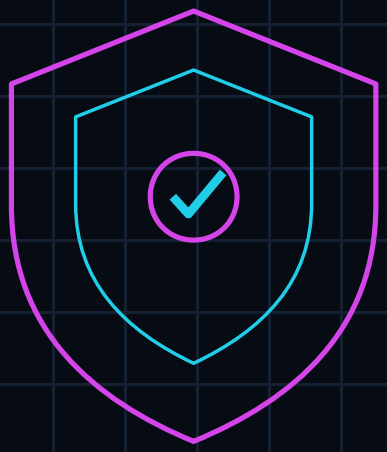


CANDIDATE STANDARD

Mythos Security, Privacy, and Trust Standard

Engineer security, privacy, and trust as system properties with explicit authority, isolation, evidence, and resilience.

PERMANENT ID
MYTHOS-FND-0003

PUBLICATION CLASS
CANDIDATE STANDARD

VERSION / STATUS
1.0.0-candidate / CANDIDATE

PERMANENT PUBLICATION IDENTITY

Mythos Security, Privacy, and Trust Standard

Universal Requirements for Risk Governance, Secure Architecture, Identity, Data Protection, Privacy, Resilience, Supply Chain, and Continuous Assurance

Document ID
MYTHOS-FND-0003

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	Security and privacy leaders; Engineers and architects; Product and data owners; Operations and incident response teams; Risk managers, assessors, and auditors
Publisher / owner	Mythos Systems / Standards Program
Public classification	Public technical standard
Canonical route	/library/standards/foundation/mythos-fnd-0003/

Expected outcomes

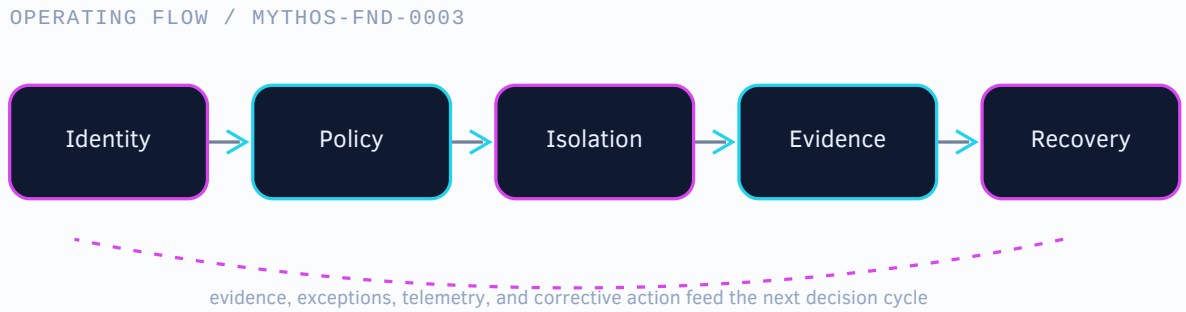
- Embed security, privacy, and trust outcomes throughout system and organizational lifecycles.
- Constrain authority, exposure, data use, and blast radius through explicit boundaries and least privilege.
- Protect software and dependency supply chains and preserve evidence needed for assurance and incident response.
- Make controls testable, continuously observable where practical, and proportionate to consequence.

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-0003
Standard	Security, Privacy, and Trust
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

Security, privacy, and trust cannot be added after architecture decisions have already established identity, data, execution, and dependency boundaries. This standard defines a unified governance and engineering system for protecting organizational operations, users, data, software, infrastructure, and delegated machine action while avoiding unsupported claims of security, privacy, sovereignty, or compliance.

The institutional objective is to integrate security, privacy, resilience, cryptography, identity, supply-chain integrity, evidence, and trust claims across the full system lifecycle. Adoption should produce a controlled operating state in which leadership can understand the material risks, engineering teams can act on explicit requirements, assessors can test implementation and operating effectiveness, and the organization can support every conformance or trust claim with current evidence.

2. Executive Findings and Required Direction

Finding	Enterprise Exposure	Required Direction
Fragmented governance	Security, privacy, resilience, and AI trust are often managed as disconnected reviews.	Use one integrated risk and control model with accountable ownership.
Ambient authority	Users, workloads, agents, and integrations often inherit broader access than necessary.	Use explicit identity, least privilege, constrained delegation, and expiring grants.
Secrets and cryptography debt	Long-lived credentials and algorithm lock-in create systemic exposure.	Broker secrets, rotate credentials, maintain cryptographic inventory, and design for agility.
Supply-chain opacity	Organizations cannot reliably prove what entered a release.	Require provenance, SBOMs, signing, dependency policy, and verified build controls.
Trust claims without evidence	Products claim privacy, locality, security, or compliance without bounded proof.	Define claim scope, evidence, limitations, and review triggers.

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.

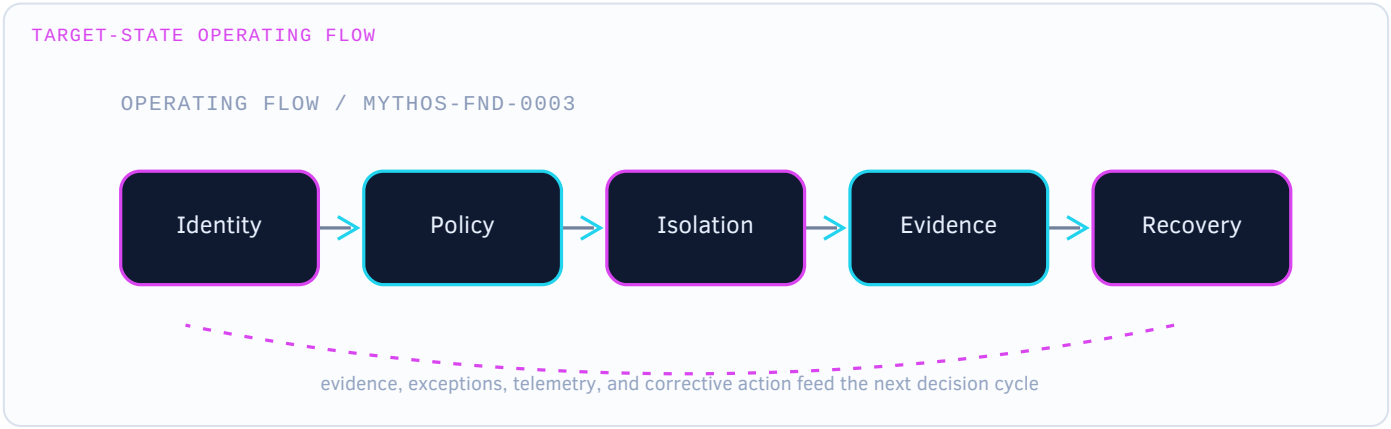
3.3 Security, Privacy, and Trust Impact

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	Integrated governance and risk model
2	Security architecture and invariants
3	Threat, abuse, and misuse modeling
4	Asset, data, and capability classification
5	Human and workload identity
6	Authorization and delegation
7	Secrets, certificates, keys, and cryptographic agility
8	Privacy purpose, minimization, consent, retention, deletion, and export
9	Isolation and sandboxing
10	Secure development and supply chain
11	Logging, audit, and evidence integrity
12	Vulnerability and exposure management
13	Incident and emergency authority
14	Backup, recovery, and continuity

#	Target-State Component
15	Third-party and AI trust
16	Continuous assurance and trust-claim registry

```
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
Board or executive risk owner	Sets risk appetite and receives material trust reporting.
Chief information security officer	Owns security governance and enterprise control outcomes.
Privacy officer	Owns privacy risk, lawful use, rights, retention, and disclosure.
Security architect	Defines trust boundaries, identity, cryptography, isolation, and invariants.
Product and service owners	Implement controls and accept residual risk within delegated authority.
Incident commander	Coordinates containment, communication, recovery, and evidence.
Supply-chain owner	Maintains provenance, dependency, and supplier assurance.
Independent assessor	Tests design and operating effectiveness.

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

- Embed security, privacy, and trust outcomes throughout system and organizational lifecycles.
- Constrain authority, exposure, data use, and blast radius through explicit boundaries and least privilege.
- Protect software and dependency supply chains and preserve evidence needed for assurance and incident response.
- Make controls testable, continuously observable where practical, and proportionate to consequence.

7. Scope

Applies to all systems that process organizational or user data, connect to networks, execute code, expose interfaces, delegate authority, integrate third parties, or affect operational, financial, safety, privacy, legal, or mission outcomes.

8. Intended Audience

- Security and privacy leaders
- Engineers and architects
- Product and data owners
- Operations and incident response teams
- Risk managers, assessors, and auditors

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

- **NIST CSWP 29** — The NIST Cybersecurity Framework (CSF) 2.0. https://doi.org/10.6028/NIST.CSWP.29
- **NIST SP 800-53 Rev. 5, Release 5.2.0** — Security and Privacy Controls for Information Systems and Organizations. https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final
- **NIST SP 800-53A Rev. 5, Release 5.2.0** — Assessing Security and Privacy Controls in Information Systems and Organizations. https://csrc.nist.gov/pubs/sp/800/53/a/r5/final
- **NIST SP 800-218 v1.1** — Secure Software Development Framework (SSDF). https://csrc.nist.gov/pubs/sp/800/218/final
- **NIST SP 800-207** — Zero Trust Architecture. https://doi.org/10.6028/NIST.SP.800-207
- **NIST SP 800-161 Rev. 1 Update 1** — Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations. https://csrc.nist.gov/pubs/sp/800/161/r1/upd1/final
- **NIST SP 800-61 Rev. 3** — Incident Response Recommendations and Considerations for Cybersecurity Risk Management. https://csrc.nist.gov/pubs/sp/800/61/r3/final
- **NIST Privacy Framework 1.0** — A Tool for Improving Privacy through Enterprise Risk Management. https://www.nist.gov/privacy-framework/privacy-framework
- **CISA CPG 2.0** — Cross-Sector Cybersecurity Performance Goals 2.0. https://www.cisa.gov/cybersecurity-performance-goals-2-0-cpg-2-0
- **CIS Controls v8.1** — CIS Critical Security Controls. https://www.cisecurity.org/controls/v8-1
- **OWASP ASVS** — Application Security Verification Standard. https://owasp.org/www-project-application-security-verification-standard/
- **SLSA 1.2** — Supply-chain Levels for Software Artifacts. https://slsa.dev/spec/v1.2/
- **SPDX 3.0** — Software Package Data Exchange specification. https://spdx.github.io/spdx-spec/v3.0/
- **CycloneDX 1.7** — OWASP software bill of materials standard. https://cyclonedx.org/specification/overview/
- **Sigstore** — Keyless signing and transparency-log ecosystem. https://docs.sigstore.dev/

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.

Term	Definition
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.
Ambient authority	Permission available to code or a principal without an explicit, scoped delegation for the current action.
Trust boundary	A transition where identity, authority, data sensitivity, integrity, execution context, or control ownership changes.
Security invariant	A condition that must remain true to maintain the intended security or privacy posture.
Cryptographic agility	The ability to inventory, replace, configure, and retire cryptographic mechanisms without uncontrolled system redesign.
Trust claim	A statement about identity, integrity, provenance, authorization, safety, privacy, or control effectiveness that requires evidence.

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.

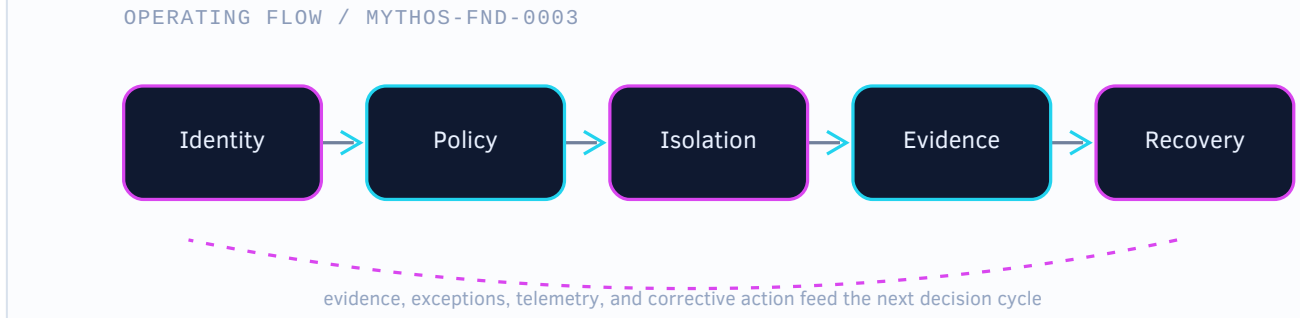
Adopting organizations SHOULD maintain a domain-specific risk register that identifies cause, affected asset or stakeholder, credible scenario, impact, existing controls, residual risk, owner, review trigger, and evidence. Risks that cross standards MUST be linked rather than copied into disconnected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

15. Governing Principles

- Deny by default and grant the minimum authority for the minimum time.
- Local, internal, signed, or vendor-provided does not automatically mean trusted.
- Trust boundaries and security invariants must be explicit and testable.
- Sensitive data collection and processing must be minimized and purpose-bound.
- Security controls must fail safely and remain operable during degradation.
- All material authority must be revocable, observable, and attributable.
- Claims of security or privacy require bounded evidence, not confidence language.

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
Board or executive risk owner	Sets risk appetite and receives material trust reporting.
Chief information security officer	Owns security governance and enterprise control outcomes.
Privacy officer	Owns privacy risk, lawful use, rights, retention, and disclosure.
Security architect	Defines trust boundaries, identity, cryptography, isolation, and invariants.
Product and service owners	Implement controls and accept residual risk within delegated authority.
Incident commander	Coordinates containment, communication, recovery, and evidence.
Supply-chain owner	Maintains provenance, dependency, and supplier assurance.
Independent assessor	Tests design and operating effectiveness.

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
Security approval based only on a checklist	Failure can create hidden risk, misleading assurance, uncontrolled cost, or unsafe operation.
Storing credentials in model or agent context	Failure can create hidden risk, misleading assurance, uncontrolled cost, or unsafe operation.
Calling a system zero trust, private, sovereign, or post-quantum without bounded evidence	Failure can create hidden risk, misleading assurance, uncontrolled cost, or unsafe operation.
Relying on network location as identity	Failure can create hidden risk, misleading assurance, uncontrolled cost, or unsafe operation.
Treating successful backup jobs as proof of recoverability	Failure can create hidden risk, misleading assurance, uncontrolled cost, or unsafe operation.
Allowing extensions or agents ambient access	Failure can create hidden risk, misleading assurance, uncontrolled cost, or unsafe operation.

21. Cross-Functional Dependencies

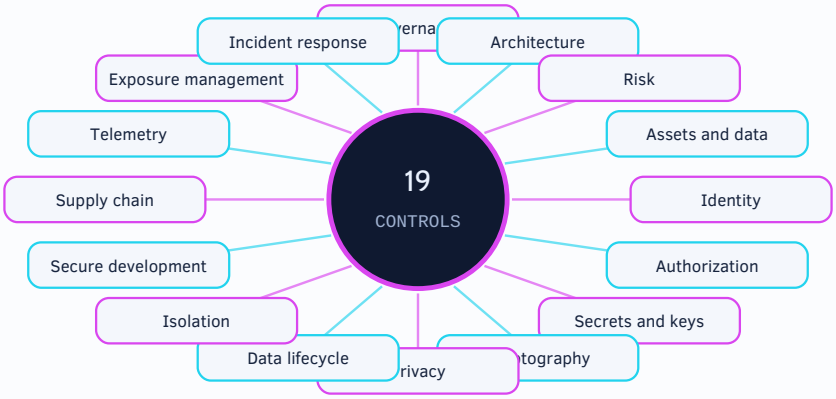
This Foundation standard depends on the remaining MYTHOS-FND standards for documentation, security and trust, quality, operations, data and integration, interfaces, extensions, AI-first behavior, and agentic orchestration. An adopting organization MUST resolve overlapping requirements through the stricter 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
- Architecture
- Risk
- Assets and data
- Identity
- Authorization
- Secrets and keys
- Cryptography
- Privacy
- Data lifecycle
- Isolation
- Secure development
- Supply chain
- Telemetry
- Exposure management
- Incident response
- Resilience
- Third parties and automation

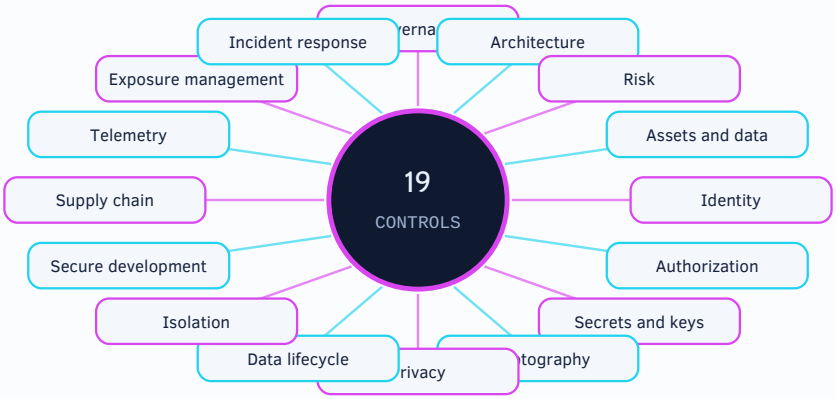
- Assurance

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-SPT-01 – Integrated security, privacy, and trust governance

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

Requirement

The organization MUST assign accountable ownership for security, privacy, and trust outcomes; define risk appetite and escalation; and integrate these concerns into product, architecture, procurement, release, operations, and retirement decisions.

Purpose

Prevents fragmented control ownership and late-stage risk discovery.

Applicability

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

Implementation guidance

- Define decision rights and separation of duties.
- Maintain an integrated risk register linked to systems, data, suppliers, and controls.
- Require material residual risk to be accepted by an authority with appropriate business accountability.

Required evidence

- Governance charter
- Risk appetite and escalation criteria
- Sample risk decisions

Assessment procedure

- **Examine:** Examine ownership and decision records.
- **Interview:** Interview accountable leaders and implementers.
- **Test:** Trace material risk from discovery through disposition.

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 — Govern
- NIST SP 800-53 — PM and RA families

NORMATIVE CONTROL

MYTHOS-FND-SPT-02 – Security architecture and invariants

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

Requirement

Each in-scope system MUST document and enforce security and privacy architecture, including assets, principal types, data flows, trust boundaries, control planes, privileged paths, failure domains, dependencies, and security invariants.

Purpose

Makes consequential boundaries and assumptions reviewable and testable.

Applicability

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

Implementation guidance

- Model normal, degraded, administrative, recovery, support, and update paths.
- Identify authoritative policy and identity decision points.
- Link invariants to automated tests or monitoring where feasible.

Required evidence

- Security architecture
- Trust-boundary diagrams
- Invariant tests

Assessment procedure

- **Examine:** Trace privileged and sensitive workflows.
- **Interview:** Compare documented controls with deployment.
- **Test:** Attempt to violate selected invariants in a controlled environment.

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 800-160 Vol. 1 Rev. 1
- NIST SP 800-207

NORMATIVE CONTROL

MYTHOS-FND-SPT-03 – Threat, abuse, and misuse modeling

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

Requirement

The organization MUST identify credible threats, abuse cases, misuse, privacy harms, dependency failures, insider scenarios, and recovery risks before release and after material change.

Purpose

Expands analysis beyond accidental defects and externally initiated attacks.

Applicability

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

Implementation guidance

- Record actor or cause, preconditions, affected assets, attack or failure path, impact, detection, mitigations, validation, and residual risk.
- Include supply-chain, administrative, cross-tenant, automation, AI, and support-channel scenarios where applicable.
- Prioritize by consequence and plausibility without treating low probability as zero risk.

Required evidence

- Threat and abuse model
- Risk treatment links
- Validation records

Assessment procedure

- **Examine:** Review scenario completeness against architecture.
- **Interview:** Conduct structured challenge or threat-model workshop.
- **Test:** Test one high-impact scenario end to end.

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-3
- NIST AI RMF — Map

NORMATIVE CONTROL

MYTHOS-FND-SPT-04 – Asset, data, and capability classification

FAMILY	PROFILES	FAILURE IMPACT	AUTOMATION POTENTIAL
Assets and data	Foundational, Advanced, High Assurance	Critical	High

Requirement

Assets, data, credentials, models, tools, interfaces, and executable capabilities MUST be classified by sensitivity, criticality, integrity, availability, privacy, provenance, retention, and authority requirements.

Purpose

Enables controls to follow the actual value and consequence of resources.

Applicability

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

Implementation guidance

- Classify unknown data conservatively until resolved.
- Propagate classification through derived data, backups, caches, logs, exports, and model context.
- Associate handling rules and owners with each class.

Required evidence

- Classification policy
- Inventories and data maps
- Handling-rule tests

Assessment procedure

- **Examine:** Sample assets and trace classification through processing.
- **Interview:** Test enforcement of handling rules.
- **Test:** Review unclassified or ownerless resources.

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 — Data Processing Management

NORMATIVE CONTROL

MYTHOS-FND-SPT-05 – Strong identity and authentication

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

Requirement

Every human, workload, device, service, agent, extension, and administrative process exercising material authority MUST have a distinct, verifiable identity and authentication strength proportionate to risk.

Purpose

Prevents shared, ambiguous, or weakly authenticated authority and supports attribution and revocation.

Applicability

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

Implementation guidance

- Prefer phishing-resistant authentication for privileged and high-impact access.
- Use short-lived workload credentials and avoid embedded static secrets.
- Define session binding, reauthentication, device posture, and recovery requirements.

Required evidence

- Identity inventory
- Authentication configuration
- Credential and session test results

Assessment procedure

- **Examine:** Attempt shared or anonymous privileged access.
- **Interview:** Verify credential lifetime and revocation.
- **Test:** Review authentication recovery for bypass risk.

Exceptions and compensating controls

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

External mappings

- NIST SP 800-53 — IA family
- CISA CPG 2.0 — account security

NORMATIVE CONTROL

MYTHOS-FND-SPT-06 – Least privilege and explicit delegation

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

Requirement

Authorization decisions MUST be deny-by-default, evaluated at authoritative enforcement points, scoped to the requested action and resource, and based on explicit policy, current identity, context, and delegated authority.

Purpose

Constrains blast radius and prevents frontend-only, ambient, stale, or transitive privilege.

Applicability

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

Implementation guidance

- Separate authentication from authorization.
- Model permissions as narrowly as operationally practical.
- Require step-up or additional approval for high-impact actions.
- Invalidate cached decisions when relevant identity or policy state changes.

Required evidence

- Authorization policy
- Decision logs
- Negative and escalation-path tests

Assessment procedure

- **Examine:** Attempt unauthorized direct calls bypassing the interface.
- **Interview:** Test revocation and policy-change propagation.
- **Test:** Review wildcard and inherited permissions.

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 family
- NIST SP 800-207

NORMATIVE CONTROL

MYTHOS-FND-SPT-07 – Secrets, certificates, and key lifecycle

FAMILY	PROFILES	FAILURE IMPACT	AUTOMATION POTENTIAL
Secrets and keys	Foundational, Advanced, High Assurance	Critical	High

Requirement

Secrets, private keys, certificates, tokens, and recovery material MUST be inventoried, protected outside ordinary source and logs, issued to specific identities and purposes, rotated or renewed, revocable, and monitored for exposure.

Purpose

Reduces credential theft, uncontrolled reuse, and long-lived compromise.

Applicability

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

Implementation guidance

- Broker access rather than distributing raw secrets where feasible.
- Separate secret references from values.
- Define emergency rotation and dependent-system recovery.
- Validate certificate chains, names, purposes, and revocation.

Required evidence

- Secrets inventory
- Issuance and rotation records
- Exposure scanning and revocation tests

Assessment procedure

- **Examine:** Search code, artifacts, logs, and backups for sampled secrets.
- **Interview:** Revoke a test credential and verify denial.
- **Test:** Review ownership and age.

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-5, SC-12, SC-17

NORMATIVE CONTROL

MYTHOS-FND-SPT-08 – Approved cryptography and crypto-agility

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

Requirement

Cryptographic mechanisms MUST be selected from approved, context-appropriate algorithms and protocols; configured securely; inventoried with dependencies; and replaceable through a documented crypto-agility plan.

Purpose

Protects confidentiality and integrity while reducing migration risk from algorithm, library, protocol, or key compromise.

Applicability

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

Implementation guidance

- Inventory algorithm, mode, parameter, key source, library, protocol, data purpose, and owner.
- Prohibit silent downgrade and unauthenticated encryption.
- Plan migration for long-lived sensitive data and cryptographic dependencies, including post-quantum transition where risk warrants.

Required evidence

- Cryptographic inventory
- Configuration policy
- Migration and downgrade tests

Assessment procedure

- **Examine:** Scan deployments and artifacts for prohibited mechanisms.
- **Interview:** Test negotiation and downgrade behavior.
- **Test:** Review replacement feasibility for critical dependencies.

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 — SC-12 and SC-13
- NIST post-quantum cryptography program

NORMATIVE CONTROL

MYTHOS-FND-SPT-09 – Purpose limitation, minimization, and consent

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

Requirement

Personal and sensitive data processing MUST have a defined purpose and lawful or authorized basis, collect and retain only what is necessary, communicate material use, and prevent secondary use outside approved bounds.

Purpose

Reduces privacy harm, legal exposure, breach impact, and opaque data practices.

Applicability

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

Implementation guidance

- Perform privacy impact assessment proportionate to data and consequence.
- Avoid dark patterns and bundled consent.
- Minimize telemetry, prompts, model context, and support bundles.
- Provide meaningful controls and alternatives when consent is the basis.

Required evidence

- Data-purpose register
- Privacy assessment
- Consent and preference records

Assessment procedure

- **Examine:** Trace sampled fields to approved purposes.
- **Interview:** Test withdrawal or preference changes.
- **Test:** Review data used for new purposes or AI training.

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
- NIST SP 800-53 — PT and DM families

NORMATIVE CONTROL

MYTHOS-FND-SPT-10 – Retention, deletion, and export protection

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

Requirement

Data retention, archival, backup, export, and deletion MUST be governed by classification, purpose, obligation, recovery needs, and user or organizational commitments, with verifiable deletion semantics and secure export controls.

Purpose

Prevents indefinite accumulation, orphan data, insecure support bundles, and false deletion claims.

Applicability

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

Implementation guidance

- Define behavior across primary stores, replicas, caches, indexes, backups, logs, embeddings, and derived artifacts.
- Encrypt and authorize sensitive exports.
- Record residual retention caused by immutable backups or legal holds.

Required evidence

- Retention schedule
- Deletion and export tests
- Deletion evidence

Assessment procedure

- **Examine:** Delete a test subject or record and inspect downstream stores.
- **Interview:** Attempt unauthorized export.
- **Test:** Review expired data and orphaned storage.

Exceptions and compensating controls

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

External mappings

- NIST SP 800-53 — SI-12 and MP family
- NIST Privacy Framework — Disassociated Processing

NORMATIVE CONTROL

MYTHOS-FND-SPT-11 – Tenant, workload, and execution isolation

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

Requirement

Systems serving multiple tenants, trust domains, plugins, users, or workloads MUST enforce isolation across identity, authorization, compute, memory, storage, network, cache, telemetry, and administrative access.

Purpose

Prevents cross-boundary disclosure, influence, resource theft, and privilege escalation.

Applicability

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

Implementation guidance

- Bind tenant or trust-domain context at authoritative entry points.
- Use defense in depth rather than relying on a single query filter or process boundary.
- Test support and break-glass paths.
- Apply resource quotas and side-channel risk analysis where warranted.

Required evidence

- Isolation architecture
- Cross-boundary test results
- Administrative access records

Assessment procedure

- **Examine:** Attempt cross-tenant reads, writes, cache access, log access, and resource exhaustion.
- **Interview:** Review support impersonation controls.
- **Test:** Test context propagation under asynchronous execution.

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-4, SC-2, SC-7, SC-39

NORMATIVE CONTROL

MYTHOS-FND-SPT-12 – Secure design and implementation lifecycle

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

Requirement

Software, infrastructure, models, prompts, policies, and configuration MUST be developed through controlled environments using reviewed changes, secure coding practices, dependency controls, protected build processes, and security verification proportionate to risk.

Purpose

Reduces preventable defects and malicious or accidental compromise during creation and change.

Applicability

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

Implementation guidance

- Define security requirements and misuse cases early.
- Protect branches, build identities, signing keys, and release workflows.
- Use static, dynamic, composition, infrastructure, secret, and policy analysis as applicable.
- Require remediation or accepted exception before release.

Required evidence

- Development policy
- Change and review records
- Security test results

Assessment procedure

- **Examine:** Sample changes from requirement to release.
- **Interview:** Attempt bypass of required review or build controls.
- **Test:** Verify findings are dispositioned.

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
- OWASP ASVS

- OWASP SAMM

NORMATIVE CONTROL

MYTHOS-FND-SPT-13 – Software and service supply-chain integrity

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

Requirement

Critical dependencies, build inputs, artifacts, suppliers, services, models, extensions, and update channels MUST have verified identity, provenance, integrity, risk evaluation, vulnerability monitoring, and supported replacement or containment plans.

Purpose

Reduces compromise through upstream components, opaque services, malicious updates, and abandoned dependencies.

Applicability

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

Implementation guidance

- Generate and preserve SBOM or equivalent inventories.
- Verify signatures and provenance at admission and deployment.
- Assess maintainer health, licensing, concentration, transitive risk, and update practices.
- Define quarantine and revocation.

Required evidence

- SBOM and dependency inventory
- Provenance attestations
- Supplier and update risk records

Assessment procedure

- **Examine:** Verify artifact signatures and provenance.
- **Interview:** Introduce an unapproved dependency in a test pipeline.
- **Test:** Review response to a withdrawn or compromised package.

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
- SLSA 1.2

- SPDX 3.0
- CycloneDX 1.7
- Sigstore

NORMATIVE CONTROL

MYTHOS-FND-SPT-14 – Security logging, audit, and evidence integrity

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

Requirement

Material security, privacy, administrative, policy, data-access, execution, extension, model, and lifecycle events MUST produce attributable, time-synchronized, access-controlled, redacted, and integrity-protected records sufficient for detection, investigation, accountability, and assessment.

Purpose

Creates evidence for operational defense without turning logs into an uncontrolled sensitive-data store.

Applicability

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

Implementation guidance

- Define required events and fields.
- Exclude or tokenize secrets and unnecessary personal data.
- Protect audit configuration and monitor gaps.
- Use tamper-evident storage or signed evidence where consequence warrants.

Required evidence

- Logging specification
- Sample events
- Integrity, retention, and access tests

Assessment procedure

- **Examine:** Perform a privileged action and trace it end to end.
- **Interview:** Test redaction and audit-disable detection.
- **Test:** Verify clock and identity consistency.

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
- CISA CPG 2.0 — logging

NORMATIVE CONTROL

MYTHOS-FND-SPT-15 – Vulnerability and exposure management

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

Requirement

The organization MUST continuously identify, validate, prioritize, remediate, mitigate, or formally accept vulnerabilities and exposures across assets, software, infrastructure, identities, configurations, suppliers, and external attack surfaces.

Purpose

Focuses action on exploitable conditions and business impact rather than scanner volume alone.

Applicability

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

Implementation guidance

- Combine severity with reachability, exposure, exploitability, asset criticality, compensating controls, and threat evidence.
- Define remediation targets and emergency pathways.
- Verify fixes and detect recurrence.

Required evidence

- Asset and exposure inventory
- Findings and service-level records
- Remediation verification

Assessment procedure

- **Examine:** Sample findings across severity and age.
- **Interview:** Reproduce or validate selected exposures.
- **Test:** Test whether recurrence or reopened exposure is detected.

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.RA and PR.PS
- CIS Controls v8.1 — Continuous Vulnerability Management

NORMATIVE CONTROL

MYTHOS-FND-SPT-16 – Incident response and emergency authority

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

Requirement

The organization MUST maintain and exercise incident capabilities for detection, triage, containment, evidence preservation, eradication, recovery, communication, legal or privacy obligations, and post-incident improvement, including narrowly governed emergency authority.

Purpose

Reduces harm and decision paralysis during high-pressure events.

Applicability

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

Implementation guidance

- Define severity, roles, communications, external dependencies, and escalation.
- Pre-authorize reversible containment actions where delay is dangerous.
- Protect evidence chain of custody.
- Review incidents for control and documentation changes.

Required evidence

- Incident plan and playbooks
- Exercise and incident records
- Post-incident actions

Assessment procedure

- **Examine:** Run a scenario exercise.
- **Interview:** Verify emergency access is logged, time-bound, and reviewed.
- **Test:** Trace corrective actions to closure.

Exceptions and compensating controls

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

External mappings

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

NORMATIVE CONTROL

MYTHOS-FND-SPT-17 – Backup, recovery, and continuity assurance

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

Requirement

Critical services and data MUST have risk-based resilience, backup, recovery, and continuity strategies that protect integrity and confidentiality and are exercised against realistic failure, corruption, compromise, and dependency-loss scenarios.

Purpose

Ensures availability claims survive actual restoration and not merely backup-job success.

Applicability

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

Implementation guidance

- Define recovery time and recovery point objectives.
- Separate or immutably protect recovery assets from common compromise paths.
- Validate restored data and software integrity.
- Include supplier and identity-system failure.

Required evidence

- Continuity and recovery plans
- Restore exercise results
- Integrity validation

Assessment procedure

- **Examine:** Restore a representative system or dataset.
- **Interview:** Test access when primary identity or network services are unavailable.
- **Test:** Review unmet objectives and remediation.

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 — Recover
- NIST SP 800-53 — CP family

NORMATIVE CONTROL

MYTHOS-FND-SPT-18 – Third-party, AI, and delegated-action trust

FAMILY	PROFILES	FAILURE IMPACT	AUTOMATION POTENTIAL
Third parties and automation	Advanced, High Assurance	Critical	High

Requirement

External services, AI systems, agents, extensions, integrations, and automated decision or execution components MUST operate within explicit data, capability, identity, approval, observability, and revocation boundaries, and their outputs MUST NOT be treated as inherently trusted.

Purpose

Constrains opaque or probabilistic components and prevents delegated systems from silently expanding authority.

Applicability

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

Implementation guidance

- Validate outputs before consequential use.
- Broker tools and credentials through policy enforcement points.
- Maintain kill switches, provider exit paths, and degraded modes.
- Assess prompt injection, tool abuse, model change, data use, and provider retention where applicable.

Required evidence

- Delegation and capability policy
- Provider and component assessments
- Adversarial and revocation tests

Assessment procedure

- **Examine:** Attempt unauthorized tool use or data disclosure.
- **Interview:** Change or remove a provider and verify controlled degradation.
- **Test:** Review whether human accountability remains explicit.

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
- OWASP LLM Top 10 2025

- OWASP Agentic Applications Top 10 2026

NORMATIVE CONTROL

MYTHOS-FND-SPT-19 – Continuous control assurance and trust claims

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

Requirement

Material security, privacy, and trust claims MUST identify scope, conditions, evidence, assessment date, confidence, limitations, and residual risk; critical controls SHOULD be continuously or regularly verified for drift and effectiveness.

Purpose

Prevents broad claims such as secure, private, zero trust, compliant, or encrypted from exceeding the evidence.

Applicability

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

Implementation guidance

- Maintain evidence freshness requirements.
- Separate design evidence from operating-effectiveness evidence.
- Use independent assessment for high-impact claims.
- Withdraw or qualify claims when evidence expires or conditions change.

Required evidence

- Control evidence register
- Assessment reports
- Claim and limitation statements

Assessment procedure

- **Examine:** Challenge sampled trust claims.
- **Interview:** Verify evidence freshness and scope.
- **Test:** Induce a safe control drift and confirm detection.

Exceptions and compensating controls

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

External mappings

- NIST SP 800-53A Rev. 5
- NIST CSF 2.0 — Govern and Identify

FOUNDATION STANDARD / STRUCTURAL PART

Part V – Implementation and Operations

24. Implementation Profiles

Profile	Required Operating State
Baseline	Asset and data classification, strong identity, least privilege, secrets lifecycle, approved cryptography, privacy controls, secure development, logging, vulnerability management, incident response, and recovery.
Enterprise	Central policy, workload identity, automated evidence, SBOM and provenance, continuous exposure management, tenant isolation, supplier assurance, and trust-claim governance.
High Assurance	Hardware-backed identity, high-isolation execution, independent red teaming, cryptographic evidence, formal threat analysis, post-quantum migration planning, continuous control validation, and four-eyes emergency governance.

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

- Security approval based only on a checklist
- Storing credentials in model or agent context
- Calling a system zero trust, private, sovereign, or post-quantum without bounded evidence
- Relying on network location as identity
- Treating successful backup jobs as proof of recoverability
- Allowing extensions or agents ambient access

30. Adoption Roadmap from Source Draft

- Establish governance, asset and data classification, threat models, trust boundaries, and accountable risk ownership.

- Implement identity, authorization, secrets, cryptography, privacy, logging, secure development, and vulnerability-management baselines.
- Add supply-chain provenance, isolation, incident response, recovery validation, and third-party controls.
- Automate policy checks, evidence collection, continuous exposure monitoring, and control-drift detection.
- For High Assurance, add independent adversarial testing, stronger isolation, tamper-evident evidence, and tested emergency revocation.

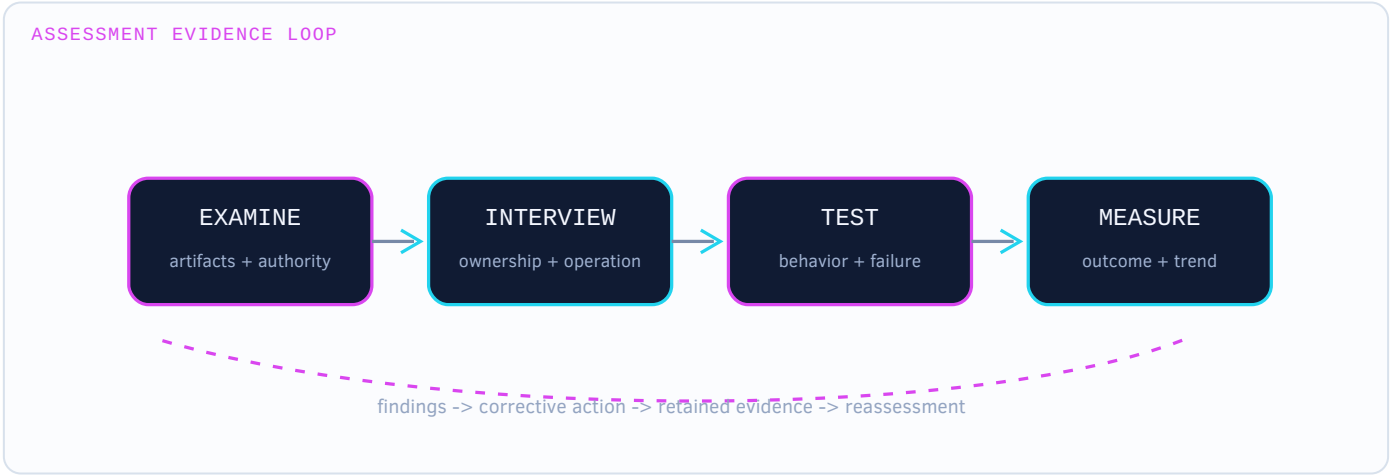
31. Limitations and Residual Risk from Source Draft

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-control verification	Applicable critical controls with current verified evidence	100%
Mean time to revoke		Risk-defined and tested

Metric	Definition	Expected use or target
	Elapsed time to revoke compromised identity, credential, key, token, extension, or release	
High-risk finding age	Age of unresolved critical and high findings beyond target	0 beyond approved target without active exception
Security telemetry coverage	Material trust boundaries and privileged actions producing usable events	100% High Assurance
Recovery validation	Critical services with exercised recovery and integrity verification	100% within defined interval

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.

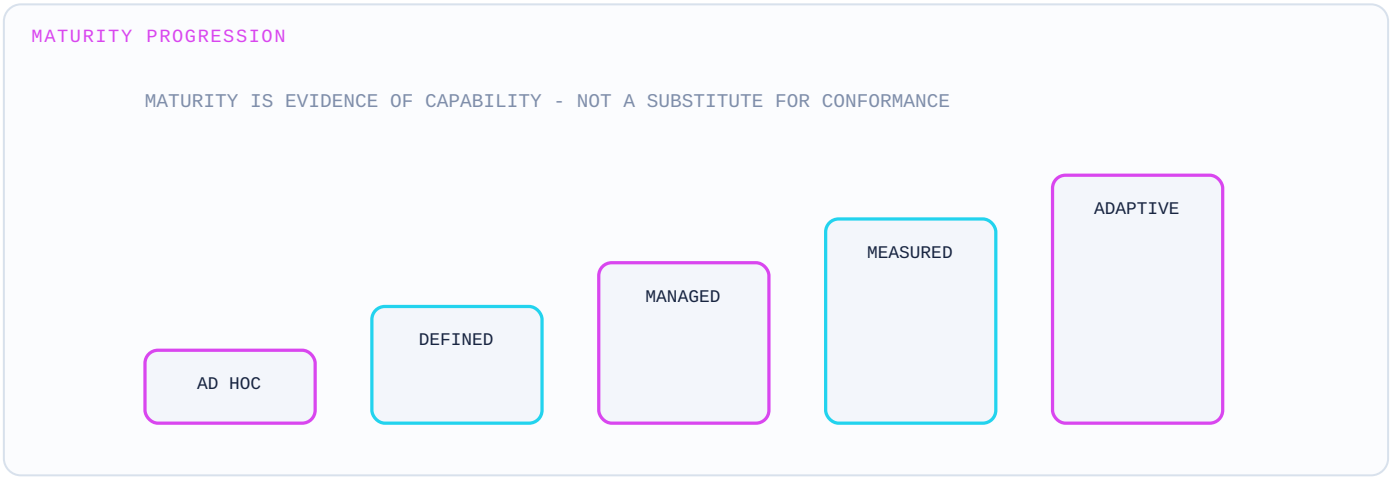
34. Exceptions and Compensating Controls

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
privileged identities without current owner	Defined by the adopting organization with owner, source, target, and cadence.
long-lived secrets beyond policy	Defined by the adopting organization with owner, source, target, and cadence.
critical assets without threat model	Defined by the adopting organization with owner, source, target, and cadence.
data stores without classification or retention rule	Defined by the adopting organization with owner, source, target, and cadence.
unsigned or unprovenanced release artifacts	Defined by the adopting organization with owner, source, target, and cadence.
critical vulnerabilities beyond target	Defined by the adopting organization with owner, source, target, and cadence.
security incidents without completed corrective actions	Defined by the adopting organization with owner, source, target, and cadence.
trust claims without current evidence	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
NIST CSF 2.0	Cybersecurity risk governance	https://www.nist.gov/cyberframework	Current	2026-09-17
NIST SP 800-53 Rev. 5	Security and privacy controls	https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final	Final update 1	2026-09-17
NIST SP 800-207	Zero Trust Architecture	https://csrc.nist.gov/pubs/sp/800/207/final	Final	2026-09-17
NIST SP 800-218	Secure Software Development Framework 1.1	https://csrc.nist.gov/pubs/sp/800/218/final	Final; 1.2 revision is draft	2026-09-17
FIPS 203	ML-KEM	https://csrc.nist.gov/pubs/fips/203/final	Final	2026-09-17
FIPS 204	ML-DSA	https://csrc.nist.gov/pubs/fips/204/final	Final	2026-09-17
FIPS 205	SLH-DSA	https://csrc.nist.gov/pubs/fips/205/final	Final	2026-09-17
NIST SP 800-227	Recommendations for Key-Encapsulation Mechanisms	https://csrc.nist.gov/pubs/sp/800/227/final	Final	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 emphasis on deny-by-default, no ambient authority, trust boundaries, cryptographic agility, privacy, isolation, secure exports, and lifecycle security.
- Generalizes implementation-specific desktop and framework guidance into technology-neutral control outcomes.
- Adds current supply-chain, incident-response, and continuous-assurance structures.
- Replaces absolute security language with scoped trust claims, evidence, and residual-risk reporting.

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-SPT-01	Governance	Integrated security, privacy, and trust governance	Foundational, Advanced, High Assurance	Partial	Critical
MYTHOS-FND-SPT-02	Architecture	Security architecture and invariants	Foundational, Advanced, High Assurance	Partial	Critical
MYTHOS-FND-SPT-03	Risk	Threat, abuse, and misuse modeling	Foundational, Advanced, High Assurance	Partial	Critical
MYTHOS-FND-SPT-04	Assets and data	Asset, data, and capability classification	Foundational, Advanced, High Assurance	High	Critical
MYTHOS-FND-SPT-05	Identity	Strong identity and authentication	Foundational, Advanced, High Assurance	High	Critical
MYTHOS-FND-SPT-06	Authorization	Least privilege and explicit delegation	Foundational, Advanced, High Assurance	High	Critical
MYTHOS-FND-SPT-07	Secrets and keys	Secrets, certificates, and key lifecycle	Foundational, Advanced, High Assurance	High	Critical
MYTHOS-FND-SPT-08	Cryptography	Approved cryptography and crypto-agility	Foundational, Advanced, High Assurance	High	Critical
MYTHOS-FND-SPT-09	Privacy	Purpose limitation, minimization, and consent	Foundational, Advanced, High Assurance	Partial	Critical
MYTHOS-FND-SPT-10	Data lifecycle	Retention, deletion, and export protection	Foundational, Advanced, High Assurance	High	Critical

Control	Family	Title	Profiles	Automation	Impact
MYTHOS-FND-SPT-11	Isolation	Tenant, workload, and execution isolation	Advanced, High Assurance	High	Critical
MYTHOS-FND-SPT-12	Secure development	Secure design and implementation lifecycle	Foundational, Advanced, High Assurance	High	Critical
MYTHOS-FND-SPT-13	Supply chain	Software and service supply-chain integrity	Foundational, Advanced, High Assurance	High	Critical
MYTHOS-FND-SPT-14	Telemetry	Security logging, audit, and evidence integrity	Foundational, Advanced, High Assurance	High	Critical
MYTHOS-FND-SPT-15	Exposure management	Vulnerability and exposure management	Foundational, Advanced, High Assurance	High	Critical
MYTHOS-FND-SPT-16	Incident response	Incident response and emergency authority	Foundational, Advanced, High Assurance	Partial	Critical
MYTHOS-FND-SPT-17	Resilience	Backup, recovery, and continuity assurance	Foundational, Advanced, High Assurance	Partial	Critical
MYTHOS-FND-SPT-18	Third parties and automation	Third-party, AI, and delegated-action trust	Advanced, High Assurance	High	Critical
MYTHOS-FND-SPT-19	Assurance	Continuous control assurance and trust claims	Foundational, Advanced, High Assurance	High	Critical

Appendix D – Minimum Conformance Claim Record

```
standard: MYTHOS-FND-0003
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