUNDATION STANDARD / STRUCTURAL PART

Part IV – Normative Control System

22. Control-Family Overview

CONTROL-FAMILY CONSTELLATION



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

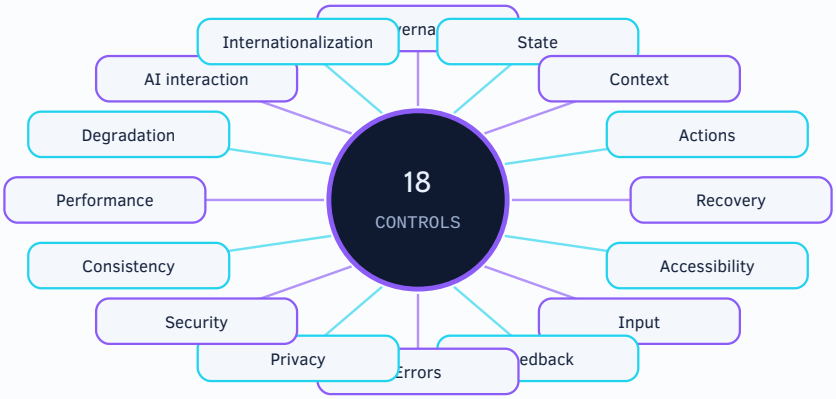
- Governance
- State
- Context
- Actions
- Recovery
- Accessibility
- Input
- Feedback
- Errors
- Privacy
- Security
- Consistency
- Performance
- Degradation
- AI interaction
- Internationalization
- Evidence
- Testing

23. Normative Controls

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

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

NORMATIVE CONTROL CONSTELLATION



NORMATIVE CONTROL

MYTHOS-FND-UI-01 – Interface ownership and critical-flow inventory

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

Requirement

The organization MUST assign accountable owners for each material interface and maintain an inventory of critical user journeys, supported modalities, user populations, risk classifications, and authoritative backend dependencies.

Purpose

Creates ownership and ensures high-risk interactions receive proportionate review.

Applicability

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

Implementation guidance

- Classify administrative and irreversible actions.
- Record supported assistive technologies and locales.

Required evidence

- Interface inventory
- Critical-flow register
- Ownership records

Assessment procedure

- **Examine:** Sample interfaces against the inventory.
- **Interview:** Interview owners.
- **Test:** Identify an unregistered critical flow.

Exceptions and compensating controls

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

External mappings

- ISO/IEC 25010:2023

NORMATIVE CONTROL

MYTHOS-FND-UI-02 – Authoritative and unambiguous system state

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

Requirement

Interfaces MUST present current, pending, failed, degraded, stale, and completed states distinctly and MUST NOT represent an operation as successful before authoritative confirmation.

Purpose

Prevents false confidence and unsafe follow-on action.

Applicability

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

Implementation guidance

- Use correlation identifiers for long-running actions.
- Show data freshness and source where material.

Required evidence

- State model
- UI tests
- Telemetry

Assessment procedure

- **Examine:** Inject delayed and failed operations.
- **Interview:** Verify stale data indicators.
- **Test:** Exercise the requirement.

Exceptions and compensating controls

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

External mappings

- NIST SP 800-53 — AU and SI families

NORMATIVE CONTROL

MYTHOS-FND-UI-03 – Scope, identity, and environment visibility

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

Requirement

Before a material action, the interface MUST display the acting identity, target scope, tenant or trust domain, environment, affected resources, and effective privilege when confusion could cause harm.

Purpose

Reduces wrong-target, wrong-environment, and confused-deputy errors.

Applicability

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

Implementation guidance

- Use persistent production indicators.
- Show inherited or delegated authority.

Required evidence

- Context design
- Critical-action screenshots
- Tests

Assessment procedure

- **Examine:** Switch tenants or environments.
- **Interview:** Verify context remains visible through confirmation.
- **Test:** Exercise the requirement.

Exceptions and compensating controls

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

External mappings

- NIST SP 800-53 — AC-6

NORMATIVE CONTROL

MYTHOS-FND-UI-04 – Safe critical-action design

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

Requirement

Critical actions MUST require explicit intent, validate preconditions and authority, disclose material consequences, and provide preview, confirmation, approval, delay, rollback, or equivalent safeguards proportionate to risk.

Purpose

Prevents accidental or unauthorized high-impact change.

Applicability

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

Implementation guidance

- Avoid generic confirmation text.
- Require typed or scoped confirmation only where it adds meaningful friction.

Required evidence

- Action classification
- Safeguard rules
- Test evidence

Assessment procedure

- **Examine:** Attempt action with failed preconditions.
- **Interview:** Verify confirmation reflects exact scope.
- **Test:** Exercise the requirement.

Exceptions and compensating controls

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

External mappings

- NIST SP 800-53 — CM-3

NORMATIVE CONTROL

MYTHOS-FND-UI-05 – Undo, cancellation, and recovery

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

Requirement

Interfaces MUST expose cancellation, retry, rollback, compensation, support, or recovery paths for recoverable failures and MUST clearly identify irreversible operations before commitment.

Purpose

Limits impact when mistakes or failures occur.

Applicability

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

Implementation guidance

- Preserve user input where safe.
- Explain partial success.

Required evidence

- Recovery design
- Failure tests
- Support procedures

Assessment procedure

- **Examine:** Interrupt representative workflows.
- **Interview:** Verify partial effects are reconciled.
- **Test:** Exercise the requirement.

Exceptions and compensating controls

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

External mappings

- ISO/IEC 25010:2023 — reliability

NORMATIVE CONTROL

MYTHOS-FND-UI-06 – Accessibility baseline

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

Requirement

Interfaces MUST satisfy applicable WCAG 2.2 Level AA requirements and MUST support keyboard operation, semantic structure, focus visibility, readable contrast, non-color cues, scalable text, and assistive-technology interpretation for critical workflows.

Purpose

Ensures equitable and reliable access.

Applicability

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

Implementation guidance

- Document exceptions by platform limitation.
- Test with representative assistive technologies.

Required evidence

- Accessibility report
- Automated scans
- Manual test records

Assessment procedure

- **Examine:** Perform keyboard-only and screen-reader tests.
- **Interview:** Check zoom and contrast.
- **Test:** Exercise the requirement.

Exceptions and compensating controls

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

External mappings

- WCAG 2.2
- WAI-ARIA 1.2

NORMATIVE CONTROL

MYTHOS-FND-UI-07 – Input validation and constraint communication

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

Requirement

Interfaces MUST validate inputs as early as practical, preserve authoritative server-side validation, explain constraints, reject ambiguous values, and prevent unsafe defaults.

Purpose

Reduces malformed, unintended, and insecure requests.

Applicability

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

Implementation guidance

- Use units and formats explicitly.
- Do not rely on placeholders as labels.

Required evidence

- Validation rules
- Negative tests
- Error catalog

Assessment procedure

- **Examine:** Submit boundary, malformed, and conflicting inputs.
- **Interview:** Bypass client validation.
- **Test:** Exercise the requirement.

Exceptions and compensating controls

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

External mappings

- OWASP ASVS

NORMATIVE CONTROL

MYTHOS-FND-UI-08 – Timely and actionable feedback

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

Requirement

Interfaces MUST provide feedback for accepted input, processing, completion, failure, conflict, timeout, throttling, and recovery, with actionable next steps and correlation where support may be required.

Purpose

Maintains user control and enables diagnosis.

Applicability

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

Implementation guidance

- Avoid indefinite spinners.
- Distinguish retryable from permanent failures.

Required evidence

- Feedback catalog
- Latency tests
- Support records

Assessment procedure

- **Examine:** Simulate each major outcome.
- **Interview:** Measure announcement to assistive technology.
- **Test:** Exercise the requirement.

Exceptions and compensating controls

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

External mappings

- ISO/IEC 25010:2023

NORMATIVE CONTROL

MYTHOS-FND-UI-09 – Non-sensitive error communication

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

Requirement

User-facing errors MUST be specific enough to support safe correction while excluding secrets, internal topology, sensitive identifiers, stack traces, or exploitable implementation detail.

Purpose

Balances usability with confidentiality and security.

Applicability

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

Implementation guidance

- Log protected diagnostic detail with correlation.
- Localize without changing machine codes.

Required evidence

- Error catalog
- Redaction rules
- Tests

Assessment procedure

- **Examine:** Trigger internal failures.
- **Interview:** Inspect output and logs.
- **Test:** Exercise the requirement.

Exceptions and compensating controls

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

External mappings

- OWASP ASVS
- NIST SP 800-53 — SI-11

NORMATIVE CONTROL

MYTHOS-FND-UI-10 – Privacy-respecting interaction

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

Requirement

Interfaces MUST disclose material data collection and sharing at the point of interaction, minimize requested data, provide appropriate preference and consent controls, and avoid coercive or deceptive choice architecture.

Purpose

Protects autonomy and privacy.

Applicability

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

Implementation guidance

- Separate necessary processing from optional personalization.
- Make rejection no harder than acceptance where choice is genuine.

Required evidence

- Data-flow map
- Consent records
- UX review

Assessment procedure

- **Examine:** Trace collected fields to purpose.
- **Interview:** Test withdrawal or preference change.
- **Test:** Exercise the requirement.

Exceptions and compensating controls

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

External mappings

- NIST Privacy Framework 1.0

NORMATIVE CONTROL

MYTHOS-FND-UI-11 – Session and sensitive-data handling

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

Requirement

Interfaces MUST protect authentication state, secrets, sensitive values, clipboard use, cached data, screenshots, exports, and inactivity behavior according to risk and platform capability.

Purpose

Reduces exposure through the interaction layer.

Applicability

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

Implementation guidance

- Mask by default without making verification impossible.
- Clear sensitive transient state.

Required evidence

- Session policy
- Storage review
- Security tests

Assessment procedure

- **Examine:** Inspect local storage and caches.
- **Interview:** Test session expiry and reauthentication.
- **Test:** Exercise the requirement.

Exceptions and compensating controls

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

External mappings

- NIST SP 800-53 — IA and SC families

NORMATIVE CONTROL

MYTHOS-FND-UI-12 – Consistent interaction semantics

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

Requirement

Equivalent controls, terms, states, shortcuts, and navigation patterns SHOULD behave consistently across the product unless a documented safety or platform constraint requires variation.

Purpose

Reduces cognitive load and operational error.

Applicability

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

Implementation guidance

- Maintain a governed component and terminology system.
- Version breaking interaction changes.

Required evidence

- Design system
- Terminology register
- Regression tests

Assessment procedure

- **Examine:** Compare equivalent workflows.
- **Interview:** Review justified deviations.
- **Test:** Exercise the requirement.

Exceptions and compensating controls

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

External mappings

- ISO/IEC 25010:2023 — usability

NORMATIVE CONTROL

MYTHOS-FND-UI-13 – Perceived and actual responsiveness

FAMILY	PROFILES	FAILURE IMPACT	AUTOMATION POTENTIAL
Performance	Advanced, High Assurance	Material	High

Requirement

Critical workflows MUST define response, feedback, rendering, and completion objectives and MUST remain operable under expected latency, scale, and constrained-device conditions.

Purpose

Prevents latency from producing duplicate actions or abandonment.

Applicability

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

Implementation guidance

- Acknowledge input quickly while preserving true completion state.
- Budget client and server latency.

Required evidence

- Performance objectives
- Real-user telemetry
- Load tests

Assessment procedure

- **Examine:** Throttle network and CPU.
- **Interview:** Measure duplicate submissions.
- **Test:** Exercise the requirement.

Exceptions and compensating controls

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

External mappings

- ISO/IEC 25010:2023 — performance efficiency

NORMATIVE CONTROL

MYTHOS-FND-UI-14 – Degraded and offline behavior

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

Requirement

Interfaces MUST define behavior for unavailable dependencies, stale data, lost connectivity, partial permissions, and incompatible versions and MUST fail safely without concealing reduced capability.

Purpose

Maintains trust and safety under non-ideal conditions.

Applicability

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

Implementation guidance

- Disable actions that cannot be safely completed.
- Queue only when semantics and user expectations are explicit.

Required evidence

- Degradation design
- Failure tests
- User messaging

Assessment procedure

- **Examine:** Disconnect dependencies mid-workflow.
- **Interview:** Verify no false success.
- **Test:** Exercise the requirement.

Exceptions and compensating controls

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

External mappings

- ISO/IEC 25010:2023 — reliability

NORMATIVE CONTROL

MYTHOS-FND-UI-15 – AI-generated output and action boundaries

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

Requirement

Interfaces presenting AI-generated content or recommendations MUST identify material uncertainty, distinguish generated from authoritative information, expose relevant sources or evidence where available, and clearly separate recommendation from execution authority.

Purpose

Prevents automation bias and accidental delegation.

Applicability

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

Implementation guidance

- Show model or policy limitations in context.
- Require review for consequential actions unless autonomy is approved.

Required evidence

- AI interaction specification
- Evaluation results
- Action logs

Assessment procedure

- **Examine:** Present conflicting evidence.
- **Interview:** Attempt to execute from unverified output.
- **Test:** Exercise the requirement.

Exceptions and compensating controls

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

External mappings

- NIST AI RMF 1.0
- NIST AI 600-1

NORMATIVE CONTROL

MYTHOS-FND-UI-16 – Locale, language, time, and unit correctness

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

Requirement

Interfaces used across locales MUST represent language, names, addresses, numbers, currencies, units, time zones, dates, sorting, and text direction without ambiguous or lossy assumptions.

Purpose

Prevents operational and financial errors across regions.

Applicability

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

Implementation guidance

- Store canonical values separately from display forms.
- Display time zone for material timestamps.

Required evidence

- Locale matrix
- Translation records
- Tests

Assessment procedure

- **Examine:** Test boundary dates, RTL text, and unit changes.
- **Interview:** Verify round trips.
- **Test:** Exercise the requirement.

Exceptions and compensating controls

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

External mappings

- WCAG 2.2

NORMATIVE CONTROL

MYTHOS-FND-UI-17 – Interaction auditability

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

Requirement

Material approvals, administrative actions, policy changes, and irreversible operations MUST produce tamper-resistant records of actor, authority, target, request, presented context, decision, outcome, time, and correlation.

Purpose

Supports accountability, incident response, and dispute resolution.

Applicability

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

Implementation guidance

- Avoid logging sensitive content unnecessarily.
- Link UI evidence to backend execution evidence.

Required evidence

- Audit records
- Integrity controls
- Reconstruction tests

Assessment procedure

- **Examine:** Reconstruct a sampled action end to end.
- **Interview:** Attempt log alteration.
- **Test:** Exercise the requirement.

Exceptions and compensating controls

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

External mappings

- NIST SP 800-53 — AU family

NORMATIVE CONTROL

MYTHOS-FND-UI-18 – Representative interface validation

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

Requirement

Critical interfaces MUST be tested with representative users, assistive technologies, devices, browsers or runtimes, permissions, data conditions, failures, and adversarial misuse before release and after material change.

Purpose

Finds failures not visible in ideal-path automation.

Applicability

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

Implementation guidance

- Combine automated, expert, and user testing.
- Prioritize consequential and high-frequency flows.

Required evidence

- Test plan
- Participant and environment matrix
- Findings

Assessment procedure

- **Examine:** Review coverage against the inventory.
- **Interview:** Reproduce a closed high-severity finding.
- **Test:** Exercise the requirement.

Exceptions and compensating controls

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

External mappings

- WCAG 2.2
- ISO/IEC 25010:2023

FOUNDATION STANDARD / STRUCTURAL PART

Part V – Implementation and Operations

24. Implementation Profiles

Profile	Required Operating State
Baseline	Authoritative state, safe actions, accessible interaction, validation, feedback, privacy, recovery, responsive behavior, AI labeling, and representative testing.
Enterprise	Shared design system, automated accessibility and visual regression, critical-flow analytics, cross-product semantics, offline/degraded patterns, and auditable user action records.
High Assurance	Independent usability and accessibility validation, high-risk action simulation, formally reviewed state machines, multi-channel confirmation, assistive redundancy, and evidence-backed human-factors assurance.

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

25. Implementation Lifecycle

25.1 Establish

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

25.2 Baseline

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

25.3 Implement

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

25.4 Assure

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

25.5 Operate and Improve

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

26. Integration Requirements

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

27. Failure Handling and Recovery

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

28. Exceptions and Compensating Controls

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

29. Prohibited Practices

- Generic approve or delete buttons without scope
- Using color as the only status signal
- Hiding errors behind friendly but non-actionable language
- Automatic destructive actions from AI suggestions
- Modal confirmations that repeat no new information
- Inaccessible custom controls
- Infinite loading states without timeout or recovery

30. Adoption Roadmap from Source Draft

- Inventory interfaces and classify critical workflows.
- Establish an interaction-state model, design tokens, accessibility baseline, and critical-action pattern library.
- Instrument outcome, error, latency, abandonment, and recovery telemetry.
- Add independent accessibility and adversarial usability testing for Advanced adoption.
- Continuously validate critical workflows across supported devices, locales, input modes, and degraded conditions.

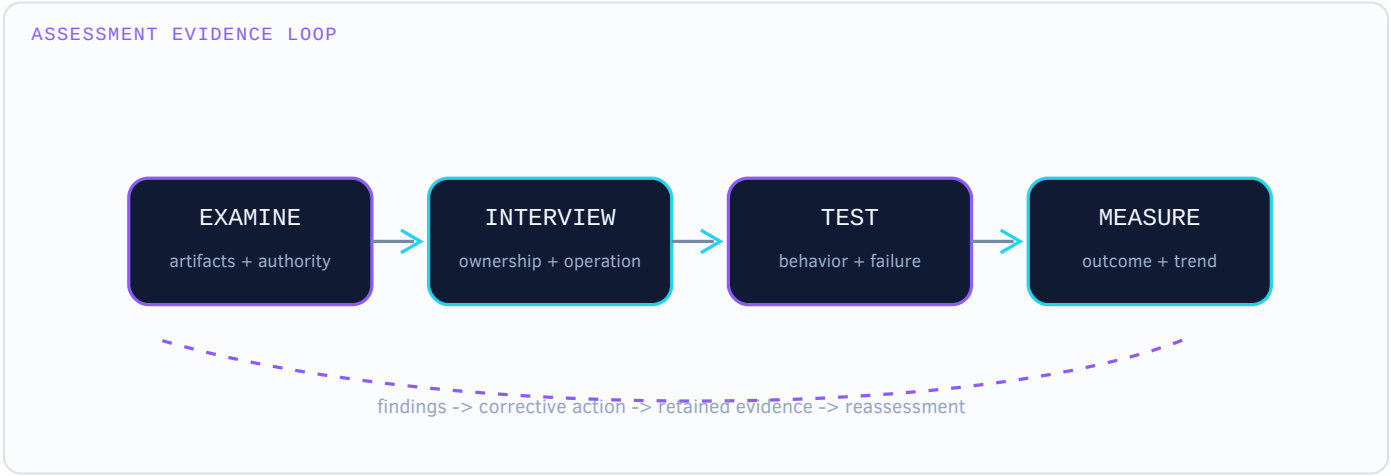
31. Limitations and Residual Risk from Source Draft

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

FOUNDATION STANDARD / STRUCTURAL PART

Part VI – Assurance and Assessment

32. Assessment Methodology



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

12.1 Finding States

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

12.2 Conformance

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

33. Metrics and Reporting from Source Draft

Metric	Definition	Expected use or target
Critical-flow completion	Successful completion of representative critical workflows without assistance	Target defined per user population and risk
	Applicable WCAG 2.2 success criteria satisfied	AA baseline; stronger criteria by profile

Metric	Definition	Expected use or target
Accessibility conformance		
False-success rate	Operations shown as complete before authoritative success	0 for critical actions
Recovery success	Users able to recover from injected errors	Measured for all critical workflows
Unsafe-action prevention	Material actions blocked or challenged when preconditions fail	100% of defined preconditions

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

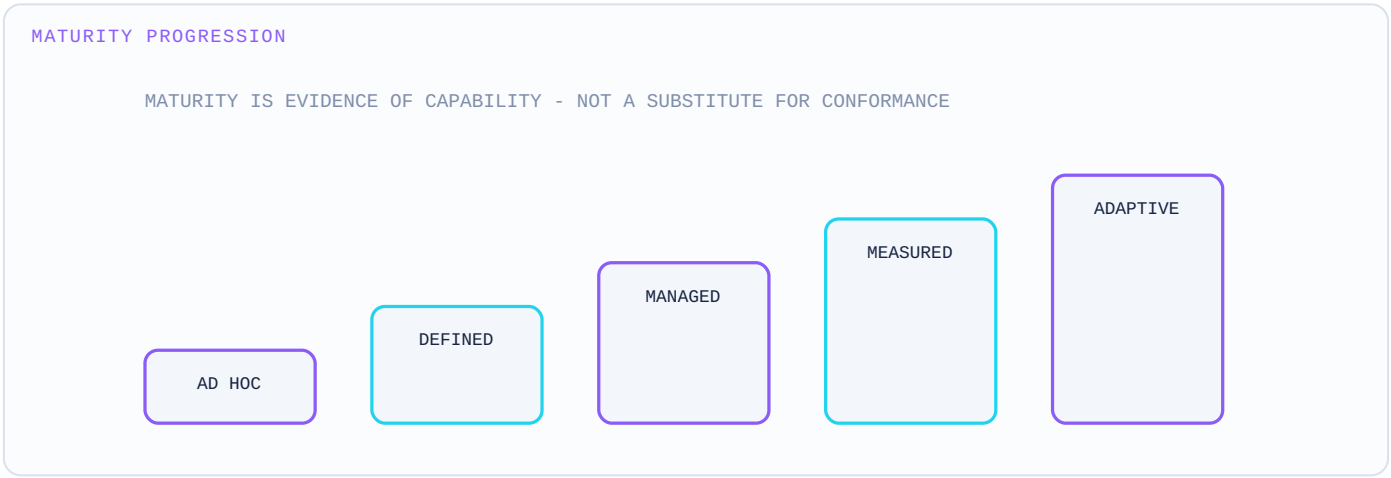
34. Exceptions and Compensating Controls

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

35. Enterprise Metric Set

Metric	Measurement Requirement
critical flows with current owner	Defined by the adopting organization with owner, source, target, and cadence.
WCAG 2.2 AA success criteria failures	Defined by the adopting organization with owner, source, target, and cadence.
critical actions with explicit scope and effect	Defined by the adopting organization with owner, source, target, and cadence.
user errors leading to rollback or incident	Defined by the adopting organization with owner, source, target, and cadence.
cancel and recovery success rate	Defined by the adopting organization with owner, source, target, and cadence.
unresolved accessibility defects	Defined by the adopting organization with owner, source, target, and cadence.
AI outputs without provenance or status label	Defined by the adopting organization with owner, source, target, and cadence.
p95 interaction and feedback latency	Defined by the adopting organization with owner, source, target, and cadence.
degraded-mode exercises passed	Defined by the adopting organization with owner, source, target, and cadence.

36. Maturity Model



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

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

37. Assessment Confidence

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

38. Executive Assurance Dashboard

The executive report SHOULD present:

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

- corrective-action status.

FOUNDATION STANDARD / STRUCTURAL PART

Part VII – Authority and Traceability

39. Cross-Standard Dependencies from Source Draft

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

40. Current External Authority Register

Authority	Relevance	Official Location	Status	Validated
WCAG 2.2	Web Content Accessibility Guidelines	https://www.w3.org/WAI/standards-guidelines/wcag/	W3C Recommendation	2026-09-17
WCAG-EM	Website Accessibility Conformance Evaluation Methodology	https://www.w3.org/WAI/test-evaluate/conformance/wcag-em/	W3C methodology	2026-09-17
WAI-ARIA 1.2	Accessible Rich Internet Applications	https://www.w3.org/TR/wai-aria-1.2/	W3C Recommendation	2026-09-17
ISO 9241-210:2019	Human-centred design for interactive systems	https://www.iso.org/standard/77520.html	Published	2026-09-17
EN 301 549 V3.2.1	Accessibility requirements for ICT products and services	https://www.etsi.org/deliver/etsi_en/301500_301599/301549/03.02.01_60/en_301549v030201p.pdf	Published	2026-09-17

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

41. Control Traceability

Each control MUST remain traceable to:

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

42. Source-Draft Preservation

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

FOUNDATION STANDARD / STRUCTURAL PART

Part VIII – Appendices

Appendix A – Source-Draft Evolution Notes

- Retains the source draft's broad interface coverage while removing aesthetic prescriptions from normative requirements.
- Converts design advice into testable controls centered on state, authority, consequence, accessibility, and recovery.
- Treats conversational and AI interfaces as interface modalities subject to the same trust requirements.

Appendix B – Change History

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

Appendix C – Control Summary

Control	Family	Title	Profiles	Automation	Impact
MYTHOS-FND-UI-01	Governance	Interface ownership and critical-flow inventory	Foundational, Advanced, High Assurance	High	Critical
MYTHOS-FND-UI-02	State	Authoritative and unambiguous system state	Foundational, Advanced, High Assurance	High	Critical
MYTHOS-FND-UI-03	Context	Scope, identity, and environment visibility	Foundational, Advanced, High Assurance	High	Critical
MYTHOS-FND-UI-04	Actions	Safe critical-action design	Foundational, Advanced, High Assurance	High	Critical
MYTHOS-FND-UI-05	Recovery	Undo, cancellation, and recovery	Foundational, Advanced, High Assurance	Partial	Critical
MYTHOS-FND-UI-06	Accessibility	Accessibility baseline	Foundational, Advanced, High Assurance	Partial	Critical
MYTHOS-FND-UI-07	Input	Input validation and constraint communication	Foundational, Advanced, High Assurance	High	Material
MYTHOS-FND-UI-08	Feedback	Timely and actionable feedback	Foundational, Advanced, High Assurance	Partial	Material
MYTHOS-FND-UI-09	Errors	Non-sensitive error communication	Foundational, Advanced, High Assurance	High	Critical
MYTHOS-FND-UI-10	Privacy	Privacy-respecting interaction	Foundational, Advanced, High Assurance	Partial	Critical
	Security	Session and sensitive-data handling		High	Critical

Control	Family	Title	Profiles	Automation	Impact
MYTHOS-FND-UI-11			Foundational, Advanced, High Assurance		
MYTHOS-FND-UI-12	Consistency	Consistent interaction semantics	Foundational, Advanced, High Assurance	Partial	Material
MYTHOS-FND-UI-13	Performance	Perceived and actual responsiveness	Advanced, High Assurance	High	Material
MYTHOS-FND-UI-14	Degradation	Degraded and offline behavior	Advanced, High Assurance	Partial	Critical
MYTHOS-FND-UI-15	AI interaction	AI-generated output and action boundaries	Foundational, Advanced, High Assurance	Partial	Critical
MYTHOS-FND-UI-16	Internationalization	Locale, language, time, and unit correctness	Advanced, High Assurance	Partial	Material
MYTHOS-FND-UI-17	Evidence	Interaction auditability	Advanced, High Assurance	High	Critical
MYTHOS-FND-UI-18	Testing	Representative interface validation	Foundational, Advanced, High Assurance	Partial	Critical

Appendix D – Minimum Conformance Claim Record

```
standard: MYTHOS-FND-0007
version: 0.2.0
profile: foundational | advanced | high_assurance
scope: <bounded systems, teams, environments, and processes>
assessment_period: <start/end>
assessor: <person or independent body>
tailoring_decisions: []
exceptions: []
findings_summary:
  satisfied: 0
  partially_satisfied: 0
  not_satisfied: 0
  not_applicable: 0
  not_assessed: 0
residual_risk_owner: <accountable role>
approval: <record reference>
```

Appendix E – Publication Review Checklist

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

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