



ENGINEERING STANDARDS LIBRARY / HARDWARE, ACCELERATED COMPUTE, AND FIRMWARE

Hardware, Accelerated Compute, and Firmware Standards Portfolio

Permanent standards portfolio for hardware, accelerated compute, and firmware.

PERMANENT DOCUMENT ID

MYTHOS-HW-PORT-0001

PUBLICATION

Portfolio Edition
Version 1.0.0-candidate

ASSURANCE PROFILE

Standard / Advanced
High Assurance

PERMANENT PUBLICATION IDENTITY

Hardware, Accelerated Compute, and Firmware Standards Portfolio			DOCUMENT ID MYTHOS-HW-PORT-0001 VERSION 1.0.0-candidate STATUS Portfolio Edition PUBLISHER Mythos Systems PUBLICATION DATE 2026-07-24 SCHEDULED REVIEW 2027-01-24 CLASSIFICATION Public
0 ATOMIC CRITERIA	6 ASSURANCE VIEWS	4 IMPLEMENTATION PROFILES	1 PERMANENT IDENTITY

Publication doctrine. This publication establishes durable requirements for its defined scope. Interpretation must preserve the permanent document identity, required evidence, controlled exceptions, source currency, and formal revision history.

INFRASTRUCTURE AND CONTROL TOPOLOGY

Hardware, Accelerated Compute, and Firmware

A trustworthy hardware, accelerated compute, and firmware standards portfolio system is a governed chain of ownership, identity, desired state, enforcement, workload or device behavior, telemetry, recovery, and independently reviewable evidence.

OWNERSHIP

Purpose, service boundary, accountable owner, suppliers, users, and retained responsibility remain explicit.

ENFORCEMENT

Identity, policy, segmentation, configuration, and local safety mechanisms constrain every trust transition.

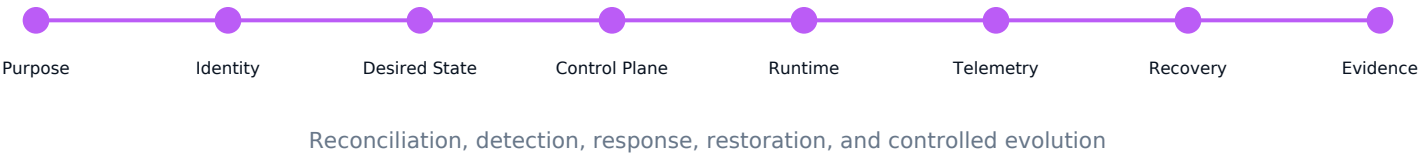
CONTINUITY

Capacity, dependency loss, safe degradation, backup, restoration, rollback, and exit are tested before reliance.

EVIDENCE

Inventory, desired state, runtime observation, tests, incidents, exceptions, and change records form the assurance chain.

GOVERNED INFRASTRUCTURE FLOW



INTERPRETATION AND ASSURANCE

How to apply this publication

Normative intent

Requirements define outcomes and constraints. Implementations may vary, but evidence must demonstrate equivalent control.

Evidence over assertion

Vendor documentation and design intent are not equivalent to reproduced behavior. Record evidence grade and uncertainty.

Risk-proportional depth

Higher consequence, autonomy, sensitivity, and irreversibility require stronger isolation, review, verification, and recovery.

Controlled exception

Exceptions require an owner, rationale, compensating control, residual-risk acceptance, expiration, and reevaluation trigger.

Normalized assessment scale

0	1	2	3	4	5
ABSENT	AD HOC	PARTIAL	OPERATIONAL	ADVANCED	LEADING

A numeric score must never hide a failed mandatory gate, missing evidence, untested workload, or unacceptable residual risk.

MYTHOS-HW-PORT-0001 / HARDWARE AND COMPUTE

Portfolio Position

Permanent standards portfolio for hardware, accelerated compute, and firmware.

OPERATING POSITION

This portfolio consolidates 2 permanent standards for hardware, accelerated compute, and firmware.

- Use it to establish a shared control vocabulary, implementation sequence, evidence profile, and adoption roadmap.
- Individual standards remain independently identifiable and citable.

MYTHOS-HW-PORT-0001 / HARDWARE AND COMPUTE

Portfolio Register

OPERATING POSITION

MYTHOS-HW-0001 - AI GPU Server and Cluster Architecture Standard

- MYTHOS-HW-0002 - Trusted Compute, DPU, and Firmware Standard

MYTHOS-HW-PORT-0001 / HARDWARE AND COMPUTE

Control Architecture

OPERATING POSITION

Reasoning proposes; policy authorizes; deterministic systems execute; evidence records.

- State, identity, sources, and learning remain governed throughout the lifecycle.
- High-consequence use requires stronger isolation, approval, reproducibility, and recovery.

MYTHOS-HW-PORT-0001 / HARDWARE AND COMPUTE

Assurance Model

OPERATING POSITION

Six assurance views: governance, architecture, security, operations, privacy/rights, and human/societal impact.

- Three implementation profiles: Foundational, Advanced, and High Assurance.
- Atomic criteria receive pass, partial, fail, not-applicable, or controlled-exception disposition.

MYTHOS-HW-PORT-0001 / HARDWARE AND COMPUTE

Adoption Sequence

OPERATING POSITION

Establish ownership and inventory.

- Classify consequence and select profile.
- Create enforceable identity, policy, execution, and data boundaries.
- Evaluate representative workloads and adversarial cases.
- Release gradually with rollback and evidence.
- Operate, reassess, and retire with preserved records.

11. Source Authority and Reference Register

Primary sources informing interpretation; current obligations and provider behavior must be verified at assessment time

NIST CSF 2.0 **Cybersecurity Framework 2.0**

<https://doi.org/10.6028/NIST.CSWP.29>
Enterprise governance and cybersecurity outcome framework.

NIST SP 800-53 Rev. 5 **Security and Privacy Controls for Information Systems and Organizations**

<https://doi.org/10.6028/NIST.SP.800-53r5>
Broad control baseline for organizational systems and services.

NIST SP 800-193 **Platform Firmware Resiliency Guidelines**

<https://doi.org/10.6028/NIST.SP.800-193>
Platform firmware protection, detection, and recovery.

TCG TPM 2.0 **Trusted Platform Module Library Specification**

<https://trustedcomputinggroup.org/resource/tpm-library-specification/>
TPM commands, objects, measurement, keys, and attestation foundations.

DMTF Redfish **Redfish Standard**

<https://www.dmtf.org/standards/redfish>
Secure and interoperable hardware-management interfaces.

NIST SP 800-155 **BIOS Integrity Measurement Guidelines**

<https://doi.org/10.6028/NIST.SP.800-155>
Firmware measurement and integrity-verification principles.

Source currency rule: authorities, specifications, legal obligations, provider services, firmware, browser behavior, carrier requirements, and operational evidence MUST be checked at assessment time. This publication records a 2026-07-24 source snapshot.



ENGINEERING STANDARDS LIBRARY / HARDWARE, ACCELERATED COMPUTE, AND FIRMWARE

AI GPU Server and Cluster Architecture Standard



Accelerated-compute topology, fabric, storage, scheduling, isolation, power, cooling, benchmarks, resilience, and lifecycle evidence.

PERMANENT DOCUMENT ID

MYTHOS-HW-0001

PUBLICATION

Candidate Standard
Version 1.0.0-candidate

ASSURANCE PROFILE

Standard / Advanced
High Assurance

PERMANENT PUBLICATION IDENTITY

AI GPU Server and Cluster Architecture Standard			DOCUMENT ID MYTHOS-HW-0001
			VERSION 1.0.0-candidate
			STATUS Candidate Standard
			PUBLISHER Mythos Systems
			PUBLICATION DATE 2026-07-24
			SCHEDULED REVIEW 2027-01-24
			CLASSIFICATION Public
18 ATOMIC CRITERIA	6 ASSURANCE VIEWS	4 IMPLEMENTATION PROFILES	1 PERMANENT IDENTITY

Publication doctrine. This publication establishes durable requirements for its defined scope. Interpretation must preserve the permanent document identity, required evidence, controlled exceptions, source currency, and formal revision history.

INFRASTRUCTURE AND CONTROL TOPOLOGY

Hardware, Accelerated Compute, and Firmware

A trustworthy AI GPU server and cluster architecture system is a governed chain of ownership, identity, desired state, enforcement, workload or device behavior, telemetry, recovery, and independently reviewable evidence.

OWNERSHIP

Purpose, service boundary, accountable owner, suppliers, users, and retained responsibility remain explicit.

ENFORCEMENT

Identity, policy, segmentation, configuration, and local safety mechanisms constrain every trust transition.

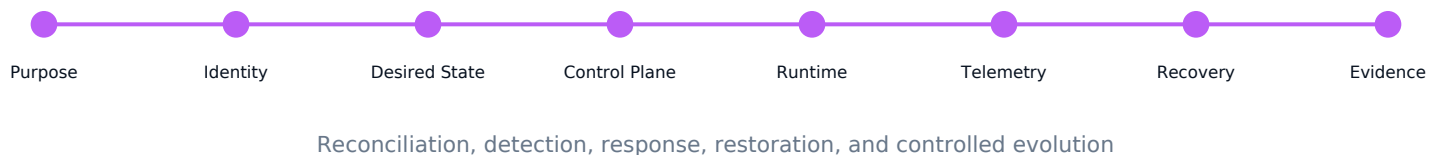
CONTINUITY

Capacity, dependency loss, safe degradation, backup, restoration, rollback, and exit are tested before reliance.

EVIDENCE

Inventory, desired state, runtime observation, tests, incidents, exceptions, and change records form the assurance chain.

GOVERNED INFRASTRUCTURE FLOW



INTERPRETATION AND ASSURANCE

How to apply this publication

Normative intent

Requirements define outcomes and constraints. Implementations may vary, but evidence must demonstrate equivalent control.

Evidence over assertion

Vendor documentation and design intent are not equivalent to reproduced behavior. Record evidence grade and uncertainty.

Risk-proportional depth

Higher consequence, autonomy, sensitivity, and irreversibility require stronger isolation, review, verification, and recovery.

Controlled exception

Exceptions require an owner, rationale, compensating control, residual-risk acceptance, expiration, and reevaluation trigger.

Normalized assessment scale



A numeric score must never hide a failed mandatory gate, missing evidence, untested workload, or unacceptable residual risk.

INTERACTIVE NAVIGATION

Contents

Executive mandate	6
Scope and applicability	7
Definitions and taxonomy	8
Architecture and trust model	9
Governance and accountability	10
Normative control system	11
Evidence and assessment	16
Assurance views and metrics	17
Failure modes and adversarial scenarios	19
Implementation profiles and lifecycle	20
Adoption roadmap and conformance	22
Source authority and revision control	24

Navigation doctrine

Bookmarks and internal links are conveniences. Permanent document identity, criterion identifiers, evidence references, and revision history remain authoritative.

MYTHOS-HW-0001 / HARDWARE AND COMPUTE

0. Executive Mandate

Purpose, strategic outcome, and non-negotiable operating doctrine

MANDATE

Organizations adopting AI GPU server and cluster architecture capabilities **MUST** define an owned service boundary, establish enforceable identity and configuration, protect data and safety, test failure and recovery, and preserve evidence sufficient for independent review.

Required outcomes

- Create a durable governance boundary for AI GPU server and cluster architecture across design, acquisition, deployment, operation, change, and retirement.
- Require risk-proportional segmentation, identity, configuration, telemetry, resilience, recovery, and supplier controls.
- Prevent central automation, administrative tooling, or provider services from becoming unbounded authority.
- Prove operation with representative workloads, devices, failure modes, and restoration exercises.
- Define measurable conformance, exceptions, reassessment triggers, and a viable exit path.

Decision boundary: conformance supports a documented assurance claim for the named scope. It does not prove universal availability, safety, regulatory acceptance, vendor fitness, or immunity from cyber-physical failure.

MYTHOS-HW-0001 / HARDWARE AND COMPUTE

1. Scope and Applicability

Boundary definition, audience, exclusions, and triggering conditions

IN SCOPE

- Architecture, acquisition, configuration, integration, and operation of AI GPU server and cluster architecture capabilities.
- Human, workload, device, service, network, data, facility, provider, supplier, and evidence dependencies.
- Design, deployment, monitoring, support, incident response, recovery, migration, and retirement.
- On-premises, hosted, managed, carrier, manufacturer, integrator, and externally operated components.

OUT OF SCOPE

- Claims of legal, safety, carrier, or regulatory approval without the responsible authority.
- Vendor certification treated as proof of the adopter configuration or operating effectiveness.
- Theoretical or laboratory behavior presented as production evidence without a declared boundary.
- Inherited controls without documented scope, owner, period, limitations, and shared responsibility.

Applicability triggers

- The capability supports a business-critical, safety-relevant, regulated, public, or externally dependent service.
- The environment can expose sensitive data, identity, control, physical process, communications, or shared infrastructure.
- A management plane, automation system, carrier, provider, or supplier can affect broad operational scope.
- Failure, compromise, or change can be difficult to detect, reverse, isolate, or recover.
- The system depends on hardware, firmware, radio, browser, cloud, endpoint, IoT, OT, or real-time media behavior.

MYTHOS-HW-0001 / HARDWARE AND COMPUTE

2. Definitions and Taxonomy

Controlled language for architecture, governance, and assessment

AUTHORITY

The right to approve, deny, constrain, or execute an action. Model output is not authority.

EVIDENCE

A reproducible source, trace, measurement, test, record, signed artifact, or documented observation supporting a claim.

ASSURANCE VIEW

A defined perspective such as governance, architecture, security, operations, privacy, or human oversight.

ATOMIC CRITERION

A uniquely identified requirement that can be assessed, evidenced, excepted, and revised independently.

IMPLEMENTATION PROFILE

A risk-proportional set of required depth, evidence, and gates for a class of use.

CONTROLLED EXCEPTION

A time-bounded deviation with owner, rationale, compensating control, residual risk, expiration, and review trigger.

DETERMINISTIC MECHANISM

A component whose inputs, policy, state transition, and side effects can be constrained and verified.

SOURCE AUTHORITY

The documented basis for treating a source as reliable for a defined claim, context, jurisdiction, and time.

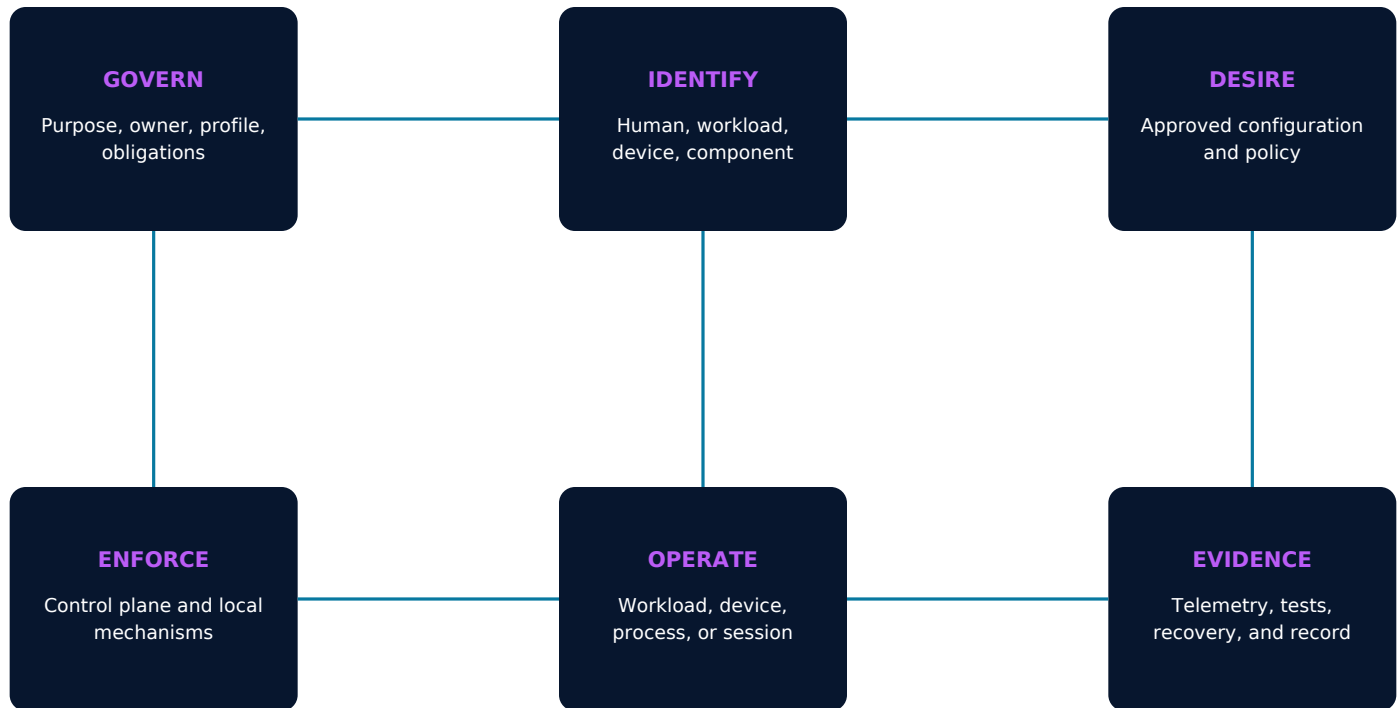
REASSESSMENT TRIGGER

A change, incident, drift signal, dependency revision, or time boundary requiring renewed evaluation.

MYTHOS-HW-0001 / HARDWARE AND COMPUTE

3. Architecture and Trust Model

Separation of governance, management, enforcement, runtime, telemetry, and recovery



Mandatory trust boundaries

- Management planes **MUST** be isolated, strongly authenticated, monitored, and recoverable.
- Identity and policy **MUST** be evaluated at every provider, network, device, workload, and administrative transition.
- Runtime state **MUST** be compared with approved desired state and material drift **MUST** trigger response.
- Safety and continuity mechanisms **MUST** remain available when cloud, WAN, identity, DNS, time, carrier, or management dependencies fail.
- Evidence **MUST** be protected from the systems and administrators whose behavior it is intended to assess.

MYTHOS-HW-0001 / HARDWARE AND COMPUTE

4. Governance and Accountability

Decision rights, separation of duties, and lifecycle ownership

ACCOUNTABLE OWNER

Accepts scope, risk tolerance, funding, and residual risk.

SYSTEM OWNER

Maintains architecture, inventory, operating boundaries, and change control.

SECURITY / PRIVACY

Defines threat, identity, data, isolation, monitoring, and incident requirements.

EVALUATION AUTHORITY

Designs representative tests, gates releases, and preserves reproducibility.

OPERATIONS

Maintains availability, rollback, recovery, evidence, and incident handling.

HUMAN OVERSIGHT

Reviews consequential decisions, exceptions, disputed outcomes, and harm signals.

DECISION PRINCIPLE

No single actor should be able to define the objective, grant authority, execute the consequential action, suppress evidence, and approve the result. Separation must be technical where consequence requires it.

MYTHOS-HW-0001 / HARDWARE AND COMPUTE

5. Normative Control System

Atomic criteria 01-04 of 18

MYTHOS-HW-0001-C01**Workload, Model, and Service-Level Requirements**

The organization **MUST** define, implement, verify, and maintain workload, model, and service-level requirements for in-scope AI GPU server and cluster architecture capabilities. The control boundary **MUST** identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE approved service contract; architecture decision; owner and risk sign-off

MYTHOS-HW-0001-C02**Accelerator, CPU, Memory, and Platform Selection**

The organization **MUST** define, implement, verify, and maintain accelerator, cpu, memory, and platform selection for in-scope AI GPU server and cluster architecture capabilities. The control boundary **MUST** identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE asset, service, dependency, supplier, region, and lifecycle inventory

MYTHOS-HW-0001-C03**Node Topology, NUMA, PCIe, and CXL Design**

The organization **MUST** define, implement, verify, and maintain node topology, numa, pcie, and cxl design for in-scope AI GPU server and cluster architecture capabilities. The control boundary **MUST** identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE desired-state configuration; policy evidence; privileged-access and negative tests

MYTHOS-HW-0001-C04**Scale-Up and Scale-Out Fabric Architecture**

The organization **MUST** define, implement, verify, and maintain scale-up and scale-out fabric architecture for in-scope AI GPU server and cluster architecture capabilities. The control boundary **MUST** identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE network, data-flow, zone, conduit, radio, device, or trust-boundary diagrams

MYTHOS-HW-0001 / HARDWARE AND COMPUTE

5. Normative Control System

Atomic criteria 05-08 of 18

MYTHOS-HW-0001-C05**RDMA, Congestion, and Lossless-Network Control**

The organization **MUST** define, implement, verify, and maintain rdma, congestion, and lossless-network control for in-scope AI GPU server and cluster architecture capabilities. The control boundary **MUST** identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE runtime logs, traces, metrics, alarms, quality, capacity, and drift evidence

MYTHOS-HW-0001-C06**Storage, Dataset, Checkpoint, and Cache Architecture**

The organization **MUST** define, implement, verify, and maintain storage, dataset, checkpoint, and cache architecture for in-scope AI GPU server and cluster architecture capabilities. The control boundary **MUST** identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE failure, failover, rollback, restoration, revocation, and recovery exercise

MYTHOS-HW-0001-C07**Scheduler, Queue, Quota, and Admission Policy**

The organization **MUST** define, implement, verify, and maintain scheduler, queue, quota, and admission policy for in-scope AI GPU server and cluster architecture capabilities. The control boundary **MUST** identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE safety, privacy, residency, consent, or physical-impact assessment

MYTHOS-HW-0001-C08**Tenant, Job, Model, and Data Isolation**

The organization **MUST** define, implement, verify, and maintain tenant, job, model, and data isolation for in-scope AI GPU server and cluster architecture capabilities. The control boundary **MUST** identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE supplier, carrier, firmware, license, support, portability, and exit evidence

MYTHOS-HW-0001 / HARDWARE AND COMPUTE

5. Normative Control System

Atomic criteria 09-12 of 18

MYTHOS-HW-0001-C09 Driver, Runtime, Library, and Compatibility Matrix

The organization **MUST** define, implement, verify, and maintain driver, runtime, library, and compatibility matrix for in-scope AI GPU server and cluster architecture capabilities. The control boundary **MUST** identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE approved service contract; architecture decision; owner and risk sign-off

MYTHOS-HW-0001-C10 Image, Container, and Artifact Provenance

The organization **MUST** define, implement, verify, and maintain image, container, and artifact provenance for in-scope AI GPU server and cluster architecture capabilities. The control boundary **MUST** identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE asset, service, dependency, supplier, region, and lifecycle inventory

MYTHOS-HW-0001-C11 Power, Cooling, Rack, and Facility Capacity

The organization **MUST** define, implement, verify, and maintain power, cooling, rack, and facility capacity for in-scope AI GPU server and cluster architecture capabilities. The control boundary **MUST** identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE desired-state configuration; policy evidence; privileged-access and negative tests

MYTHOS-HW-0001-C12 Thermal, ECC, Link, and Hardware Health Monitoring

The organization **MUST** define, implement, verify, and maintain thermal, ecc, link, and hardware health monitoring for in-scope AI GPU server and cluster architecture capabilities. The control boundary **MUST** identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE network, data-flow, zone, conduit, radio, device, or trust-boundary diagrams

MYTHOS-HW-0001 / HARDWARE AND COMPUTE

5. Normative Control System

Atomic criteria 13-15 of 18

MYTHOS-HW-0001-C13 **Representative Benchmark and Scaling Efficiency**

The organization **MUST** define, implement, verify, and maintain representative benchmark and scaling efficiency for in-scope AI GPU server and cluster architecture capabilities. The control boundary **MUST** identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE runtime logs, traces, metrics, alarms, quality, capacity, and drift evidence

MYTHOS-HW-0001-C14 **Failure Injection, Job Recovery, and Checkpoint Restore**

The organization **MUST** define, implement, verify, and maintain failure injection, job recovery, and checkpoint restore for in-scope AI GPU server and cluster architecture capabilities. The control boundary **MUST** identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE failure, failover, rollback, restoration, revocation, and recovery exercise

MYTHOS-HW-0001-C15 **Capacity Planning, Energy, and Cost per Useful Result**

The organization **MUST** define, implement, verify, and maintain capacity planning, energy, and cost per useful result for in-scope AI GPU server and cluster architecture capabilities. The control boundary **MUST** identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE safety, privacy, residency, consent, or physical-impact assessment

MYTHOS-HW-0001 / HARDWARE AND COMPUTE

5. Normative Control System

Atomic criteria 16-18 of 18

MYTHOS-HW-0001-C16**Administrative Access and Out-of-Band Control**

The organization **MUST** define, implement, verify, and maintain administrative access and out-of-band control for in-scope AI GPU server and cluster architecture capabilities. The control boundary **MUST** identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE supplier, carrier, firmware, license, support, portability, and exit evidence

MYTHOS-HW-0001-C17**Spares, Firmware, Repair, and End-of-Life**

The organization **MUST** define, implement, verify, and maintain spares, firmware, repair, and end-of-life for in-scope AI GPU server and cluster architecture capabilities. The control boundary **MUST** identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE approved service contract; architecture decision; owner and risk sign-off

MYTHOS-HW-0001-C18**Cluster Evidence and Periodic Requalification**

The organization **MUST** define, implement, verify, and maintain cluster evidence and periodic requalification for in-scope AI GPU server and cluster architecture capabilities. The control boundary **MUST** identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE asset, service, dependency, supplier, region, and lifecycle inventory

MYTHOS-HW-0001 / HARDWARE AND COMPUTE

6. Evidence and Assessment

Examine, interview, test, observe, restore, and trace

EXAMINE

Policies, inventories, diagrams, configuration, code, firmware, contracts, provider evidence, logs, exceptions, and lifecycle records.

INTERVIEW

Accountable owners, architects, engineers, operators, safety personnel, security teams, vendors, carriers, integrators, and responders.

TEST

Identity, segmentation, policy, negative paths, malformed input, capacity stress, dependency loss, failover, rollback, and revocation.

RESTORE

Independent restoration of configuration, data, service, device, controller, cluster, media, or browser state from protected evidence.

OBSERVE

Production-like performance, quality, drift, resource use, physical behavior, alarms, user impact, and incident execution.

TRACE

End-to-end linkage from approved intent and identity through change, runtime behavior, telemetry, outcome, exception, and review.

Evidence grades

A

Independently reproducible, complete, current, integrity-protected, and representative.

B

Reproduced by the implementing organization with strong traceability and controlled scope.

C

Partially reproduced or indirect; limitations, inherited responsibility, and uncertainty recorded.

D

Assertion, diagram, design intent, certificate, or vendor statement without reproduced behavior.

MYTHOS-HW-0001 / HARDWARE AND COMPUTE

7. Assurance Views

Six perspectives required for a complete assurance claim

GOVERNANCE

Ownership, purpose, risk tolerance, policy, exception, and decision rights.

ARCHITECTURE

Boundaries, dependencies, failure modes, state, data flow, and portability.

SECURITY

Identity, authorization, isolation, secrets, abuse resistance, and incident response.

OPERATIONS

Reliability, performance, cost, observability, change, recovery, and support.

PRIVACY / RIGHTS

Purpose limitation, minimization, consent, access, correction, deletion, and egress.

HUMAN / SOCIETAL

Usability, accessibility, disclosure, contestability, impact, and human control.

Conformance requires a defensible position across every applicable view. A strong aggregate score cannot compensate for an unowned system, a failed mandatory gate, untested recovery, or evidence below the accepted grade.

MYTHOS-HW-0001 / HARDWARE AND COMPUTE

7.2 Evaluation Metrics and Decision Gates

Measures must expose service behavior, control effectiveness, failure, uncertainty, and cost

SERVICE

Availability, correctness, coverage, quality, latency, throughput, and user or process outcome.

CONTROL

Unauthorized attempt, policy denial, drift, segmentation escape, privilege, and exception exposure.

RESILIENCE

Failover success, recovery time, data loss, safe degradation, restore validity, and dependency survival.

SECURITY

Exploitability, credential exposure, supply-chain integrity, attack detection, containment, and revocation.

CAPACITY

Utilization, saturation, queueing, radio or fabric headroom, thermal margin, quota, and forecast error.

OPERATIONS

Change failure, mean time to detect, repair, support burden, vendor escalation, and evidence completeness.

PRIVACY / SAFETY

Unauthorized egress, retention breach, consent coverage, unsafe action, physical consequence, and contestability.

LIFECYCLE

Patch debt, end-of-support exposure, portability, replacement time, retirement completion, and reassessment age.

Decision gate: thresholds **MUST** be declared before assessment, cover representative load and failure conditions, and identify mandatory safety, identity, recovery, and evidence failures that block promotion.

MYTHOS-HW-0001 / HARDWARE AND COMPUTE

8. Failure Modes and Adversarial Scenarios

Challenge assumptions before the system is trusted with consequential work

BMC COMPROMISE

Out-of-band management provides persistent control beneath the operating system.

REQUIRED: PREVENT | DETECT | CONTAIN | RECOVER | EVIDENCE

FIRMWARE SUPPLY-CHAIN ATTACK

Signed or trusted firmware is malicious, vulnerable, or incorrectly sourced.

REQUIRED: PREVENT | DETECT | CONTAIN | RECOVER | EVIDENCE

DMA BOUNDARY BYPASS

A device accesses memory outside its assigned trust domain.

REQUIRED: PREVENT | DETECT | CONTAIN | RECOVER | EVIDENCE

ATTESTATION REPLAY

Stale or forged evidence causes keys or workloads to be released to an untrusted platform.

REQUIRED: PREVENT | DETECT | CONTAIN | RECOVER | EVIDENCE

POWER OR THERMAL COLLAPSE

Facility or rack constraints create correlated hardware failure.

REQUIRED: PREVENT | DETECT | CONTAIN | RECOVER | EVIDENCE

CROSS-TENANT LEAKAGE

Scheduler, cache, fabric, storage, or diagnostics expose another workload.

REQUIRED: PREVENT | DETECT | CONTAIN | RECOVER | EVIDENCE

Adversarial testing MUST protect people and production systems. Use isolated environments, synthetic or minimized data, bounded authority, kill switches, explicit legal and ethical review, and documented stop conditions.

9. Implementation Profiles

Risk-proportional implementation without weakening mandatory boundaries

FOUNDATIONAL	ADVANCED	HIGH ASSURANCE
TYPICAL SCOPE Low consequence, limited autonomy, non-sensitive data, reversible outputs.	TYPICAL SCOPE Business-critical workflow, sensitive data, multiple tools or providers, moderate autonomy.	TYPICAL SCOPE Safety, security, regulated, financial, identity, or broadly consequential use.
MINIMUM DEPTH Named owner; inventory; basic evaluation; access control; logging; rollback; annual review.	MINIMUM DEPTH Formal threat model; representative evaluation; approval gates; isolated execution; tested recovery; quarterly review.	MINIMUM DEPTH Independent challenge; strongest identity; deterministic enforcement; comprehensive evidence; canary release; continuous monitoring.

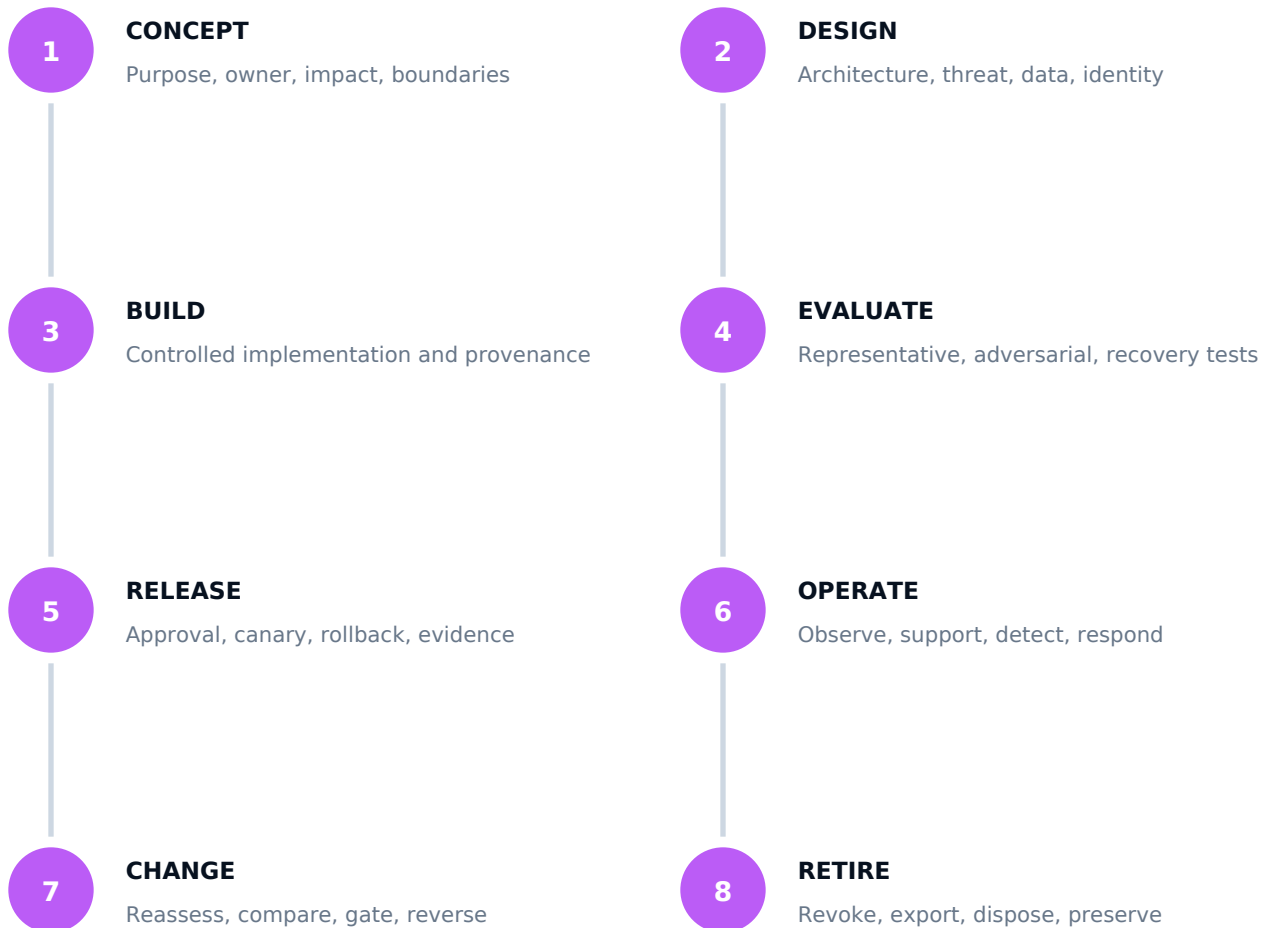
Profile selection rule

Choose the highest profile triggered by consequence, autonomy, sensitivity, scale, irreversibility, external dependency, or inability to rapidly detect and recover. Tailoring may strengthen controls; it may not erase a mandatory gate without a controlled exception.

MYTHOS-HW-0001 / HARDWARE AND COMPUTE

9.2 Operational Lifecycle

Evidence-bearing operation from concept through retirement



LIFECYCLE INVARIANT

Every stage **MUST** leave sufficient evidence for the next authority to understand what was intended, what changed, what was tested, what failed, what was accepted, what remains uncertain, and how to recover or exit.

MYTHOS-HW-0001 / HARDWARE AND COMPUTE

10. Adoption Roadmap

A sequenced path from uncontrolled capability to evidence-bearing operation

0-30 DAYS**Establish ownership and truth**

Inventory systems and dependencies; classify risk; freeze unsupported claims; identify immediate privilege, data, and evidence gaps.

31-90 DAYS**Create enforceable boundaries**

Define policy; isolate execution; implement identity and approval gates; establish representative evaluation and baseline telemetry.

3-6 MONTHS**Prove recovery and operating control**

Exercise failure, rollback, revocation, incident, provider exit, and state-recovery scenarios; mature evidence packaging.

6-12 MONTHS**Scale assurance**

Automate control checks; expand workload coverage; independent challenge; portfolio metrics; controlled exception expiry; continuous reassessment.

Adoption is complete only when operating evidence demonstrates the selected profile in the actual deployment context. Documentation alone is not conformance.

MYTHOS-HW-0001 / HARDWARE AND COMPUTE

10.2 Conformance and Exception Statement

What an assurance claim must contain

SYSTEM / SERVICE Named, versioned capability and deployment boundary.	PROFILE Foundational, Advanced, or High Assurance with trigger rationale.
SCOPE Workloads, users, data, tools, regions, providers, and exclusions.	CRITERIA Pass, partial, fail, not applicable, and exception status for every criterion.
EVIDENCE Artifact references, evidence grade, date, environment, and reproducibility.	LIMITATIONS Known failure modes, unsupported workloads, uncertainty, and residual risk.
EXCEPTIONS Owner, rationale, compensating control, expiration, and approval.	VALIDITY Assessment date, change boundary, review date, and reassessment triggers.

Prohibited claim: “compliant” without the named scope, profile, evidence date, limitations, exceptions, and authority accepting residual risk.

MYTHOS-HW-0001 / HARDWARE AND COMPUTE

11. Source Authority and Reference Register

Primary sources informing interpretation; current obligations and provider behavior must be verified at assessment time

NIST CSF 2.0

Cybersecurity Framework 2.0

<https://doi.org/10.6028/NIST.CSWP.29>

Enterprise governance and cybersecurity outcome framework.

NIST SP 800-53 Rev. 5

Security and Privacy Controls for Information Systems and Organizations

<https://doi.org/10.6028/NIST.SP.800-53r5>

Broad control baseline for organizational systems and services.

NIST SP 800-193

Platform Firmware Resiliency Guidelines

<https://doi.org/10.6028/NIST.SP.800-193>

Platform firmware protection, detection, and recovery.

TCG TPM 2.0

Trusted Platform Module Library Specification

<https://trustedcomputinggroup.org/resource/tpm-library-specification/>

TPM commands, objects, measurement, keys, and attestation foundations.

DMTF Redfish

Redfish Standard

<https://www.dmtf.org/standards/redfish>

Secure and interoperable hardware-management interfaces.

NIST SP 800-155

BIOS Integrity Measurement Guidelines

<https://doi.org/10.6028/NIST.SP.800-155>

Firmware measurement and integrity-verification principles.

Source currency rule: authorities, specifications, legal obligations, provider services, firmware, browser behavior, carrier requirements, and operational evidence MUST be checked at assessment time. This publication records a 2026-07-24 source snapshot.

MYTHOS-HW-0001 / HARDWARE AND COMPUTE

11.2 Revision History and Decision Register

Permanent identity, controlled change, and publication integrity

VERSION	DATE	STATE	SUMMARY
1.0.0-candidate	2026-07-24	Candidate	Permanent-publication edition; source refresh; expanded criteria, evidence, assurance, and lifecycle guidance.
Next review	2027-01-24	Scheduled	Review source currency, threat evolution, operating evidence, adoption feedback, and proposed revisions.

Publication decisions

- PERMANENT IDENTITY** The document ID remains stable across revisions; batch or production sequence metadata is not public identity.
- CHANGE CONTROL** Normative changes require rationale, impact analysis, affected-criterion mapping, and approval.
- SUPERSESSION** A superseded edition remains traceable; current routes and catalogs identify the active edition.
- CORRECTION** Material errors require a recorded correction, affected-evidence analysis, and notification appropriate to impact.
- ARCHIVAL INTEGRITY** Published artifacts receive hashes, metadata, and a release manifest sufficient for independent verification.

END OF PERMANENT PUBLICATION / MYTHOS-HW-0001

MYTHOS SYSTEMS / ENGINEERING STANDARDS LIBRARY



ENGINEERING STANDARDS LIBRARY / HARDWARE, ACCELERATED COMPUTE, AND FIRMWARE

Trusted Compute, DPU, and Firmware Standard

Roots of trust, secure and measured boot, attestation, BMC, DPU, DMA isolation, confidential computing, firmware, and lifecycle assurance.

PERMANENT DOCUMENT ID

MYTHOS-HW-0002

PUBLICATION

Candidate Standard
Version 1.0.0-candidate

ASSURANCE PROFILE

Standard / Advanced
High Assurance

PERMANENT PUBLICATION IDENTITY

Trusted Compute, DPU, and Firmware Standard			DOCUMENT ID MYTHOS-HW-0002 VERSION 1.0.0-candidate STATUS Candidate Standard PUBLISHER Mythos Systems PUBLICATION DATE 2026-07-24 SCHEDULED REVIEW 2027-01-24 CLASSIFICATION Public
18 ATOMIC CRITERIA	6 ASSURANCE VIEWS	4 IMPLEMENTATION PROFILES	1 PERMANENT IDENTITY

Publication doctrine. This publication establishes durable requirements for its defined scope. Interpretation must preserve the permanent document identity, required evidence, controlled exceptions, source currency, and formal revision history.

INFRASTRUCTURE AND CONTROL TOPOLOGY

Hardware, Accelerated Compute, and Firmware

A trustworthy trusted compute, DPU, and firmware system is a governed chain of ownership, identity, desired state, enforcement, workload or device behavior, telemetry, recovery, and independently reviewable evidence.

OWNERSHIP

Purpose, service boundary, accountable owner, suppliers, users, and retained responsibility remain explicit.

ENFORCEMENT

Identity, policy, segmentation, configuration, and local safety mechanisms constrain every trust transition.

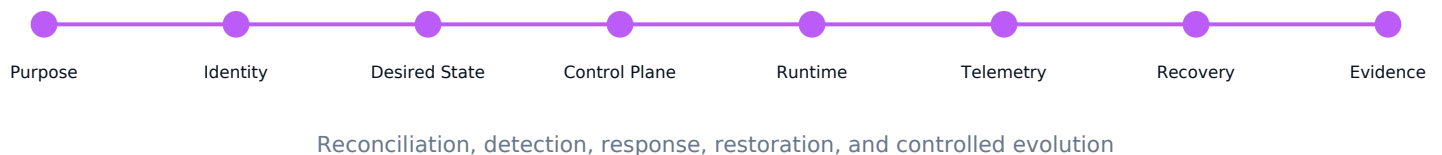
CONTINUITY

Capacity, dependency loss, safe degradation, backup, restoration, rollback, and exit are tested before reliance.

EVIDENCE

Inventory, desired state, runtime observation, tests, incidents, exceptions, and change records form the assurance chain.

GOVERNED INFRASTRUCTURE FLOW



INTERPRETATION AND ASSURANCE

How to apply this publication

Normative intent

Requirements define outcomes and constraints. Implementations may vary, but evidence must demonstrate equivalent control.

Evidence over assertion

Vendor documentation and design intent are not equivalent to reproduced behavior. Record evidence grade and uncertainty.

Risk-proportional depth

Higher consequence, autonomy, sensitivity, and irreversibility require stronger isolation, review, verification, and recovery.

Controlled exception

Exceptions require an owner, rationale, compensating control, residual-risk acceptance, expiration, and reevaluation trigger.

Normalized assessment scale



A numeric score must never hide a failed mandatory gate, missing evidence, untested workload, or unacceptable residual risk.

INTERACTIVE NAVIGATION

Contents

Executive mandate	6
Scope and applicability	7
Definitions and taxonomy	8
Architecture and trust model	9
Governance and accountability	10
Normative control system	11
Evidence and assessment	16
Assurance views and metrics	17
Failure modes and adversarial scenarios	19
Implementation profiles and lifecycle	20
Adoption roadmap and conformance	22
Source authority and revision control	24

Navigation doctrine

Bookmarks and internal links are conveniences. Permanent document identity, criterion identifiers, evidence references, and revision history remain authoritative.

MYTHOS-HW-0002 / HARDWARE AND COMPUTE

0. Executive Mandate

Purpose, strategic outcome, and non-negotiable operating doctrine

MANDATE

Organizations adopting trusted compute, DPU, and firmware capabilities **MUST** define an owned service boundary, establish enforceable identity and configuration, protect data and safety, test failure and recovery, and preserve evidence sufficient for independent review.

Required outcomes

- Create a durable governance boundary for trusted compute, DPU, and firmware across design, acquisition, deployment, operation, change, and retirement.
- Require risk-proportional segmentation, identity, configuration, telemetry, resilience, recovery, and supplier controls.
- Prevent central automation, administrative tooling, or provider services from becoming unbounded authority.
- Prove operation with representative workloads, devices, failure modes, and restoration exercises.
- Define measurable conformance, exceptions, reassessment triggers, and a viable exit path.

Decision boundary: conformance supports a documented assurance claim for the named scope. It does not prove universal availability, safety, regulatory acceptance, vendor fitness, or immunity from cyber-physical failure.

MYTHOS-HW-0002 / HARDWARE AND COMPUTE

1. Scope and Applicability

Boundary definition, audience, exclusions, and triggering conditions

IN SCOPE

- Architecture, acquisition, configuration, integration, and operation of trusted compute, DPU, and firmware capabilities.
- Human, workload, device, service, network, data, facility, provider, supplier, and evidence dependencies.
- Design, deployment, monitoring, support, incident response, recovery, migration, and retirement.
- On-premises, hosted, managed, carrier, manufacturer, integrator, and externally operated components.

OUT OF SCOPE

- Claims of legal, safety, carrier, or regulatory approval without the responsible authority.
- Vendor certification treated as proof of the adopter configuration or operating effectiveness.
- Theoretical or laboratory behavior presented as production evidence without a declared boundary.
- Inherited controls without documented scope, owner, period, limitations, and shared responsibility.

Applicability triggers

- The capability supports a business-critical, safety-relevant, regulated, public, or externally dependent service.
- The environment can expose sensitive data, identity, control, physical process, communications, or shared infrastructure.
- A management plane, automation system, carrier, provider, or supplier can affect broad operational scope.
- Failure, compromise, or change can be difficult to detect, reverse, isolate, or recover.
- The system depends on hardware, firmware, radio, browser, cloud, endpoint, IoT, OT, or real-time media behavior.

MYTHOS-HW-0002 / HARDWARE AND COMPUTE

2. Definitions and Taxonomy

Controlled language for architecture, governance, and assessment

AUTHORITY

The right to approve, deny, constrain, or execute an action. Model output is not authority.

EVIDENCE

A reproducible source, trace, measurement, test, record, signed artifact, or documented observation supporting a claim.

ASSURANCE VIEW

A defined perspective such as governance, architecture, security, operations, privacy, or human oversight.

ATOMIC CRITERION

A uniquely identified requirement that can be assessed, evidenced, excepted, and revised independently.

IMPLEMENTATION PROFILE

A risk-proportional set of required depth, evidence, and gates for a class of use.

CONTROLLED EXCEPTION

A time-bounded deviation with owner, rationale, compensating control, residual risk, expiration, and review trigger.

DETERMINISTIC MECHANISM

A component whose inputs, policy, state transition, and side effects can be constrained and verified.

SOURCE AUTHORITY

The documented basis for treating a source as reliable for a defined claim, context, jurisdiction, and time.

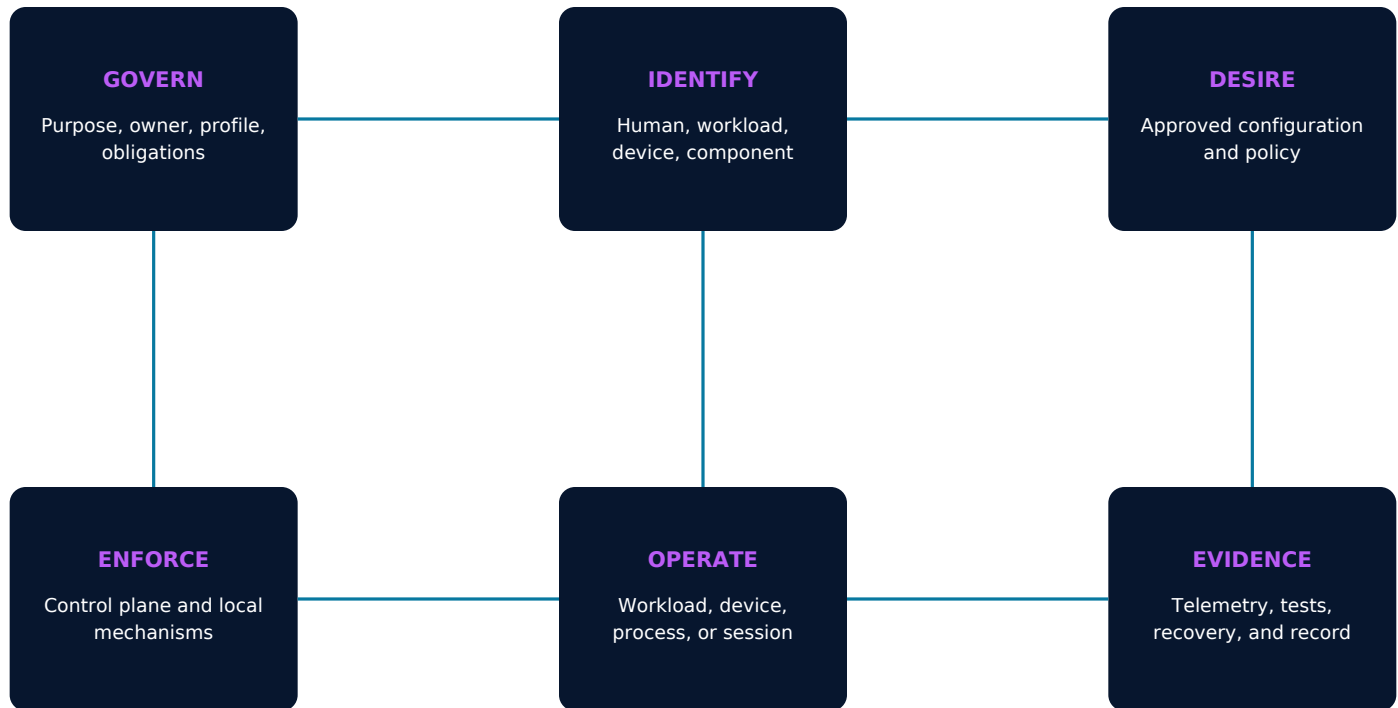
REASSESSMENT TRIGGER

A change, incident, drift signal, dependency revision, or time boundary requiring renewed evaluation.

MYTHOS-HW-0002 / HARDWARE AND COMPUTE

3. Architecture and Trust Model

Separation of governance, management, enforcement, runtime, telemetry, and recovery



Mandatory trust boundaries

- Management planes **MUST** be isolated, strongly authenticated, monitored, and recoverable.
- Identity and policy **MUST** be evaluated at every provider, network, device, workload, and administrative transition.
- Runtime state **MUST** be compared with approved desired state and material drift **MUST** trigger response.
- Safety and continuity mechanisms **MUST** remain available when cloud, WAN, identity, DNS, time, carrier, or management dependencies fail.
- Evidence **MUST** be protected from the systems and administrators whose behavior it is intended to assess.

MYTHOS-HW-0002 / HARDWARE AND COMPUTE

4. Governance and Accountability

Decision rights, separation of duties, and lifecycle ownership

ACCOUNTABLE OWNER

Accepts scope, risk tolerance, funding, and residual risk.

SYSTEM OWNER

Maintains architecture, inventory, operating boundaries, and change control.

SECURITY / PRIVACY

Defines threat, identity, data, isolation, monitoring, and incident requirements.

EVALUATION AUTHORITY

Designs representative tests, gates releases, and preserves reproducibility.

OPERATIONS

Maintains availability, rollback, recovery, evidence, and incident handling.

HUMAN OVERSIGHT

Reviews consequential decisions, exceptions, disputed outcomes, and harm signals.

DECISION PRINCIPLE

No single actor should be able to define the objective, grant authority, execute the consequential action, suppress evidence, and approve the result. Separation must be technical where consequence requires it.

MYTHOS-HW-0002 / HARDWARE AND COMPUTE

5. Normative Control System

Atomic criteria 01-04 of 18

MYTHOS-HW-0002-C01

Hardware Trust Model and Component Inventory

The organization **MUST** define, implement, verify, and maintain hardware trust model and component inventory for in-scope trusted compute, DPU, and firmware capabilities. The control boundary **MUST** identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE approved service contract; architecture decision; owner and risk sign-off

MYTHOS-HW-0002-C02

Root of Trust, TPM, DICE, and Endorsement Identity

The organization **MUST** define, implement, verify, and maintain root of trust, tpm, dice, and endorsement identity for in-scope trusted compute, DPU, and firmware capabilities. The control boundary **MUST** identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE asset, service, dependency, supplier, region, and lifecycle inventory

MYTHOS-HW-0002-C03

Secure Boot, Measured Boot, and Reference Values

The organization **MUST** define, implement, verify, and maintain secure boot, measured boot, and reference values for in-scope trusted compute, DPU, and firmware capabilities. The control boundary **MUST** identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE desired-state configuration; policy evidence; privileged-access and negative tests

MYTHOS-HW-0002-C04

Remote Attestation and Verifier Policy

The organization **MUST** define, implement, verify, and maintain remote attestation and verifier policy for in-scope trusted compute, DPU, and firmware capabilities. The control boundary **MUST** identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE network, data-flow, zone, conduit, radio, device, or trust-boundary diagrams

MYTHOS-HW-0002 / HARDWARE AND COMPUTE

5. Normative Control System

Atomic criteria 05-08 of 18

MYTHOS-HW-0002-C05**BMC, Service Processor, and Out-of-Band Isolation**

The organization **MUST** define, implement, verify, and maintain bmc, service processor, and out-of-band isolation for in-scope trusted compute, DPU, and firmware capabilities. The control boundary **MUST** identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE runtime logs, traces, metrics, alarms, quality, capacity, and drift evidence

MYTHOS-HW-0002-C06**Firmware Source, Signing, and Update Authority**

The organization **MUST** define, implement, verify, and maintain firmware source, signing, and update authority for in-scope trusted compute, DPU, and firmware capabilities. The control boundary **MUST** identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE failure, failover, rollback, restoration, revocation, and recovery exercise

MYTHOS-HW-0002-C07**DPU, SmartNIC, and Infrastructure Processing Boundary**

The organization **MUST** define, implement, verify, and maintain dpu, smartnic, and infrastructure processing boundary for in-scope trusted compute, DPU, and firmware capabilities. The control boundary **MUST** identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE safety, privacy, residency, consent, or physical-impact assessment

MYTHOS-HW-0002-C08**IOMMU, DMA, PCIe, and Device Assignment Isolation**

The organization **MUST** define, implement, verify, and maintain iommu, dma, pcie, and device assignment isolation for in-scope trusted compute, DPU, and firmware capabilities. The control boundary **MUST** identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE supplier, carrier, firmware, license, support, portability, and exit evidence

MYTHOS-HW-0002 / HARDWARE AND COMPUTE

5. Normative Control System

Atomic criteria 09-12 of 18

MYTHOS-HW-0002-C09**Confidential Computing and Key-Release Policy**

The organization **MUST** define, implement, verify, and maintain confidential computing and key-release policy for in-scope trusted compute, DPU, and firmware capabilities. The control boundary **MUST** identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE approved service contract; architecture decision; owner and risk sign-off

MYTHOS-HW-0002-C10**Supply-Chain Provenance and Counterfeit Detection**

The organization **MUST** define, implement, verify, and maintain supply-chain provenance and counterfeit detection for in-scope trusted compute, DPU, and firmware capabilities. The control boundary **MUST** identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE asset, service, dependency, supplier, region, and lifecycle inventory

MYTHOS-HW-0002-C11**Debug, Recovery, Manufacturing, and Service Modes**

The organization **MUST** define, implement, verify, and maintain debug, recovery, manufacturing, and service modes for in-scope trusted compute, DPU, and firmware capabilities. The control boundary **MUST** identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE desired-state configuration; policy evidence; privileged-access and negative tests

MYTHOS-HW-0002-C12**Secrets, Certificates, and Hardware-Bound Keys**

The organization **MUST** define, implement, verify, and maintain secrets, certificates, and hardware-bound keys for in-scope trusted compute, DPU, and firmware capabilities. The control boundary **MUST** identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE network, data-flow, zone, conduit, radio, device, or trust-boundary diagrams

MYTHOS-HW-0002 / HARDWARE AND COMPUTE

5. Normative Control System

Atomic criteria 13-15 of 18

MYTHOS-HW-0002-C13**Vulnerability, Revocation, and Emergency Update**

The organization **MUST** define, implement, verify, and maintain vulnerability, revocation, and emergency update for in-scope trusted compute, DPU, and firmware capabilities. The control boundary **MUST** identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE runtime logs, traces, metrics, alarms, quality, capacity, and drift evidence

MYTHOS-HW-0002-C14**Attestation Replay, Freshness, and Evidence Integrity**

The organization **MUST** define, implement, verify, and maintain attestation replay, freshness, and evidence integrity for in-scope trusted compute, DPU, and firmware capabilities. The control boundary **MUST** identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE failure, failover, rollback, restoration, revocation, and recovery exercise

MYTHOS-HW-0002-C15**Tenant Placement and Trusted-Scheduling Decisions**

The organization **MUST** define, implement, verify, and maintain tenant placement and trusted-scheduling decisions for in-scope trusted compute, DPU, and firmware capabilities. The control boundary **MUST** identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE safety, privacy, residency, consent, or physical-impact assessment

MYTHOS-HW-0002 / HARDWARE AND COMPUTE

5. Normative Control System

Atomic criteria 16-18 of 18

MYTHOS-HW-0002-C16**Repair, Replacement, RMA, and Ownership Transfer**

The organization MUST define, implement, verify, and maintain repair, replacement, rma, and ownership transfer for in-scope trusted compute, DPU, and firmware capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE supplier, carrier, firmware, license, support, portability, and exit evidence

MYTHOS-HW-0002-C17**Sanitization, Decommissioning, and Key Destruction**

The organization MUST define, implement, verify, and maintain sanitization, decommissioning, and key destruction for in-scope trusted compute, DPU, and firmware capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE approved service contract; architecture decision; owner and risk sign-off

MYTHOS-HW-0002-C18**Trust Evidence and Periodic Reference-Value Review**

The organization MUST define, implement, verify, and maintain trust evidence and periodic reference-value review for in-scope trusted compute, DPU, and firmware capabilities. The control boundary MUST identify accountable ownership, affected services and assets, authoritative desired state, trust transitions, failure and recovery behavior, minimum evidence, inherited responsibility, and reassessment triggers.

MINIMUM EVIDENCE asset, service, dependency, supplier, region, and lifecycle inventory

6. Evidence and Assessment

Examine, interview, test, observe, restore, and trace

EXAMINE

Policies, inventories, diagrams, configuration, code, firmware, contracts, provider evidence, logs, exceptions, and lifecycle records.

INTERVIEW

Accountable owners, architects, engineers, operators, safety personnel, security teams, vendors, carriers, integrators, and responders.

TEST

Identity, segmentation, policy, negative paths, malformed input, capacity stress, dependency loss, failover, rollback, and revocation.

RESTORE

Independent restoration of configuration, data, service, device, controller, cluster, media, or browser state from protected evidence.

OBSERVE

Production-like performance, quality, drift, resource use, physical behavior, alarms, user impact, and incident execution.

TRACE

End-to-end linkage from approved intent and identity through change, runtime behavior, telemetry, outcome, exception, and review.

Evidence grades

A

Independently reproducible, complete, current, integrity-protected, and representative.

B

Reproduced by the implementing organization with strong traceability and controlled scope.

C

Partially reproduced or indirect; limitations, inherited responsibility, and uncertainty recorded.

D

Assertion, diagram, design intent, certificate, or vendor statement without reproduced behavior.

MYTHOS-HW-0002 / HARDWARE AND COMPUTE

7. Assurance Views

Six perspectives required for a complete assurance claim

GOVERNANCE

Ownership, purpose, risk tolerance, policy, exception, and decision rights.

ARCHITECTURE

Boundaries, dependencies, failure modes, state, data flow, and portability.

SECURITY

Identity, authorization, isolation, secrets, abuse resistance, and incident response.

OPERATIONS

Reliability, performance, cost, observability, change, recovery, and support.

PRIVACY / RIGHTS

Purpose limitation, minimization, consent, access, correction, deletion, and egress.

HUMAN / SOCIETAL

Usability, accessibility, disclosure, contestability, impact, and human control.

Conformance requires a defensible position across every applicable view. A strong aggregate score cannot compensate for an unowned system, a failed mandatory gate, untested recovery, or evidence below the accepted grade.

MYTHOS-HW-0002 / HARDWARE AND COMPUTE

7.2 Evaluation Metrics and Decision Gates

Measures must expose service behavior, control effectiveness, failure, uncertainty, and cost

SERVICE

Availability, correctness, coverage, quality, latency, throughput, and user or process outcome.

CONTROL

Unauthorized attempt, policy denial, drift, segmentation escape, privilege, and exception exposure.

RESILIENCE

Failover success, recovery time, data loss, safe degradation, restore validity, and dependency survival.

SECURITY

Exploitability, credential exposure, supply-chain integrity, attack detection, containment, and revocation.

CAPACITY

Utilization, saturation, queueing, radio or fabric headroom, thermal margin, quota, and forecast error.

OPERATIONS

Change failure, mean time to detect, repair, support burden, vendor escalation, and evidence completeness.

PRIVACY / SAFETY

Unauthorized egress, retention breach, consent coverage, unsafe action, physical consequence, and contestability.

LIFECYCLE

Patch debt, end-of-support exposure, portability, replacement time, retirement completion, and reassessment age.

Decision gate: thresholds **MUST** be declared before assessment, cover representative load and failure conditions, and identify mandatory safety, identity, recovery, and evidence failures that block promotion.

MYTHOS-HW-0002 / HARDWARE AND COMPUTE

8. Failure Modes and Adversarial Scenarios

Challenge assumptions before the system is trusted with consequential work

BMC COMPROMISE

Out-of-band management provides persistent control beneath the operating system.

REQUIRED: PREVENT | DETECT | CONTAIN | RECOVER | EVIDENCE

FIRMWARE SUPPLY-CHAIN ATTACK

Signed or trusted firmware is malicious, vulnerable, or incorrectly sourced.

REQUIRED: PREVENT | DETECT | CONTAIN | RECOVER | EVIDENCE

DMA BOUNDARY BYPASS

A device accesses memory outside its assigned trust domain.

REQUIRED: PREVENT | DETECT | CONTAIN | RECOVER | EVIDENCE

ATTESTATION REPLAY

Stale or forged evidence causes keys or workloads to be released to an untrusted platform.

REQUIRED: PREVENT | DETECT | CONTAIN | RECOVER | EVIDENCE

POWER OR THERMAL COLLAPSE

Facility or rack constraints create correlated hardware failure.

REQUIRED: PREVENT | DETECT | CONTAIN | RECOVER | EVIDENCE

CROSS-TENANT LEAKAGE

Scheduler, cache, fabric, storage, or diagnostics expose another workload.

REQUIRED: PREVENT | DETECT | CONTAIN | RECOVER | EVIDENCE

Adversarial testing MUST protect people and production systems. Use isolated environments, synthetic or minimized data, bounded authority, kill switches, explicit legal and ethical review, and documented stop conditions.

9. Implementation Profiles

Risk-proportional implementation without weakening mandatory boundaries

FOUNDATIONAL	ADVANCED	HIGH ASSURANCE
TYPICAL SCOPE Low consequence, limited autonomy, non-sensitive data, reversible outputs.	TYPICAL SCOPE Business-critical workflow, sensitive data, multiple tools or providers, moderate autonomy.	TYPICAL SCOPE Safety, security, regulated, financial, identity, or broadly consequential use.
MINIMUM DEPTH Named owner; inventory; basic evaluation; access control; logging; rollback; annual review.	MINIMUM DEPTH Formal threat model; representative evaluation; approval gates; isolated execution; tested recovery; quarterly review.	MINIMUM DEPTH Independent challenge; strongest identity; deterministic enforcement; comprehensive evidence; canary release; continuous monitoring.

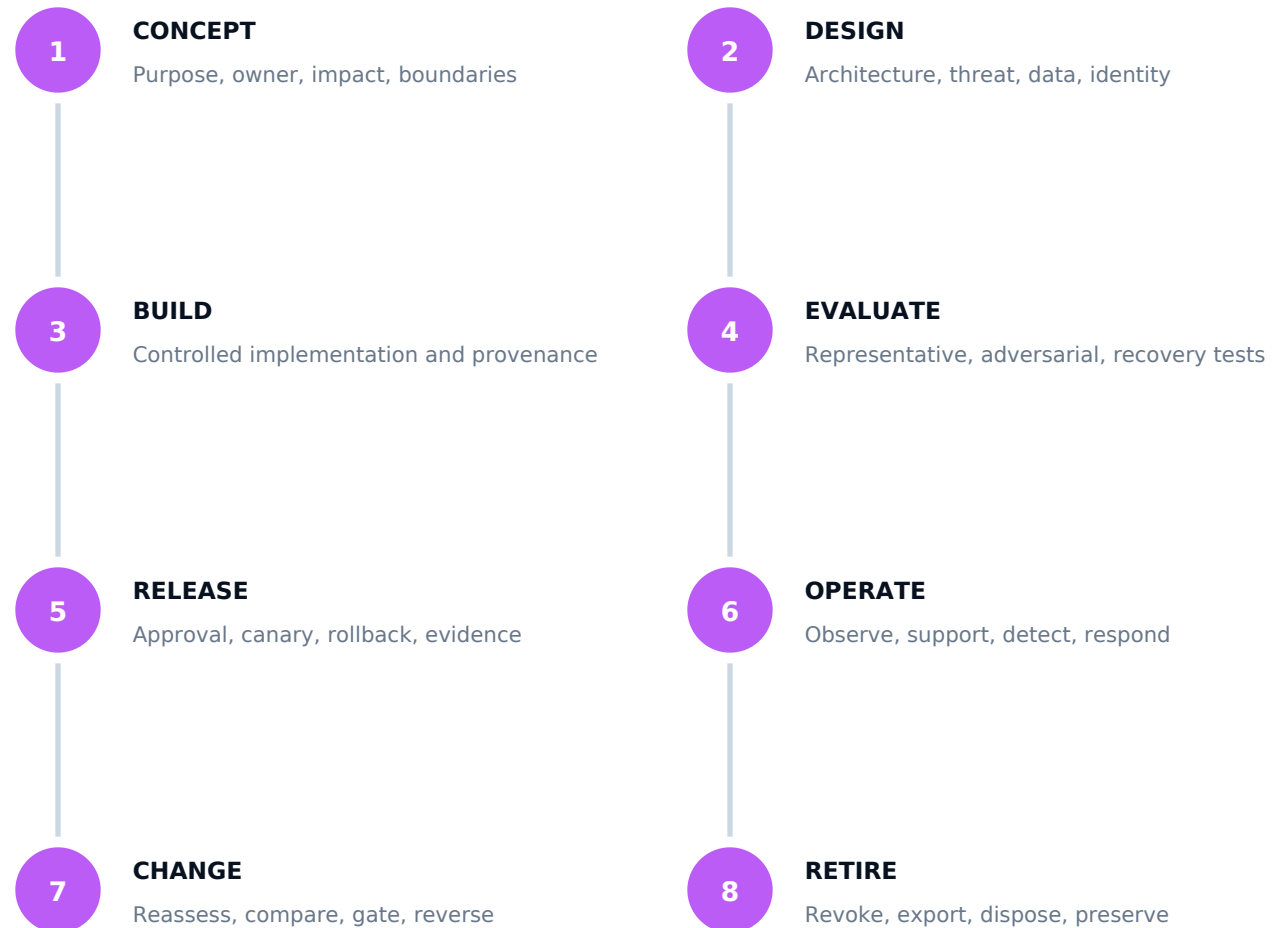
Profile selection rule

Choose the highest profile triggered by consequence, autonomy, sensitivity, scale, irreversibility, external dependency, or inability to rapidly detect and recover. Tailoring may strengthen controls; it may not erase a mandatory gate without a controlled exception.

MYTHOS-HW-0002 / HARDWARE AND COMPUTE

9.2 Operational Lifecycle

Evidence-bearing operation from concept through retirement



LIFECYCLE INVARIANT

Every stage **MUST** leave sufficient evidence for the next authority to understand what was intended, what changed, what was tested, what failed, what was accepted, what remains uncertain, and how to recover or exit.

MYTHOS-HW-0002 / HARDWARE AND COMPUTE

10. Adoption Roadmap

A sequenced path from uncontrolled capability to evidence-bearing operation

0-30 DAYS**Establish ownership and truth**

Inventory systems and dependencies; classify risk; freeze unsupported claims; identify immediate privilege, data, and evidence gaps.

31-90 DAYS**Create enforceable boundaries**

Define policy; isolate execution; implement identity and approval gates; establish representative evaluation and baseline telemetry.

3-6 MONTHS**Prove recovery and operating control**

Exercise failure, rollback, revocation, incident, provider exit, and state-recovery scenarios; mature evidence packaging.

6-12 MONTHS**Scale assurance**

Automate control checks; expand workload coverage; independent challenge; portfolio metrics; controlled exception expiry; continuous reassessment.

Adoption is complete only when operating evidence demonstrates the selected profile in the actual deployment context. Documentation alone is not conformance.

MYTHOS-HW-0002 / HARDWARE AND COMPUTE

10.2 Conformance and Exception Statement

What an assurance claim must contain

SYSTEM / SERVICE Named, versioned capability and deployment boundary.	PROFILE Foundational, Advanced, or High Assurance with trigger rationale.
SCOPE Workloads, users, data, tools, regions, providers, and exclusions.	CRITERIA Pass, partial, fail, not applicable, and exception status for every criterion.
EVIDENCE Artifact references, evidence grade, date, environment, and reproducibility.	LIMITATIONS Known failure modes, unsupported workloads, uncertainty, and residual risk.
EXCEPTIONS Owner, rationale, compensating control, expiration, and approval.	VALIDITY Assessment date, change boundary, review date, and reassessment triggers.

Prohibited claim: “compliant” without the named scope, profile, evidence date, limitations, exceptions, and authority accepting residual risk.

MYTHOS-HW-0002 / HARDWARE AND COMPUTE

11. Source Authority and Reference Register

Primary sources informing interpretation; current obligations and provider behavior must be verified at assessment time

NIST CSF 2.0 **Cybersecurity Framework 2.0**

<https://doi.org/10.6028/NIST.CSWP.29>
Enterprise governance and cybersecurity outcome framework.

NIST SP 800-53 Rev. 5 **Security and Privacy Controls for Information Systems and Organizations**

<https://doi.org/10.6028/NIST.SP.800-53r5>
Broad control baseline for organizational systems and services.

NIST SP 800-193 **Platform Firmware Resiliency Guidelines**

<https://doi.org/10.6028/NIST.SP.800-193>
Platform firmware protection, detection, and recovery.

TCG TPM 2.0 **Trusted Platform Module Library Specification**

<https://trustedcomputinggroup.org/resource/tpm-library-specification/>
TPM commands, objects, measurement, keys, and attestation foundations.

DMTF Redfish **Redfish Standard**

<https://www.dmtf.org/standards/redfish>
Secure and interoperable hardware-management interfaces.

NIST SP 800-155 **BIOS Integrity Measurement Guidelines**

<https://doi.org/10.6028/NIST.SP.800-155>
Firmware measurement and integrity-verification principles.

Source currency rule: authorities, specifications, legal obligations, provider services, firmware, browser behavior, carrier requirements, and operational evidence MUST be checked at assessment time. This publication records a 2026-07-24 source snapshot.

11.2 Revision History and Decision Register

Permanent identity, controlled change, and publication integrity

VERSION	DATE	STATE	SUMMARY
1.0.0-candidate	2026-07-24	Candidate	Permanent-publication edition; source refresh; expanded criteria, evidence, assurance, and lifecycle guidance.
Next review	2027-01-24	Scheduled	Review source currency, threat evolution, operating evidence, adoption feedback, and proposed revisions.

Publication decisions

- PERMANENT IDENTITY

The document ID remains stable across revisions; batch or production sequence metadata is not public identity.
- CHANGE CONTROL

Normative changes require rationale, impact analysis, affected-criterion mapping, and approval.
- SUPERSESSION

A superseded edition remains traceable; current routes and catalogs identify the active edition.
- CORRECTION

Material errors require a recorded correction, affected-evidence analysis, and notification appropriate to impact.
- ARCHIVAL INTEGRITY

Published artifacts receive hashes, metadata, and a release manifest sufficient for independent verification.

END OF PERMANENT PUBLICATION / MYTHOS-HW-0002
MYTHOS SYSTEMS / ENGINEERING STANDARDS LIBRARY