ENGINEERING STANDARDS LIBRARY / TELECOMMUNICATIONS AND RADIO SYSTEMS

Telecommunications and Radio Systems Standards Portfolio

Permanent standards portfolio for telecommunications and radio systems.

PERMANENT DOCUMENT ID

MYTHOS-TEL-PORT-0001

PUBLICATION

Portfolio Edition
Version 1.0.0-candidate

ASSURANCE PROFILE

Standard / Advanced
High Assurance

PERMANENT PUBLICATION IDENTITY

Telecommunications and Radio Systems Standards Portfolio

DOCUMENT ID
MYTHOS-TEL-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	6	4	1
ATOMIC CRITERIA	ASSURANCE VIEWS	IMPLEMENTATION PROFILES	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

Telecommunications and Radio Systems

A trustworthy telecommunications and radio systems 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

Reconciliation, detection, response, restoration, and controlled evolution

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-TEL-PORT-0001 / TELECOMMUNICATIONS

Portfolio Position

Permanent standards portfolio for telecommunications and radio systems.

OPERATING POSITION

This portfolio consolidates 3 permanent standards for telecommunications and radio systems.

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

MYTHOS-TEL-PORT-0001 / TELECOMMUNICATIONS

Portfolio Register

OPERATING POSITION

MYTHOS-TEL-0001 - 5G, 6G, Core Network, Open RAN, and Slicing Standard

- MYTHOS-TEL-0002 - Distributed Antenna Systems and Indoor RF Standard
- MYTHOS-TEL-0003 - Enterprise Telephony, VoIP, and Call-Control Standard

MYTHOS-TEL-PORT-0001 / TELECOMMUNICATIONS

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-TEL-PORT-0001 / TELECOMMUNICATIONS

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-TEL-PORT-0001 / TELECOMMUNICATIONS

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.

MYTHOS-TEL-PORT-0001 / TELECOMMUNICATIONS

11. Source Authority and Reference Register

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

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.

3GPP Specifications	**3GPP technical specifications and reports**

https://www.3gpp.org/specifications-technologies/specifications-by-series

Mobile-system architecture, security, radio, core, and service specifications.

O-RAN Alliance	**O-RAN specifications and security work**

https://www.o-ran.org/specifications

Open RAN architecture, interfaces, management, and security.

GSMA NESAS	**Network Equipment Security Assurance Scheme**

https://www.gsma.com/solutions-and-impact/technologies/security/network-equipment-security-assurance-scheme/

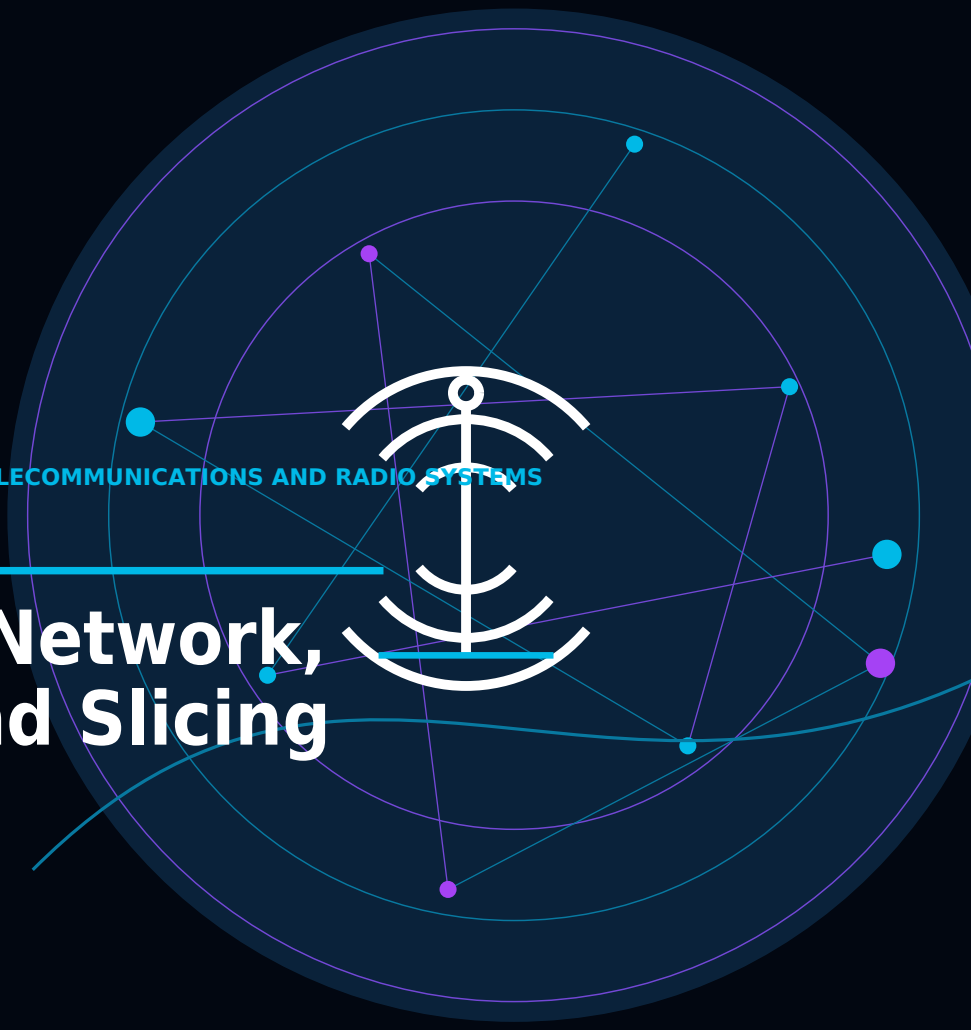
Telecom equipment security development and assessment scheme.

IETF SIP	**Session Initiation Protocol - RFC 3261**

https://www.rfc-editor.org/rfc/rfc3261

Core SIP signaling model and protocol semantics.

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 / TELECOMMUNICATIONS AND RADIO SYSTEMS

5G, 6G, Core Network, Open RAN, and Slicing Standard

Mobile-core and RAN architecture, identity, slicing, timing, MEC, cloud-native functions, assurance, and lifecycle governance.

PERMANENT DOCUMENT ID

MYTHOS-TEL-0001

PUBLICATION

Candidate Standard
Version 1.0.0-candidate

ASSURANCE PROFILE

Standard / Advanced
High Assurance

PERMANENT PUBLICATION IDENTITY

5G, 6G, Core Network, Open RAN, and Slicing Standard

DOCUMENT ID
MYTHOS-TEL-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	6	4	1
ATOMIC CRITERIA	ASSURANCE VIEWS	IMPLEMENTATION PROFILES	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

Telecommunications and Radio Systems

A trustworthy 5G, 6G, Open RAN, and network slicing 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

Reconciliation, detection, response, restoration, and controlled evolution

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.

INTERACTIVE NAVIGATION

Contents

Navigation doctrine

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

MYTHOS-TEL-0001 / TELECOMMUNICATIONS

0. Executive Mandate

Purpose, strategic outcome, and non-negotiable operating doctrine

MANDATE

Organizations adopting 5G, 6G, Open RAN, and network slicing 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 5G, 6G, Open RAN, and network slicing 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-TEL-0001 / TELECOMMUNICATIONS

1. Scope and Applicability

Boundary definition, audience, exclusions, and triggering conditions

IN SCOPE

- Architecture, acquisition, configuration, integration, and operation of 5G, 6G, Open RAN, and network slicing 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-TEL-0001 / TELECOMMUNICATIONS

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.

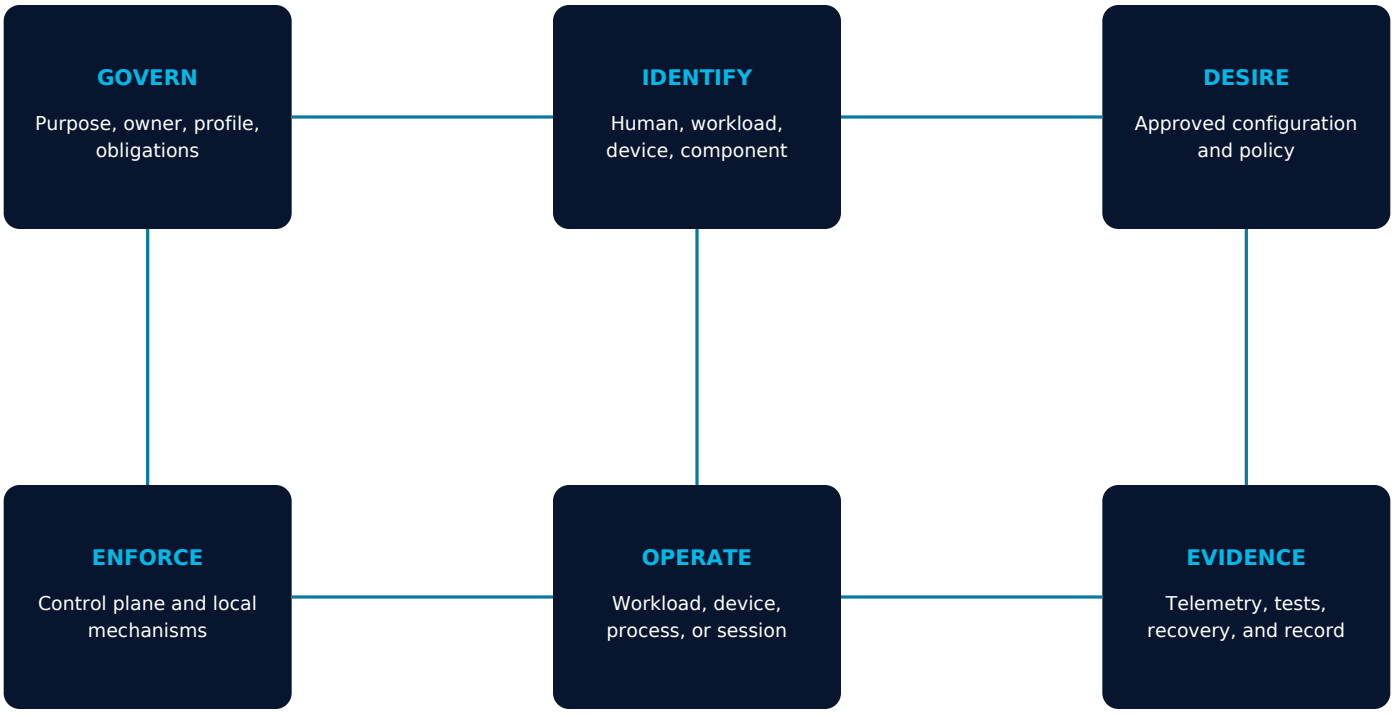
REASSESSMENT TRIGGER

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

MYTHOS-TEL-0001 / TELECOMMUNICATIONS

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-TEL-0001 / TELECOMMUNICATIONS

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-TEL-0001 / TELECOMMUNICATIONS

5. Normative Control System

Atomic criteria 01-04 of 18

MYTHOS-TEL-0001-C01 Release Profile, Service Scope, and Regulatory Boundary

The organization MUST define, implement, verify, and maintain release profile, service scope, and regulatory boundary for in-scope 5G, 6G, Open RAN, and network slicing 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-TEL-0001-C02 Subscriber, SIM, eSIM, and Network Identity

The organization MUST define, implement, verify, and maintain subscriber, sim, esim, and network identity for in-scope 5G, 6G, Open RAN, and network slicing 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-TEL-0001-C03 RAN, Transport, Core, and Edge Trust Domains

The organization MUST define, implement, verify, and maintain ran, transport, core, and edge trust domains for in-scope 5G, 6G, Open RAN, and network slicing 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-TEL-0001-C04 Service-Based Interface and API Protection

The organization MUST define, implement, verify, and maintain service-based interface and api protection for in-scope 5G, 6G, Open RAN, and network slicing 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-TEL-0001 / TELECOMMUNICATIONS

5. Normative Control System

Atomic criteria 05-08 of 18

MYTHOS-TEL-0001-C05 Control-Plane and User-Plane Separation

The organization MUST define, implement, verify, and maintain control-plane and user-plane separation for in-scope 5G, 6G, Open RAN, and network slicing 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-TEL-0001-C06 Slice Definition, Admission, and Isolation Evidence

The organization MUST define, implement, verify, and maintain slice definition, admission, and isolation evidence for in-scope 5G, 6G, Open RAN, and network slicing 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-TEL-0001-C07 QoS, Policy, Charging, and Resource Enforcement

The organization MUST define, implement, verify, and maintain qos, policy, charging, and resource enforcement for in-scope 5G, 6G, Open RAN, and network slicing 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-TEL-0001-C08 Open RAN SMO, RIC, xApp, and rApp Governance

The organization MUST define, implement, verify, and maintain open ran smo, ric, xapp, and rapp governance for in-scope 5G, 6G, Open RAN, and network slicing 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-TEL-0001 / TELECOMMUNICATIONS

5. Normative Control System

Atomic criteria 09-12 of 18

MYTHOS-TEL-0001-C09 Virtualized and Cloud-Native Network Function Security

The organization MUST define, implement, verify, and maintain virtualized and cloud-native network function security for in-scope 5G, 6G, Open RAN, and network slicing 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-TEL-0001-C10 MEC Workload, Data, and Local-Breakout Control

The organization MUST define, implement, verify, and maintain mec workload, data, and local-breakout control for in-scope 5G, 6G, Open RAN, and network slicing 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-TEL-0001-C11 Timing, Synchronization, and Positioning Resilience

The organization MUST define, implement, verify, and maintain timing, synchronization, and positioning resilience for in-scope 5G, 6G, Open RAN, and network slicing 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-TEL-0001-C12 Roaming, Interconnect, and Partner Trust

The organization MUST define, implement, verify, and maintain roaming, interconnect, and partner trust for in-scope 5G, 6G, Open RAN, and network slicing 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-TEL-0001 / TELECOMMUNICATIONS

5. Normative Control System

Atomic criteria 13-15 of 18

MYTHOS-TEL-0001-C13 Lawful, Emergency, and Priority-Service Obligations

The organization MUST define, implement, verify, and maintain lawful, emergency, and priority-service obligations for in-scope 5G, 6G, Open RAN, and network slicing 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-TEL-0001-C14 Signaling, Fraud, and Abuse Detection

The organization MUST define, implement, verify, and maintain signaling, fraud, and abuse detection for in-scope 5G, 6G, Open RAN, and network slicing 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-TEL-0001-C15 Capacity, Mobility, and Service Quality Assurance

The organization MUST define, implement, verify, and maintain capacity, mobility, and service quality assurance for in-scope 5G, 6G, Open RAN, and network slicing 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-TEL-0001 / TELECOMMUNICATIONS

5. Normative Control System

Atomic criteria 16-18 of 18

MYTHOS-TEL-0001-C16 Software, Model, and Supply-Chain Governance

The organization MUST define, implement, verify, and maintain software, model, and supply-chain governance for in-scope 5G, 6G, Open RAN, and network slicing 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-TEL-0001-C17 Outage, Disaster, and Regional Recovery

The organization MUST define, implement, verify, and maintain outage, disaster, and regional recovery for in-scope 5G, 6G, Open RAN, and network slicing 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-TEL-0001-C18 Lifecycle Evidence and Technology Reassessment

The organization MUST define, implement, verify, and maintain lifecycle evidence and technology reassessment for in-scope 5G, 6G, Open RAN, and network slicing 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-TEL-0001 / TELECOMMUNICATIONS

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-TEL-0001 / TELECOMMUNICATIONS

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-TEL-0001 / TELECOMMUNICATIONS

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-TEL-0001 / TELECOMMUNICATIONS

8. Failure Modes and Adversarial Scenarios

Challenge assumptions before the system is trusted with consequential work

SUBSCRIBER IDENTITY COMPROMISE

SIM, eSIM, credential, or provisioning weakness enables impersonation.

REQUIRED: PREVENT | DETECT | CONTAIN | RECOVER | EVIDENCE

SLICE ISOLATION FAILURE

A label implies isolation not enforced across radio, transport, core, edge, and cloud.

REQUIRED: PREVENT | DETECT | CONTAIN | RECOVER | EVIDENCE

SIGNALING ABUSE

Protocol manipulation causes fraud, denial, interception, or unauthorized routing.

REQUIRED: PREVENT | DETECT | CONTAIN | RECOVER | EVIDENCE

TIMING LOSS

Synchronization failure degrades radio, handoff, positioning, or service quality.

REQUIRED: PREVENT | DETECT | CONTAIN | RECOVER | EVIDENCE

RF INTERFERENCE

Coverage, PIM, noise, or external interference defeats expected service.

REQUIRED: PREVENT | DETECT | CONTAIN | RECOVER | EVIDENCE

EMERGENCY-SERVICE FAILURE

Calling, location, priority, public-safety, or survivability obligations are not met.

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.

MYTHOS-TEL-0001 / TELECOMMUNICATIONS

9. Implementation Profiles

Risk-proportional implementation without weakening mandatory boundaries

FOUNDATIONAL

TYPICAL SCOPE

Low consequence, limited autonomy, non-sensitive data, reversible outputs.

MINIMUM DEPTH

Named owner; inventory; basic evaluation; access control; logging; rollback; annual review.

ADVANCED

TYPICAL SCOPE

Business-critical workflow, sensitive data, multiple tools or providers, moderate autonomy.

MINIMUM DEPTH

Formal threat model; representative evaluation; approval gates; isolated execution; tested recovery; quarterly review.

HIGH ASSURANCE

TYPICAL SCOPE

Safety, security, regulated, financial, identity, or broadly consequential use.

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-TEL-0001 / TELECOMMUNICATIONS

9.2 Operational Lifecycle

Evidence-bearing operation from concept through retirement

1 **CONCEPT**
Purpose, owner, impact, boundaries

2 **DESIGN**
Architecture, threat, data, identity

3 **BUILD**
Controlled implementation and provenance

4 **EVALUATE**
Representative, adversarial, recovery tests

5 **RELEASE**
Approval, canary, rollback, evidence

6 **OPERATE**
Observe, support, detect, respond

7 **CHANGE**
Reassess, compare, gate, reverse

8 **RETIRE**
Revoke, export, dispose, preserve

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-TEL-0001 / TELECOMMUNICATIONS

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-TEL-0001 / TELECOMMUNICATIONS

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-TEL-0001 / TELECOMMUNICATIONS

11. Source Authority and Reference Register

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

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.

3GPP Specifications — **3GPP technical specifications and reports**

https://www.3gpp.org/specifications-technologies/specifications-by-series

Mobile-system architecture, security, radio, core, and service specifications.

O-RAN Alliance — **O-RAN specifications and security work**

https://www.o-ran.org/specifications

Open RAN architecture, interfaces, management, and security.

GSMA NESAS — **Network Equipment Security Assurance Scheme**

https://www.gsma.com/solutions-and-impact/technologies/security/network-equipment-security-assurance-scheme/

Telecom equipment security development and assessment scheme.

IETF SIP — **Session Initiation Protocol - RFC 3261**

https://www.rfc-editor.org/rfc/rfc3261

Core SIP signaling model and protocol semantics.

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-TEL-0001 / TELECOMMUNICATIONS

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-TEL-0001

MYTHOS SYSTEMS / ENGINEERING STANDARDS LIBRARY

ENGINEERING STANDARDS LIBRARY / TELECOMMUNICATIONS AND RADIO SYSTEMS

Distributed Antenna Systems and Indoor RF Standard

Indoor RF, DAS, neutral-host, public-safety coverage, interference, power, survivability, acceptance, and operational evidence.

PERMANENT DOCUMENT ID

MYTHOS-TEL-0002

PUBLICATION

Candidate Standard
Version 1.0.0-candidate

ASSURANCE PROFILE

Standard / Advanced
High Assurance

PERMANENT PUBLICATION IDENTITY

Distributed Antenna Systems and Indoor RF Standard

DOCUMENT ID
MYTHOS-TEL-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	6	4	1
ATOMIC CRITERIA	ASSURANCE VIEWS	IMPLEMENTATION PROFILES	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

Telecommunications and Radio Systems

A trustworthy distributed antenna systems and indoor RF 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

Reconciliation, detection, response, restoration, and controlled evolution

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.

INTERACTIVE NAVIGATION

Contents

Navigation doctrine

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

MYTHOS-TEL-0002 / TELECOMMUNICATIONS

0. Executive Mandate

Purpose, strategic outcome, and non-negotiable operating doctrine

MANDATE

Organizations adopting distributed antenna systems and indoor RF 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 distributed antenna systems and indoor RF 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-TEL-0002 / TELECOMMUNICATIONS

1. Scope and Applicability

Boundary definition, audience, exclusions, and triggering conditions

IN SCOPE

- Architecture, acquisition, configuration, integration, and operation of distributed antenna systems and indoor RF 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-TEL-0002 / TELECOMMUNICATIONS

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.

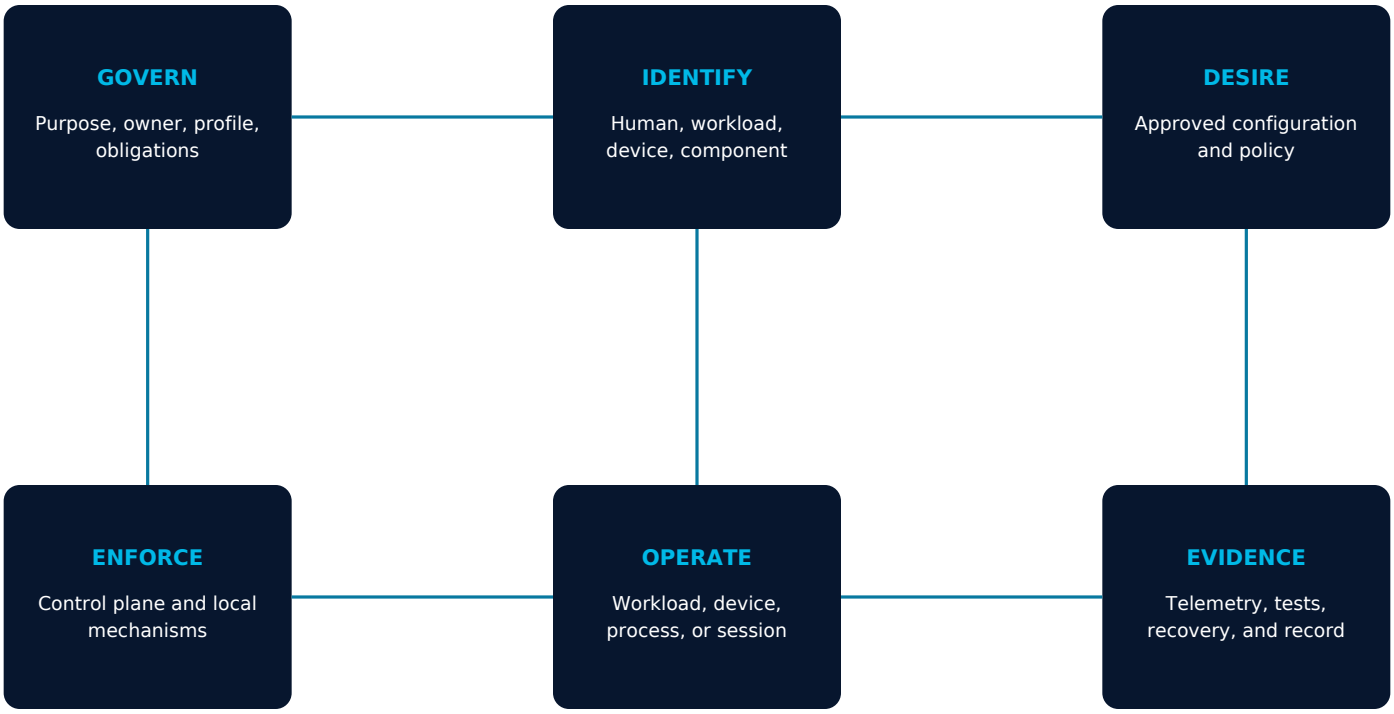
REASSESSMENT TRIGGER

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

MYTHOS-TEL-0002 / TELECOMMUNICATIONS

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-TEL-0002 / TELECOMMUNICATIONS

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-TEL-0002 / TELECOMMUNICATIONS

5. Normative Control System

Atomic criteria 01-04 of 18

MYTHOS-TEL-0002-C01 Coverage Purpose, Occupancy, and Authority Boundary

The organization MUST define, implement, verify, and maintain coverage purpose, occupancy, and authority boundary for in-scope distributed antenna systems and indoor RF 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-TEL-0002-C02 RF Survey, Prediction, and Design Assumptions

The organization MUST define, implement, verify, and maintain rf survey, prediction, and design assumptions for in-scope distributed antenna systems and indoor RF 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-TEL-0002-C03 Carrier, Band, Technology, and Capacity Plan

The organization MUST define, implement, verify, and maintain carrier, band, technology, and capacity plan for in-scope distributed antenna systems and indoor RF 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-TEL-0002-C04 Public-Safety Radio and AHJ Requirements

The organization MUST define, implement, verify, and maintain public-safety radio and ahj requirements for in-scope distributed antenna systems and indoor RF 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-TEL-0002 / TELECOMMUNICATIONS

5. Normative Control System

Atomic criteria 05-08 of 18

MYTHOS-TEL-0002-C05 Head-End, Source, Fiber, and Remote-Unit Architecture

The organization MUST define, implement, verify, and maintain head-end, source, fiber, and remote-unit architecture for in-scope distributed antenna systems and indoor RF 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-TEL-0002-C06 Neutral-Host and Multi-Operator Governance

The organization MUST define, implement, verify, and maintain neutral-host and multi-operator governance for in-scope distributed antenna systems and indoor RF 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-TEL-0002-C07 Link Budget, Noise, Interference, and PIM Control

The organization MUST define, implement, verify, and maintain link budget, noise, interference, and pim control for in-scope distributed antenna systems and indoor RF 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-TEL-0002-C08 Antenna Placement, Isolation, and Exposure Safety

The organization MUST define, implement, verify, and maintain antenna placement, isolation, and exposure safety for in-scope distributed antenna systems and indoor RF 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-TEL-0002 / TELECOMMUNICATIONS

5. Normative Control System

Atomic criteria 09-12 of 18

MYTHOS-TEL-0002-C09 Backhaul, Timing, Synchronization, and Monitoring

The organization MUST define, implement, verify, and maintain backhaul, timing, synchronization, and monitoring for in-scope distributed antenna systems and indoor RF 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-TEL-0002-C10 Power, Battery, Generator, and Survivability

The organization MUST define, implement, verify, and maintain power, battery, generator, and survivability for in-scope distributed antenna systems and indoor RF 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-TEL-0002-C11 Physical Security, Firestopping, and Pathway Integrity

The organization MUST define, implement, verify, and maintain physical security, firestopping, and pathway integrity for in-scope distributed antenna systems and indoor RF 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-TEL-0002-C12 Configuration, Firmware, and Change Control

The organization MUST define, implement, verify, and maintain configuration, firmware, and change control for in-scope distributed antenna systems and indoor RF 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-TEL-0002 / TELECOMMUNICATIONS

5. Normative Control System

Atomic criteria 13-15 of 18

MYTHOS-TEL-0002-C13 Acceptance Testing and Grid-Based Validation

The organization MUST define, implement, verify, and maintain acceptance testing and grid-based validation for in-scope distributed antenna systems and indoor RF 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-TEL-0002-C14 Voice, Data, Emergency, and Handoff Performance

The organization MUST define, implement, verify, and maintain voice, data, emergency, and handoff performance for in-scope distributed antenna systems and indoor RF 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-TEL-0002-C15 Fault Localization, Alarming, and Maintenance

The organization MUST define, implement, verify, and maintain fault localization, alarming, and maintenance for in-scope distributed antenna systems and indoor RF 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-TEL-0002 / TELECOMMUNICATIONS

5. Normative Control System

Atomic criteria 16-18 of 18

MYTHOS-TEL-0002-C16 Capacity Growth and Technology Refresh

The organization MUST define, implement, verify, and maintain capacity growth and technology refresh for in-scope distributed antenna systems and indoor RF 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-TEL-0002-C17 Incident, Outage, and Emergency Coordination

The organization MUST define, implement, verify, and maintain incident, outage, and emergency coordination for in-scope distributed antenna systems and indoor RF 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-TEL-0002-C18 As-Built Evidence and Periodic Recertification

The organization MUST define, implement, verify, and maintain as-built evidence and periodic recertification for in-scope distributed antenna systems and indoor RF 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-TEL-0002 / TELECOMMUNICATIONS

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-TEL-0002 / TELECOMMUNICATIONS

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-TEL-0002 / TELECOMMUNICATIONS

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-TEL-0002 / TELECOMMUNICATIONS

8. Failure Modes and Adversarial Scenarios

Challenge assumptions before the system is trusted with consequential work

SUBSCRIBER IDENTITY COMPROMISE

SIM, eSIM, credential, or provisioning weakness enables impersonation.

REQUIRED: PREVENT | DETECT | CONTAIN | RECOVER | EVIDENCE

SLICE ISOLATION FAILURE

A label implies isolation not enforced across radio, transport, core, edge, and cloud.

REQUIRED: PREVENT | DETECT | CONTAIN | RECOVER | EVIDENCE

SIGNALING ABUSE

Protocol manipulation causes fraud, denial, interception, or unauthorized routing.

REQUIRED: PREVENT | DETECT | CONTAIN | RECOVER | EVIDENCE

TIMING LOSS

Synchronization failure degrades radio, handoff, positioning, or service quality.

REQUIRED: PREVENT | DETECT | CONTAIN | RECOVER | EVIDENCE

RF INTERFERENCE

Coverage, PIM, noise, or external interference defeats expected service.

REQUIRED: PREVENT | DETECT | CONTAIN | RECOVER | EVIDENCE

EMERGENCY-SERVICE FAILURE

Calling, location, priority, public-safety, or survivability obligations are not met.

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.

MYTHOS-TEL-0002 / TELECOMMUNICATIONS

9. Implementation Profiles

Risk-proportional implementation without weakening mandatory boundaries

FOUNDATIONAL

TYPICAL SCOPE

Low consequence, limited autonomy, non-sensitive data, reversible outputs.

MINIMUM DEPTH

Named owner; inventory; basic evaluation; access control; logging; rollback; annual review.

ADVANCED

TYPICAL SCOPE

Business-critical workflow, sensitive data, multiple tools or providers, moderate autonomy.

MINIMUM DEPTH

Formal threat model; representative evaluation; approval gates; isolated execution; tested recovery; quarterly review.

HIGH ASSURANCE

TYPICAL SCOPE

Safety, security, regulated, financial, identity, or broadly consequential use.

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-TEL-0002 / TELECOMMUNICATIONS

9.2 Operational Lifecycle

Evidence-bearing operation from concept through retirement

1 **CONCEPT**
Purpose, owner, impact, boundaries

2 **DESIGN**
Architecture, threat, data, identity

3 **BUILD**
Controlled implementation and provenance

4 **EVALUATE**
Representative, adversarial, recovery tests

5 **RELEASE**
Approval, canary, rollback, evidence

6 **OPERATE**
Observe, support, detect, respond

7 **CHANGE**
Reassess, compare, gate, reverse

8 **RETIRE**
Revoke, export, dispose, preserve

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-TEL-0002 / TELECOMMUNICATIONS

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-TEL-0002 / TELECOMMUNICATIONS

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-TEL-0002 / TELECOMMUNICATIONS

11. Source Authority and Reference Register

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

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.

3GPP Specifications — **3GPP technical specifications and reports**

https://www.3gpp.org/specifications-technologies/specifications-by-series

Mobile-system architecture, security, radio, core, and service specifications.

O-RAN Alliance — **O-RAN specifications and security work**

https://www.o-ran.org/specifications

Open RAN architecture, interfaces, management, and security.

GSMA NESAS — **Network Equipment Security Assurance Scheme**

https://www.gsma.com/solutions-and-impact/technologies/security/network-equipment-security-assurance-scheme/

Telecom equipment security development and assessment scheme.

IETF SIP — **Session Initiation Protocol - RFC 3261**

https://www.rfc-editor.org/rfc/rfc3261

Core SIP signaling model and protocol semantics.

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-TEL-0002 / TELECOMMUNICATIONS

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-TEL-0002

MYTHOS SYSTEMS / ENGINEERING STANDARDS LIBRARY

MYTHOS SYSTEMS

ENGINEERING STANDARDS LIBRARY / TELECOMMUNICATIONS AND RADIO SYSTEMS

Enterprise Telephony, VoIP, and Call-Control Standard

SIP and call-control architecture, identity, SBCs, emergency calling, fraud, recording, quality, recovery, and evidence.

PERMANENT DOCUMENT ID

MYTHOS-TEL-0003

PUBLICATION

Candidate Standard
Version 1.0.0-candidate

ASSURANCE PROFILE

Standard / Advanced
High Assurance

PERMANENT PUBLICATION IDENTITY

Enterprise Telephony, VoIP, and Call-Control Standard

DOCUMENT ID
MYTHOS-TEL-0003

VERSION
1.0.0-candidate

STATUS
Candidate Standard

PUBLISHER
Mythos Systems

PUBLICATION DATE
2026-07-24

SCHEDULED REVIEW
2027-01-24

CLASSIFICATION
Public

18	6	4	1
ATOMIC CRITERIA	ASSURANCE VIEWS	IMPLEMENTATION PROFILES	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

Telecommunications and Radio Systems

A trustworthy enterprise telephony and call control 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

Reconciliation, detection, response, restoration, and controlled evolution

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.

INTERACTIVE NAVIGATION

Contents

Navigation doctrine

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

MYTHOS-TEL-0003 / TELECOMMUNICATIONS

0. Executive Mandate

Purpose, strategic outcome, and non-negotiable operating doctrine

MANDATE

Organizations adopting enterprise telephony and call control 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 enterprise telephony and call control 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-TEL-0003 / TELECOMMUNICATIONS

1. Scope and Applicability

Boundary definition, audience, exclusions, and triggering conditions

IN SCOPE

- Architecture, acquisition, configuration, integration, and operation of enterprise telephony and call control 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-TEL-0003 / TELECOMMUNICATIONS

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.

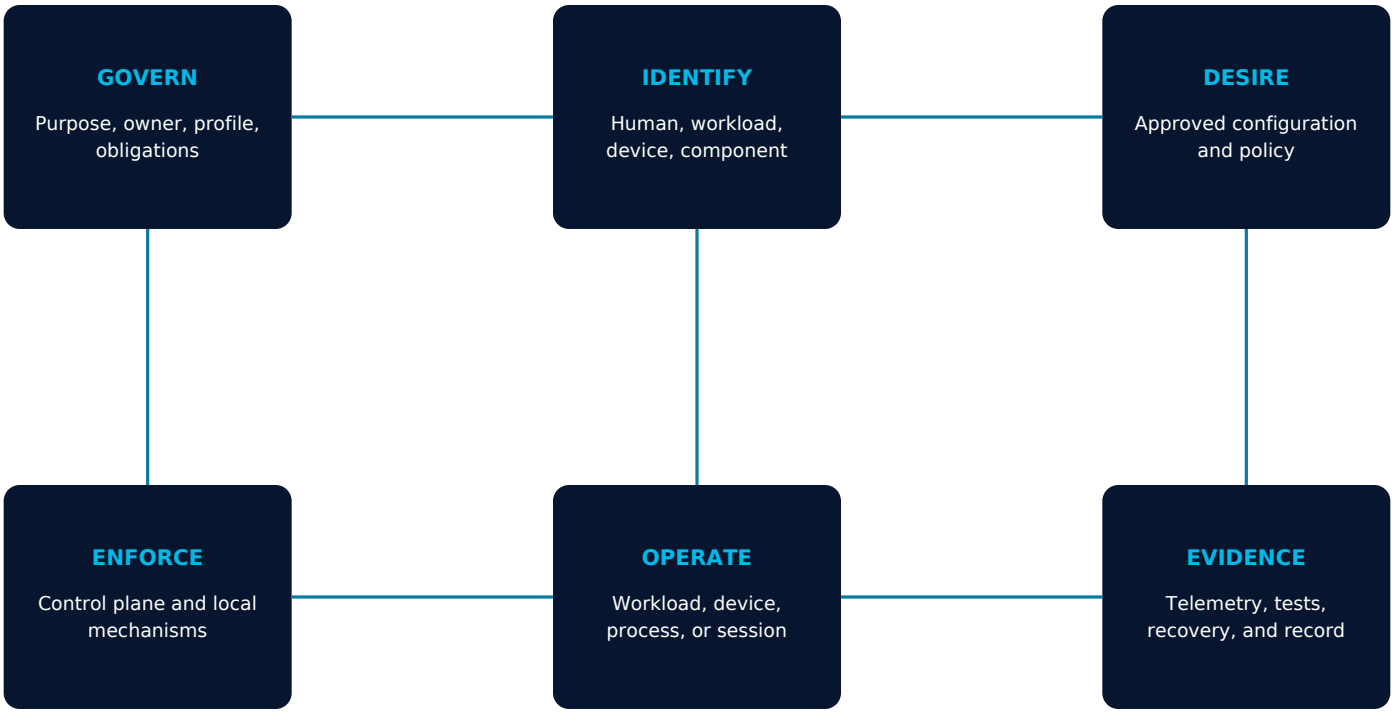
REASSESSMENT TRIGGER

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

MYTHOS-TEL-0003 / TELECOMMUNICATIONS

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-TEL-0003 / TELECOMMUNICATIONS

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-TEL-0003 / TELECOMMUNICATIONS

5. Normative Control System

Atomic criteria 01-04 of 18

MYTHOS-TEL-0003-C01 Telephony Service Boundary and Numbering Plan

The organization MUST define, implement, verify, and maintain telephony service boundary and numbering plan for in-scope enterprise telephony and call control 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-TEL-0003-C02 User, Device, Trunk, and Application Identity

The organization MUST define, implement, verify, and maintain user, device, trunk, and application identity for in-scope enterprise telephony and call control 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-TEL-0003-C03 Call-Control Cluster and Administrative Access

The organization MUST define, implement, verify, and maintain call-control cluster and administrative access for in-scope enterprise telephony and call control 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-TEL-0003-C04 SIP Trunk, SBC, and Carrier Interconnection

The organization MUST define, implement, verify, and maintain sip trunk, sbc, and carrier interconnection for in-scope enterprise telephony and call control 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-TEL-0003 / TELECOMMUNICATIONS

5. Normative Control System

Atomic criteria 05-08 of 18

MYTHOS-TEL-0003-C05 Signaling Authentication, Encryption, and Policy

The organization MUST define, implement, verify, and maintain signaling authentication, encryption, and policy for in-scope enterprise telephony and call control 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-TEL-0003-C06 Media Security, NAT Traversal, and Relay

The organization MUST define, implement, verify, and maintain media security, nat traversal, and relay for in-scope enterprise telephony and call control 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-TEL-0003-C07 Dial Plan, Route Pattern, and Toll Restriction

The organization MUST define, implement, verify, and maintain dial plan, route pattern, and toll restriction for in-scope enterprise telephony and call control 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-TEL-0003-C08 Emergency Calling, Location, and Notification

The organization MUST define, implement, verify, and maintain emergency calling, location, and notification for in-scope enterprise telephony and call control 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-TEL-0003 / TELECOMMUNICATIONS

5. Normative Control System

Atomic criteria 09-12 of 18

MYTHOS-TEL-0003-C09 Fraud, Robocall, and Abuse Prevention

The organization MUST define, implement, verify, and maintain fraud, robocall, and abuse prevention for in-scope enterprise telephony and call control 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-TEL-0003-C10 Voice Endpoint and Softphone Governance

The organization MUST define, implement, verify, and maintain voice endpoint and softphone governance for in-scope enterprise telephony and call control 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-TEL-0003-C11 Voicemail, Recording, Consent, and Retention

The organization MUST define, implement, verify, and maintain voicemail, recording, consent, and retention for in-scope enterprise telephony and call control 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-TEL-0003-C12 Contact Center, Bot, and Application Integration

The organization MUST define, implement, verify, and maintain contact center, bot, and application integration for in-scope enterprise telephony and call control 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-TEL-0003 / TELECOMMUNICATIONS

5. Normative Control System

Atomic criteria 13-15 of 18

MYTHOS-TEL-0003-C13 QoS, Jitter, Loss, Latency, and MOS Evidence

The organization MUST define, implement, verify, and maintain qos, jitter, loss, latency, and mos evidence for in-scope enterprise telephony and call control 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-TEL-0003-C14 Monitoring, CDR, Trace, and Troubleshooting

The organization MUST define, implement, verify, and maintain monitoring, cdr, trace, and troubleshooting for in-scope enterprise telephony and call control 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-TEL-0003-C15 High Availability, Survivability, and Carrier Failure

The organization MUST define, implement, verify, and maintain high availability, survivability, and carrier failure for in-scope enterprise telephony and call control 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-TEL-0003 / TELECOMMUNICATIONS

5. Normative Control System

Atomic criteria 16-18 of 18

MYTHOS-TEL-0003-C16 Backup, Restore, and Disaster-Recovery Exercise

The organization MUST define, implement, verify, and maintain backup, restore, and disaster-recovery exercise for in-scope enterprise telephony and call control 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-TEL-0003-C17 Change, Upgrade, Certificate, and Codec Lifecycle

The organization MUST define, implement, verify, and maintain change, upgrade, certificate, and codec lifecycle for in-scope enterprise telephony and call control 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-TEL-0003-C18 Telephony Evidence and Periodic Reassessment

The organization MUST define, implement, verify, and maintain telephony evidence and periodic reassessment for in-scope enterprise telephony and call control 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-TEL-0003 / TELECOMMUNICATIONS

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	B	C	D
Independently reproducible, complete, current, integrity-protected, and representative.	Reproduced by the implementing organization with strong traceability and controlled scope.	Partially reproduced or indirect; limitations, inherited responsibility, and uncertainty recorded.	Assertion, diagram, design intent, certificate, or vendor statement without reproduced behavior.

MYTHOS-TEL-0003 / TELECOMMUNICATIONS

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-TEL-0003 / TELECOMMUNICATIONS

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-TEL-0003 / TELECOMMUNICATIONS

8. Failure Modes and Adversarial Scenarios

Challenge assumptions before the system is trusted with consequential work

SUBSCRIBER IDENTITY COMPROMISE

SIM, eSIM, credential, or provisioning weakness enables impersonation.

REQUIRED: PREVENT | DETECT | CONTAIN | RECOVER | EVIDENCE

SLICE ISOLATION FAILURE

A label implies isolation not enforced across radio, transport, core, edge, and cloud.

REQUIRED: PREVENT | DETECT | CONTAIN | RECOVER | EVIDENCE

SIGNALING ABUSE

Protocol manipulation causes fraud, denial, interception, or unauthorized routing.

REQUIRED: PREVENT | DETECT | CONTAIN | RECOVER | EVIDENCE

TIMING LOSS

Synchronization failure degrades radio, handoff, positioning, or service quality.

REQUIRED: PREVENT | DETECT | CONTAIN | RECOVER | EVIDENCE

RF INTERFERENCE

Coverage, PIM, noise, or external interference defeats expected service.

REQUIRED: PREVENT | DETECT | CONTAIN | RECOVER | EVIDENCE

EMERGENCY-SERVICE FAILURE

Calling, location, priority, public-safety, or survivability obligations are not met.

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.

MYTHOS-TEL-0003 / TELECOMMUNICATIONS

9. Implementation Profiles

Risk-proportional implementation without weakening mandatory boundaries

FOUNDATIONAL

TYPICAL SCOPE

Low consequence, limited autonomy, non-sensitive data, reversible outputs.

MINIMUM DEPTH

Named owner; inventory; basic evaluation; access control; logging; rollback; annual review.

ADVANCED

TYPICAL SCOPE

Business-critical workflow, sensitive data, multiple tools or providers, moderate autonomy.

MINIMUM DEPTH

Formal threat model; representative evaluation; approval gates; isolated execution; tested recovery; quarterly review.

HIGH ASSURANCE

TYPICAL SCOPE

Safety, security, regulated, financial, identity, or broadly consequential use.

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-TEL-0003 / TELECOMMUNICATIONS

9.2 Operational Lifecycle

Evidence-bearing operation from concept through retirement

1 **CONCEPT**
Purpose, owner, impact, boundaries

2 **DESIGN**
Architecture, threat, data, identity

3 **BUILD**
Controlled implementation and provenance

4 **EVALUATE**
Representative, adversarial, recovery tests

5 **RELEASE**
Approval, canary, rollback, evidence

6 **OPERATE**
Observe, support, detect, respond

7 **CHANGE**
Reassess, compare, gate, reverse

8 **RETIRE**
Revoke, export, dispose, preserve

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-TEL-0003 / TELECOMMUNICATIONS

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-TEL-0003 / TELECOMMUNICATIONS

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-TEL-0003 / TELECOMMUNICATIONS

11. Source Authority and Reference Register

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

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.

3GPP Specifications — **3GPP technical specifications and reports**

https://www.3gpp.org/specifications-technologies/specifications-by-series

Mobile-system architecture, security, radio, core, and service specifications.

O-RAN Alliance — **O-RAN specifications and security work**

https://www.o-ran.org/specifications

Open RAN architecture, interfaces, management, and security.

GSMA NESAS — **Network Equipment Security Assurance Scheme**

https://www.gsma.com/solutions-and-impact/technologies/security/network-equipment-security-assurance-scheme/

Telecom equipment security development and assessment scheme.

IETF SIP — **Session Initiation Protocol - RFC 3261**

https://www.rfc-editor.org/rfc/rfc3261

Core SIP signaling model and protocol semantics.

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-TEL-0003 / TELECOMMUNICATIONS

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-TEL-0003

MYTHOS SYSTEMS / ENGINEERING STANDARDS LIBRARY