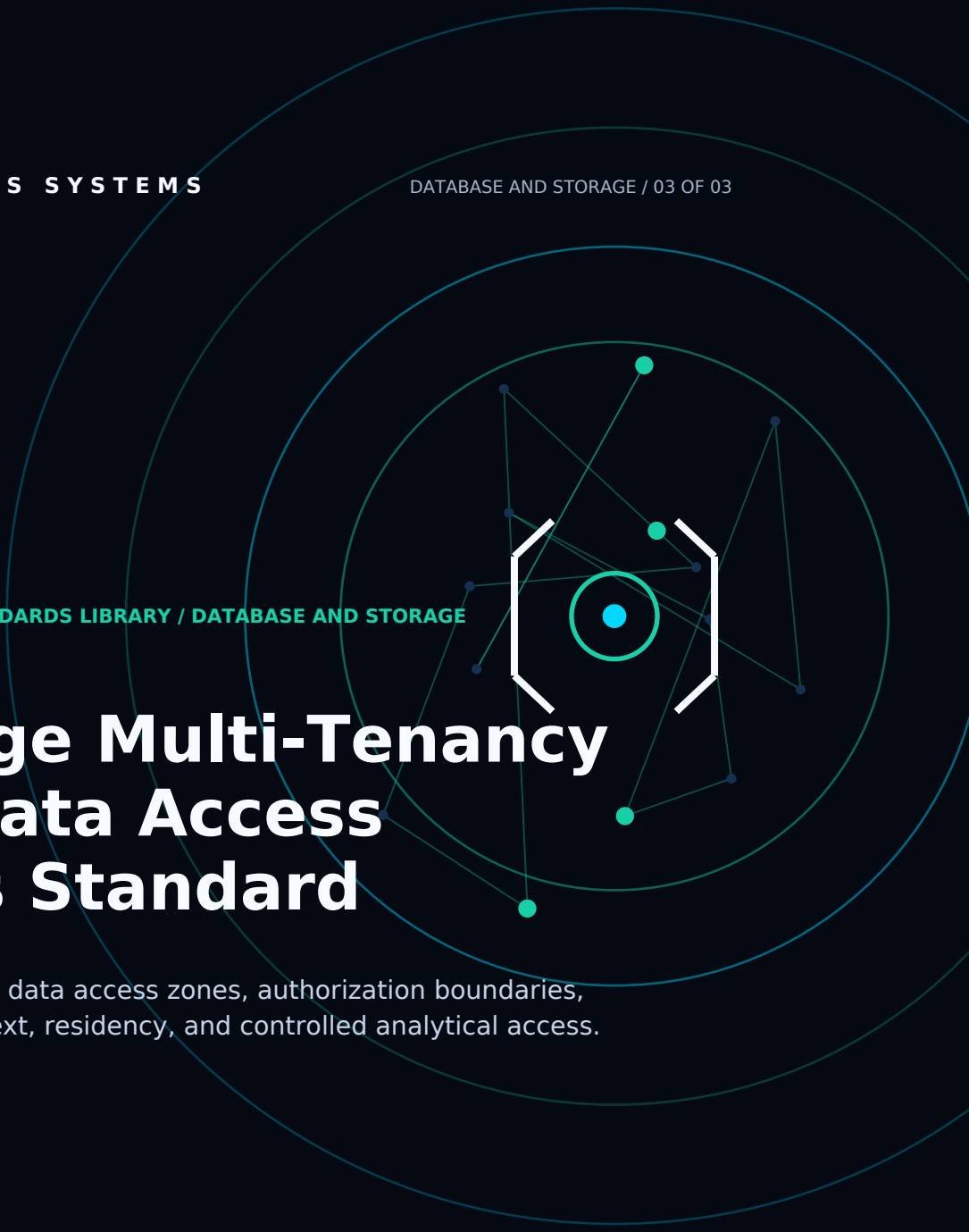


ENGINEERING STANDARDS LIBRARY / DATABASE AND STORAGE

Storage Multi-Tenancy and Data Access Zones Standard

Tenant isolation, data access zones, authorization boundaries, encryption context, residency, and controlled analytical access.

PERMANENT DOCUMENT ID

MYTHOS-DBS-0003

PUBLICATION

Candidate Standard
Version 1.0.0-candidate

ASSURANCE PROFILE

Standard / Advanced
High Assurance

PERMANENT PUBLICATION IDENTITY

Storage Multi-Tenancy and Data Access Zones Standard

DOCUMENT ID
MYTHOS-DBS-0003

VERSION
1.0.0-candidate

STATUS
Candidate Standard

PUBLISHER
Mythos Systems

PUBLICATION DATE
2026-07-24

SCHEDULED REVIEW
2027-01-24

12	6	4	1
ATOMIC CRITERIA	ASSURANCE VIEWS	IMPLEMENTATION PROFILES	PERMANENT IDENTITY

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

DOMAIN CONTROL SYSTEM

MYTHOS-DBS-0003 inside the database and storage standard constellation

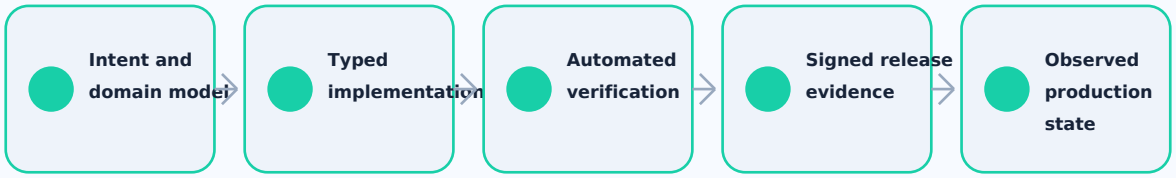
Connected assurance	Architecture, implementation, operations, evidence, and lifecycle are evaluated as one controlled system.
Specialization rule	Companion standards may add precision, but they cannot silently weaken this publication's requirements.

EXECUTIVE POSITION

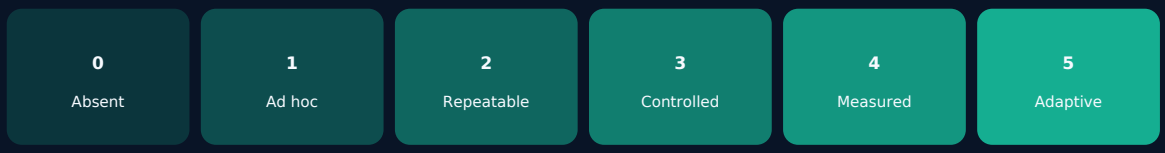
Storage Multi-Tenancy and Data Access Zones Standard

The architecture of multi-tenant storage has failed.

Evidence-bearing delivery path



Assurance maturity spectrum



CONTENTS

Publication navigation

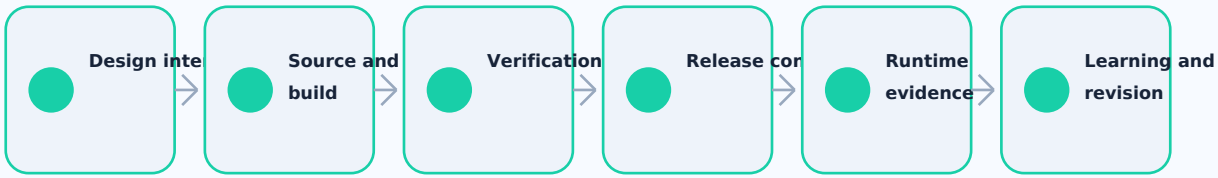
CONTROL TOPOLOGY

Assurance model and evaluation surface

The standard is assessed as an evidence-bearing system. Capability scores do not replace mandatory gates, implementation proof, or operational validation.

Capability family	Evaluation nodes
Logical Isolation (DAZ Boundaries) (Weight: 20%)	1
Independent Authentication Mapping (Weight: 20%)	1
Dedicated Network Groupnets (Weight: 15%)	1
Kubernetes CSI Integration (Weight: 15%)	1
Per-Zone Encryption (KMS) (Weight: 15%)	1
Observability and Auditability (Weight: 15%)	1
Suite Composition	2
Additional Evaluation Dimension	4

Lifecycle control loop



EVALUATION INDEX

Criteria and evidence map

#	Capability family	Criterion
1	Logical Isolation (DAZ Boundaries) (Weight: 20%)	Tenant Visibility
2	Independent Authentication Mapping (Weight: 20%)	Identity Boundary
3	Dedicated Network Groupnets (Weight: 15%)	Network Traffic Isolation
4	Kubernetes CSI Integration (Weight: 15%)	Cloud-Native Storage
5	Per-Zone Encryption (KMS) (Weight: 15%)	Cryptographic Sovereignty
6	Observability and Auditability (Weight: 15%)	Per-Tenant Telemetry
7	Suite Composition	MSTS-Isolation
8	Suite Composition	MSTS-Crypto
9	Additional Evaluation Dimension	Storage Tenancy Dimensions
10	Additional Evaluation Dimension	The Storage Tenancy Doctrine
11	Additional Evaluation Dimension	Scoring Model
12	Additional Evaluation Dimension	Suite Composition

NORMATIVE PUBLICATION

Requirements, evaluation methodology, and implementation guidance

The following body preserves the substantive source standard while normalizing publication status, identity, navigation, and visual presentation.

Executive Mandate

The architecture of multi-tenant storage has failed.

Organizations attempt to consolidate massive unstructured data lakes onto a single scale-out storage cluster (e.g., Dell PowerScale/Isilon, NetApp ONTAP) to maximize hardware utilization. To isolate tenants, they rely on filesystem permissions (POSIX ACLs, NTFS) and export rules. When a tenant's application is compromised, or an administrator misconfigures a share, the attacker can mount the cluster and map the directory structures of every other tenant on the physical fabric. Furthermore, because the entire cluster shares a single authentication provider (Active Directory), a compromise of the storage cluster's service account grants instant access to all data across all tenants.

This standard exists because:

1. Shared Namespaces are a Liability: Relying on filesystem permissions to isolate tenants guarantees eventual data leakage. Systems MUST implement logical Data Access Zones (DAZ) that partition the cluster at the OS and network levels, mathematically preventing cross-tenant visibility.
2. Authentication Must Be Bounded: A single cluster-wide authentication realm is a critical blast radius. Systems MUST map independent authentication providers (AD/LDAP) to each DAZ. A compromised credential in Tenant A's Active Directory MUST NOT be valid in Tenant B's Access Zone.
3. Network Traffic Must Be Isolated: Tenants sharing the same storage IP interfaces allows for packet sniffing and IP-spoofing based attacks. Systems MUST utilize dedicated network groupnets, subnets, and IP pools per DAZ, enforced by network microsegmentation.
4. Cloud-Native Storage Must Be Zone-Aware: Kubernetes persistent volumes (PVs) provisioned via Container Storage Interface (CSI) drivers frequently default to broad cluster access. Systems MUST bind CSI storage classes to specific DAZs, ensuring containerized workloads are physically incapable of mounting volumes outside their tenant boundary.

This document establishes the Mythos Storage Tenancy Standard (MSTS), a comprehensive, evidence-based methodology for evaluating enterprise storage clusters against absolute tenant isolation, cryptographic data sovereignty, and zero-trust access boundaries.

Scope and Applicability

In Scope

This standard covers the evaluation of:

1. Scale-out storage architectures (Dell PowerScale/Isilon, NetApp, Pure FlashBlade)
1. Data Access Zones (DAZ) and logical cluster partitioning
1. Multi-tenant authentication mapping (AD/LDAP/IdP integration)
1. Network groupnets, subnet pools, and SmartConnect zones
1. Kubernetes Container Storage Interface (CSI) multi-tenancy
1. Per-zone Key Management Service (KMS) integration and cryptographic erasure

Out of Scope

1. General relational database scaling (covered in MYTHOS-DBS-0001)
1. General network microsegmentation policy (covered in MYTHOS-SEC-0007)
1. General identity and PKI infrastructure (covered in MYTHOS-ID-0001)

Audience

1. Storage architects and infrastructure engineers
1. Platform engineers managing Kubernetes stateful workloads
1. Security engineers evaluating multi-tenant data isolation
1. Compliance teams managing sovereign data boundaries
1. Standards bodies seeking a reference storage tenancy methodology

Definitions and Taxonomy

Storage Tenancy Dimensions

Dimension	Definition
Data Access Zone (DAZ)	A logical partition within a physical storage cluster that isolates data, network configurations, and authentication systems, rendering tenants invisible to one another.
Groupnet	A networking construct (specifically in PowerScale/Isilon) that defines a distinct subnet, IP address pool, and DNS zone for a specific Access Zone, ensuring network traffic isolation.
Auth Mapping	The architectural practice of binding a specific, external authentication provider (e.g., a dedicated Active Directory forest or LDAP tree) exclusively to a single Data Access Zone.
Zone-Aware CSI	A Kubernetes Container Storage Interface driver configuration where StorageClasses are explicitly bound to a specific tenant's Access Zone, restricting PV provisioning to that isolated domain.
Cryptographic Erasure	The process of rendering a tenant's data permanently unreadable by securely destroying the specific Data Encryption Key (DEK) assigned to their Access Zone, rather than overwriting the physical disks.

The Storage Tenancy Doctrine

> A filesystem permission is a suggestion; an Access Zone is a boundary. A shared authentication realm is a critical blast radius. A shared IP interface is a sniffing vector. If Tenant A can map Tenant B's directory structure, the architecture has failed.

Evaluation Methodology

Scoring Model

Each capability is scored from 0 to 5.

Score	Meaning
0	Fails basic task; single namespace, shared AD, filesystem ACLs for isolation
1	Basic share-level access, but shared authentication and network planes
2	Functional isolation, but lacks independent auth mapping or CSI integration
3	Solid production performance; DAZ implemented, independent AD, dedicated groupnets, zone-aware CSI
4	Strong performance; Per-zone KMS encryption, formally verified network isolation
5	Best-in-class; sets the standard for mathematically proven, zero-trust storage tenancy

Weighting

Category	Weight	Rationale
Logical Isolation (DAZ Boundaries)	20%	Shared namespaces guarantee eventual cross-tenant data leakage
Independent Authentication Mapping	20%	Shared AD realms allow compromised credentials to pivot across tenants
Dedicated Network Groupnets	15%	Shared IP interfaces allow packet sniffing and ARP spoofing
Kubernetes CSI Integration	15%	Default CSI configurations allow containers to mount any PV
Per-Zone Encryption (KMS)	15%	Cluster-wide encryption keys prevent secure cryptographic erasure
Observability & Auditability	15%	Multi-tenant environments require per-tenant audit trails

Total: 100%

A system MUST score at least 3.0 in Logical Isolation and Independent Authentication to be considered for production.

Evaluation Categories

Logical Isolation (DAZ Boundaries) (Weight: 20%)

Tenant Visibility

Is the physical storage cluster partitioned into logically invisible Access Zones?

Score	Criteria
0	Single namespace; tenants share the same root directory and can browse each other's folders
1	Separate shares/export points, but the underlying namespace is visible
2	Separate filesystems/subdirectories, but managed via a single cluster control plane
3	Full Data Access Zone (DAZ) implementation: Tenants connect to zone-specific IP interfaces and can only see their own root directory; cross-zone visibility is abolished
4	Zone-specific SMB shares and NFS exports with strict host-based access controls mapped to DAZ network pools
5	Perfect isolation: Formally verified DAZ boundaries, zero ability for a tenant to enumerate or access another tenant's data structures, cryptographic proof of tenancy separation

Independent Authentication Mapping (Weight: 20%)

Identity Boundary

Does each tenant utilize a dedicated authentication provider, or do they share a cluster-wide AD?

Score	Criteria
0	Single cluster-wide Active Directory/LDAP integration for all tenants
1	Multiple AD domains, but joined into a single trust forest on the storage cluster
2	Separate AD domains, but the storage cluster uses a shared service account to join them all
3	Independent Auth Mapping: Each DAZ is joined to a completely separate, tenant-specific AD/LDAP/IdP with no trust relationship
4	Per-zone local service accounts; cluster management plane utilizes ZTNA and PAM, decoupled from tenant data access
5	Perfect boundary: Formally verified identity isolation, zero cross-tenant credential validity, cryptographic non-repudiation of per-zone access

Dedicated Network Groupnets (Weight: 15%)

Network Traffic Isolation

How is storage network traffic isolated between tenants?

Score	Criteria
0	All tenants connect to the same storage IP interfaces (SmartConnect zones)
1	Separate VLANs, but routed through the same storage cluster interfaces

Score	Criteria
2	Dedicated IP pools per tenant, but sharing the same physical L2 broadcast domain
3	Dedicated Groupnets: Each DAZ possesses its own subnet, IP address pool, and DNS zone, mapped to dedicated physical or logically partitioned network interfaces
4	Storage interfaces mapped to tenant-specific VRFs (Virtual Routing and Forwarding) or physical DPUs, enforcing L3 isolation
5	Perfect isolation: Formally verified network boundaries, zero ability to sniff or spoof neighboring tenant traffic, mathematical proof of groupnet segregation

Kubernetes CSI Integration (Weight: 15%)

Cloud-Native Storage

How are Kubernetes persistent volumes (PVs) provisioned and bound to tenants?

Score	Criteria
0	Single default StorageClass used by all namespaces; any pod can request a PV
1	Multiple StorageClasses, but they share the same underlying storage pool and access zone
2	Tenant-specific StorageClasses, but lacking network or auth isolation on the backend
3	Zone-Aware CSI: StorageClasses are explicitly parameterized to provision volumes within a specific DAZ; Kubernetes RBAC restricts namespaces to their corresponding StorageClass
4	CSI drivers utilize per-tenant cloud credentials or Kerberos tickets to mount volumes, authenticating directly to the tenant's DAZ
5	Perfect integration: Formally verified CSI RBAC, zero ability for a container to mount a cross-tenant PV, mathematical proof of cloud-native tenancy isolation

Per-Zone Encryption (KMS) (Weight: 15%)

Cryptographic Sovereignty

Is data encrypted at rest with per-tenant keys?

Score	Criteria
0	No encryption at rest
1	Cluster-wide encryption utilizing a single shared key
2	Self-encrypting drives (SEDs) with a single global key
3	Per-zone KMS integration: Each DAZ is bound to a tenant-specific Key Encryption Key (KEK) in an external KMS (e.g., HashiCorp Vault, AWS KMS)
4	Per-volume/per-file encryption utilizing tenant-specific Data Encryption Keys (DEKs) wrapped by the zone KEK
5	Perfect sovereignty: Formally verified cryptographic boundaries, zero ability to read tenant data without their specific KEK, mathematical proof of secure cryptographic erasure upon tenant offboarding

Observability and Auditability (Weight: 15%)

Per-Tenant Telemetry

Can security teams attribute every storage access event to a specific tenant and zone?

Score	Criteria
0	Single cluster-wide audit log; impossible to distinguish tenant actions
1	Basic logging, but lacks zone context or user attribution
2	Per-zone logging, but requires manual extraction and correlation
3	Per-DAZ audit logs streamed to a centralized SIEM, tagged with tenant ID, zone ID, and user identity
4	Real-time anomaly detection per tenant (e.g., detecting a sudden spike in reads indicative of data exfiltration)
5	Perfect observability: Formally verified audit trails, zero blind spots in cross-tenant telemetry, cryptographic attestation of per-zone data access

The Mythos Storage Suite (MSTS)

Traditional benchmarks measure IOPS (Input/Output Operations Per Second). The MSTS evaluates cross-tenant visibility, auth isolation, and cryptographic sovereignty.

Suite Composition

MSTS-Isolation

1. Cross-Zone Mount Test: 100+ tests attempting to mount Tenant B's NFS export or SMB share using Tenant A's credentials and network interface, verifying the DAZ and groupnet boundaries drop the connection.
1. Namespace Enumeration Test: 50+ tests attempting to browse the root directory of the storage cluster from a tenant context, verifying the DAZ restricts visibility to only the tenant's specific directory.

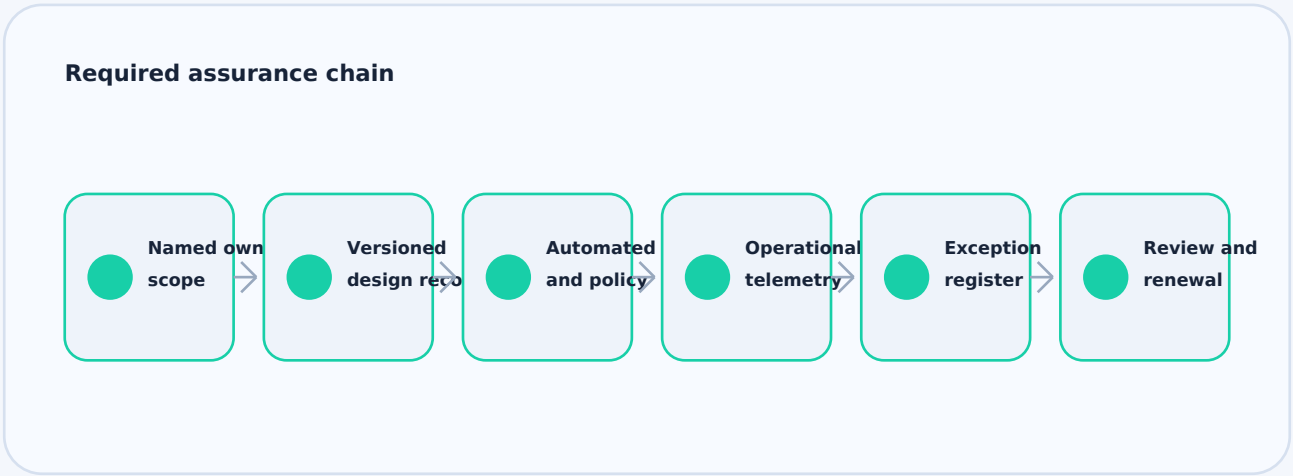
MSTS-Crypto

1. Cryptographic Erasure Test: 100+ tests simulating the offboarding of a tenant, verifying that destroying their KMS key immediately renders all their data on the physical cluster permanently unreadable (zero plaintext remnants).
1. CSI Privilege Escalation Test: 50+ tests attempting to provision a Persistent Volume in Tenant A's Kubernetes namespace using Tenant B's StorageClass, verifying RBAC and zone-aware CSI block the action.

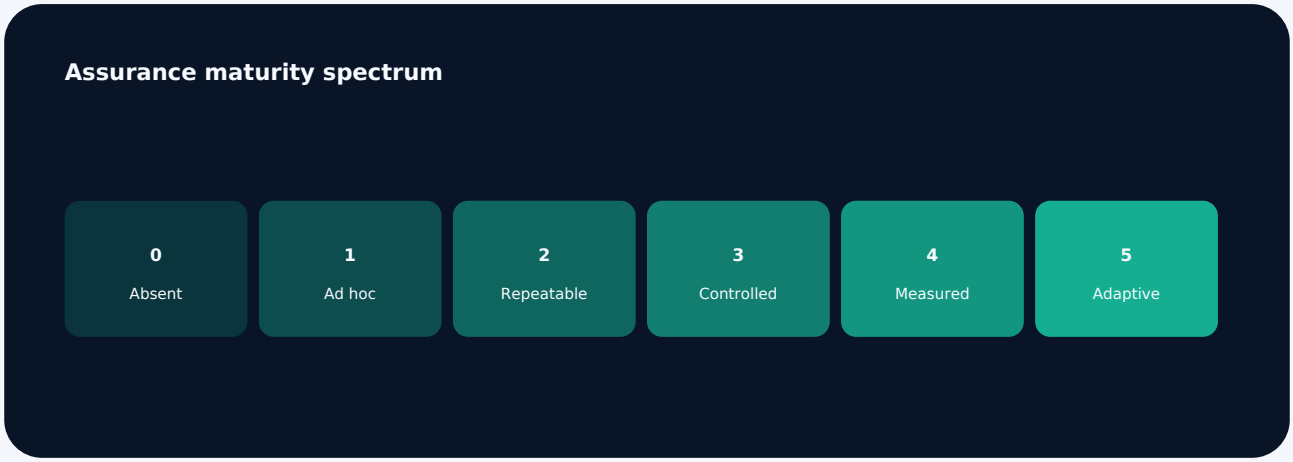
Execution Protocol

ASSURANCE AND ADOPTION

Implementation evidence and review gates



A passing score is not sufficient without current evidence. High-assurance adoption requires traceable design decisions, reproducible builds, independently reviewable tests, controlled secrets, runtime observability, failure exercises, and a dated exception register.



Current authority register

Authority	Version / snapshot	Applicability	Review by
OpenTelemetry Project: OpenTelemetry Documentation and Specification	Rolling specification snapshot; profiles public alpha and declarative configuration stable in 2026	High	2026-10-22
PostgreSQL Global Development Group: PostgreSQL Documentation	Rolling official documentation snapshot	High	2026-10-22

Research limitation. Official documentation establishes published interfaces and declared behavior. It does not prove the performance, security, interoperability, cost, or operational suitability of a specific implementation. Those claims require controlled testing and retained evidence.