ENGINEERING STANDARDS LIBRARY / RELIABILITY ENGINEERING

Disaster Recovery, Multi-Region, and Failure Testing Standard

Failure-domain architecture, recovery objectives, multi-region design, restore validation, game days, and crisis readiness.

PERMANENT DOCUMENT ID

MYTHOS-SRE-0002

PUBLICATION

Candidate Standard
Version 1.0.0-candidate

ASSURANCE PROFILE

Standard / Advanced
High Assurance

PERMANENT PUBLICATION IDENTITY

Disaster Recovery, Multi-Region, and Failure Testing Standard

DOCUMENT ID
MYTHOS-SRE-0002

VERSION
1.0.0-candidate

STATUS
Candidate Standard

PUBLISHER
Mythos Systems

PUBLICATION DATE
2026-07-24

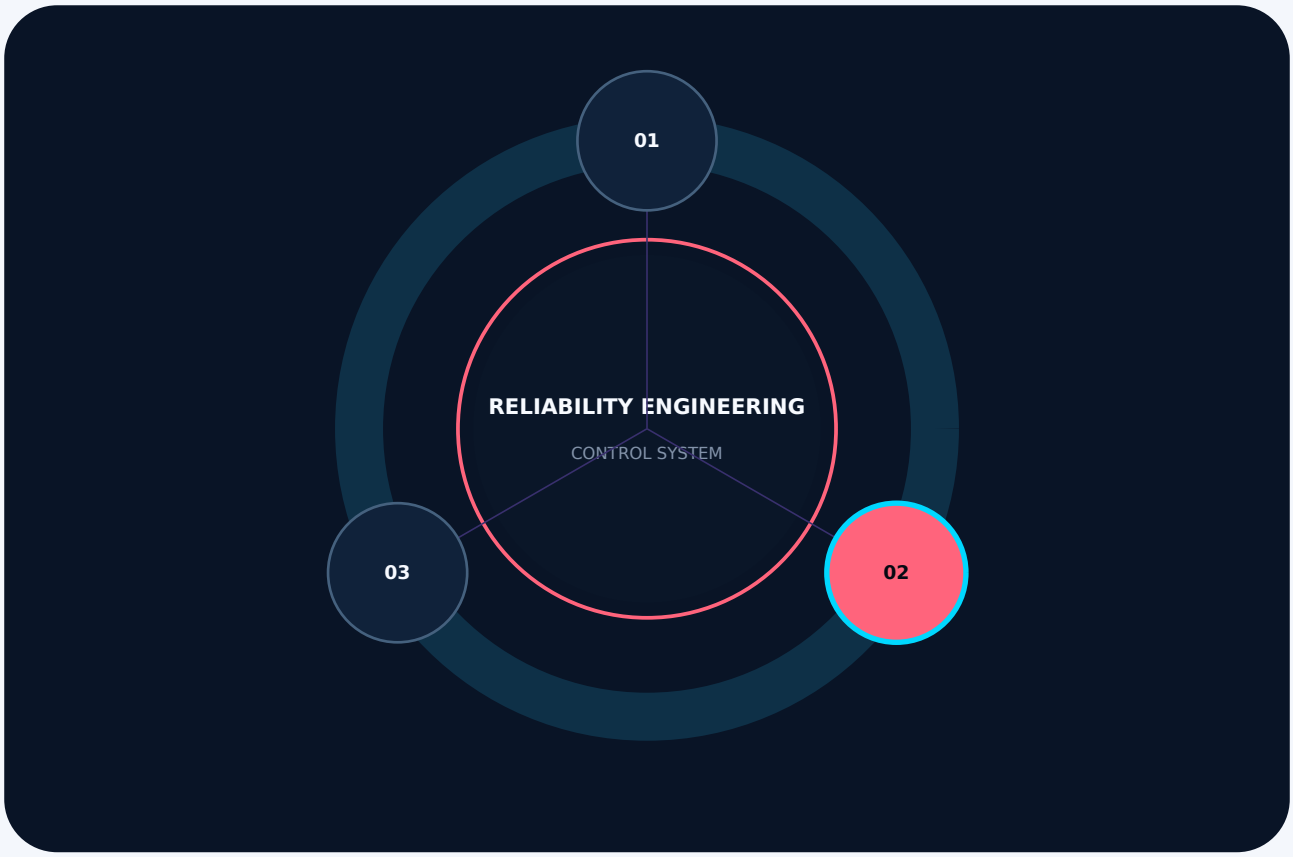
SCHEDULED REVIEW
2027-01-24

11	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-SRE-0002 inside the reliability engineering standard constellation

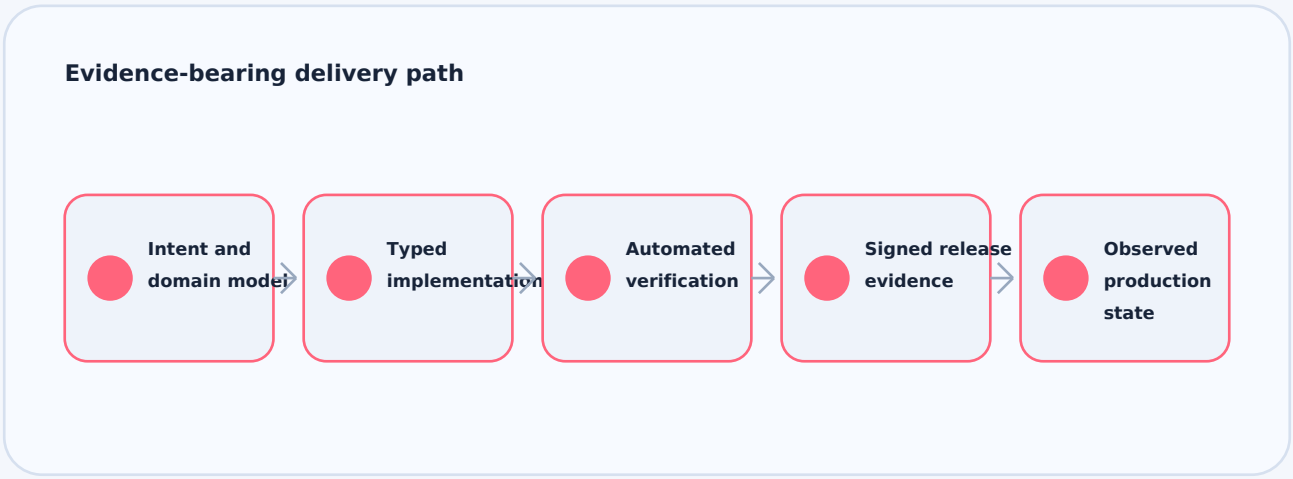


Connected assurance	Architecture, implementation, operations, evidence, and lifecycle are evaluated as one controlled system.
Specialization rule	Companion standards may add precision, but they cannot silently weaken this publication's requirements.

EXECUTIVE POSITION

Disaster Recovery, Multi-Region, and Failure Testing Standard

The architecture of disaster recovery has failed.



CONTENTS

Publication navigation

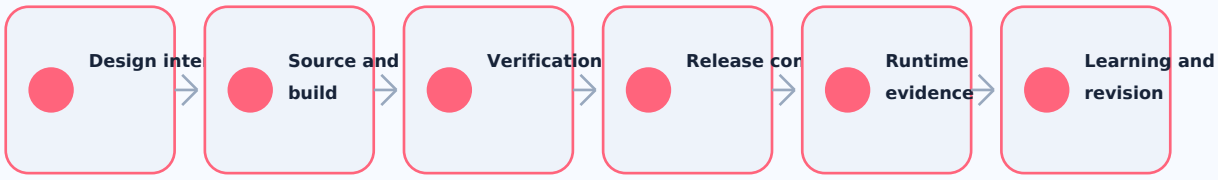
CONTROL TOPOLOGY

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
Multi-Region Topology & Traffic Shifting (Weight: 20%)	1
RTO/RPO Enforcement & State Integrity (Weight: 20%)	1
Chaos Engineering & Fault Injection (Weight: 20%)	1
Stateful Recovery & Durable Replay (Weight: 15%)	1
Blast Radius & Cell-Based Architecture (Weight: 15%)	1
Automation & Runbook Execution (Weight: 10%)	1
Suite Composition	2
Additional Evaluation Dimension	3

Lifecycle control loop



EVALUATION INDEX

Criteria and evidence map

#	Capability family	Criterion
1	Multi-Region Topology & Traffic Shifting (Weight: 20%)	Global Routing
2	RTO/RPO Enforcement & State Integrity (Weight: 20%)	Data Loss Bounds
3	Chaos Engineering & Fault Injection (Weight: 20%)	Resilience Validation
4	Stateful Recovery & Durable Replay (Weight: 15%)	Workflow Continuity
5	Blast Radius & Cell-Based Architecture (Weight: 15%)	Containment
6	Automation & Runbook Execution (Weight: 10%)	Operator Intervention
7	Suite Composition	MDRS-Blackout
8	Suite Composition	MDRS-Chaos
9	Additional Evaluation Dimension	DR Dimensions
10	Additional Evaluation Dimension	The DR Doctrine
11	Additional Evaluation Dimension	Scoring Model

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 disaster recovery has failed.

Organizations write 100-page DR runbooks that are never executed until a catastrophic outage occurs. When the cloud provider's primary region goes down, they attempt to failover to the passive region, only to discover the DNS TTL is too high, the database replicas are 5 hours stale, and the application cannot start because it hardcodes the primary region's S3 bucket name.

This standard exists because:

1. An Untested DR Plan is Fiction: A DR strategy that relies on a PDF document and manual operator intervention during a 3 AM crisis is guaranteed to fail. DR plans MUST be continuously automated and tested in production via chaos engineering.
2. Active-Passive is a Legacy Crutch: A hot-standby region that sits idle is a waste of capital and a reliability risk. When failover occurs, the passive region is instantly overwhelmed by production traffic it has never handled. Architectures MUST be active-active, serving live traffic from all regions simultaneously.
3. RTO/RPO Must Be Mathematically Bounded, Not Hoped For: "We aim for zero data loss" is a wish, not an architecture. Recovery Time Objective (RTO) and Recovery Point Objective (RPO) MUST be mathematically enforced by synchronous replication, automated traffic shifting, and durable execution runtimes.
4. Stateful Failover is the Hardest Problem: Stateless compute fails over easily; databases do not. Relying on asynchronous database replication guarantees data loss (RPO > 0). Systems MUST utilize distributed SQL, CRDTs, or event sourcing to ensure state convergence across regions without split-brain.

This document establishes the Mythos DR & Resilience Standard (MDRS), a comprehensive, evidence-based methodology for evaluating disaster recovery architectures against active-active topology, chaos readiness, and mathematically proven state integrity.

Scope and Applicability

In Scope

This standard covers the evaluation of:

1. Multi-region architectures (Active-Active vs. Active-Passive)

1. Recovery Time Objective (RTO) and Recovery Point Objective (RPO) enforcement
1. Global traffic management and DNS failover (Route 53, Cloudflare)
1. Chaos engineering and fault injection (Gremlin, Chaos Mesh)
1. Stateful DR: Distributed SQL, synchronous replication, CRDTs
1. Durable execution replay and workflow recovery

Out of Scope

1. General SLO definitions and alerting (covered in MYTHOS-SRE-0001)
1. General event sourcing patterns (covered in MYTHOS-DAT-0004)
1. General database high availability (covered in MYTHOS-DBS-0001)

Audience

1. Site Reliability Engineers (SREs) and platform architects
1. Distributed systems engineers building multi-region services
1. Security engineers evaluating ransomware regional isolation
1. Compliance teams managing RTO/RPO mandates
1. Standards bodies seeking a reference DR methodology

Definitions and Taxonomy

DR Dimensions

Dimension	Definition
RTO (Recovery Time Objective)	The maximum acceptable time between a disaster and the restoration of service. Enforced by automated traffic shifting and infrastructure provisioning.
RPO (Recovery Point Objective)	The maximum acceptable amount of data loss, measured in time. Enforced by synchronous replication or durable event sourcing.
Active-Active Multi-Region	An architecture where multiple geographic regions simultaneously serve live production traffic and replicate state bi-directionally.
Chaos Engineering	The discipline of experimenting on a system by injecting failures (e.g., killing pods, severing network links) in production to verify resilience and validate DR assumptions.
Split-Brain	A failure scenario where a network partition causes two regions to both assume they are the primary write master, resulting in irreconcilable data conflicts.
CRDT (Conflict-free Replicated Data Type)	A data structure that can be replicated across multiple networked computers, updated independently and concurrently, and mathematically resolved without conflicts.

The DR Doctrine

> An untested DR plan is fiction. Active-passive is a waste of capital. An RPO of zero requires synchronous math, not hope. If you are not injecting failures in production, you are flying blind.

Evaluation Methodology

Scoring Model

Each capability is scored from 0 to 5.

Score	Meaning
0	Fails basic task; single region, paper DR plan, async DB replication, no chaos
1	Basic backups to another region, but manual restore required
2	Functional active-passive, but RPO > 0 and failover is manual/scripted
3	Solid production performance; Active-Active, RTO/RPO bounded, automated failover, chaos in staging
4	Strong performance; RPO=0 via sync replication, chaos in prod, CRDT/distributed SQL state
5	Best-in-class; sets the standard for mathematically verified, autonomous regional resilience

Weighting

Category	Weight	Rationale
Multi-Region Topology & Traffic Shifting	20%	Active-passive fails under sudden load shifts; DNS TTLs cause outages
RTO/RPO Enforcement & State Integrity	20%	Async replication guarantees data loss; RPO=0 requires synchronous math
Chaos Engineering & Fault Injection	20%	Untested failover mechanisms guarantee failure during a real disaster
Stateful Recovery & Durable Replay	15%	Stateless compute is easy; database failover is the true test
Blast Radius & Cell-Based Architecture	15%	A failure in one region or service must not cascade globally
Automation & Runbook Execution	10%	Manual operator intervention during a crisis is too slow

Total: 100%

A system MUST score at least 3.0 in Multi-Region Topology and Chaos Engineering to be considered for production use.

Evaluation Categories

Multi-Region Topology & Traffic Shifting (Weight: 20%)

Global Routing

How is traffic routed and failed over between regions?

Score	Criteria
0	Single region; no failover capability
1	Active-Passive; manual DNS updates required to failover (RTO > 1 hour)

Score	Criteria
2	Automated DNS failover, but high TTLs (minutes) cause partial outages
3	Active-Active: both regions serve live traffic; global load balancer routes based on latency/health
4	Sub-second traffic shifting via BGP Anycast or global mesh routing
5	Perfect topology: formally verified routing bounds, zero DNS caching delays, seamless regional evacuation

RTO/RPO Enforcement & State Integrity (Weight: 20%)

Data Loss Bounds

Are RTO and RPO mathematically guaranteed, or just hoped for?

Score	Criteria
0	Async DB replication; RPO is "whatever the replication lag is" (data loss guaranteed)
1	Periodic snapshots to backup region; RPO > 1 hour
2	Near-real-time replication, but accepts data loss on failover
3	Synchronous replication ensuring RPO = 0 (zero data loss)
4	Distributed SQL (CockroachDB/Spanner) or CRDTs providing globally consistent state
5	Perfect integrity: formally verified consensus algorithms, zero split-brain risk, mathematical proof of state parity

Chaos Engineering & Fault Injection (Weight: 20%)

Resilience Validation

Is the DR plan continuously tested via failure injection?

Score	Criteria
0	No testing; DR plan exists only in a document
1	Failover tested manually once a year
2	Chaos engineering in staging environment
3	Chaos engineering in production (e.g., killing pods, severing network links)
4	Automated Game Days simulating full regional blackouts
5	Perfect validation: formally verified blast radius bounds, continuous autonomous failure injection, mathematical proof of self-healing

Stateful Recovery & Durable Replay (Weight: 15%)

Workflow Continuity

Can long-running workflows and agent tasks survive a regional failure?

Score	Criteria
0	In-memory workflows; state lost on regional crash

Score	Criteria
1	Checkpoints exist, but manual restart required
2	Workflows recover, but side-effects may be re-executed (violating idempotency)
3	Durable execution runtime (Temporal) with global state store; workflows replay deterministically
4	Multi-region durable runtime; workflows seamlessly migrate to healthy region
5	Perfect continuity: formally verified deterministic replay, zero side-effect duplication, sub-second state migration

Blast Radius & Cell-Based Architecture (Weight: 15%)

Containment

Can a failure in one service or region be prevented from cascading globally?

Score	Criteria
0	Shared global dependency (e.g., single global database); failure cascades everywhere
1	Basic namespace isolation, but shared control plane
2	Regional isolation for compute, but shared global state
3	Cell-based architecture: each region/cell is fully self-contained and independent
4	Bulkheads and circuit breakers preventing cross-cell cascading failures
5	Perfect containment: formally verified blast radius limits, zero cross-regional cascade potential

Automation & Runbook Execution (Weight: 10%)

Operator Intervention

How much human intervention is required during a regional disaster?

Score	Criteria
0	100% manual; engineers must SSH into boxes and run scripts
1	Runbooks exist, but require manual step-by-step execution
2	Single-click failover scripts, but require human authorization
3	Fully automated failover triggered by health checks; humans only observe
4	Autonomous failover with automated rollback if the recovery fails
5	Perfect automation: formally verified runbook execution, zero human latency in the recovery path

The Mythos DR Suite (MDRS)

Traditional DR benchmarks measure backup restore speed. The MDRS evaluates regional blackout survival, state convergence, and zero-downtime traffic shifting.

Suite Composition

MDRS-Blackout

1. Region Kill Test: 100+ tests simulating a total AWS region failure (cutting all network and API access), verifying traffic shifts to the secondary region in < 60 seconds (RTO).
1. State Parity Test: 50+ tests verifying that the secondary region has zero data loss (RPO = 0) after the failover.

MDRS-Chaos

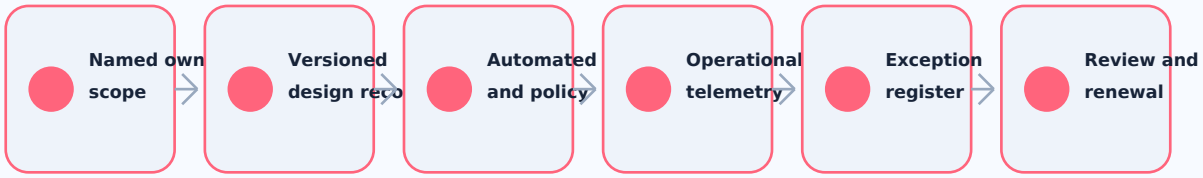
1. Latency Injection Test: 100+ tests injecting 500ms network latency between regions, verifying the distributed SQL/CRDT state converges without timing out.
1. Pod Destruction Test: 50+ tests randomly killing 30% of stateless pods in production, verifying the auto-scaler and mesh reroute traffic without breaching SLOs.

Execution Protocol

ASSURANCE AND ADOPTION

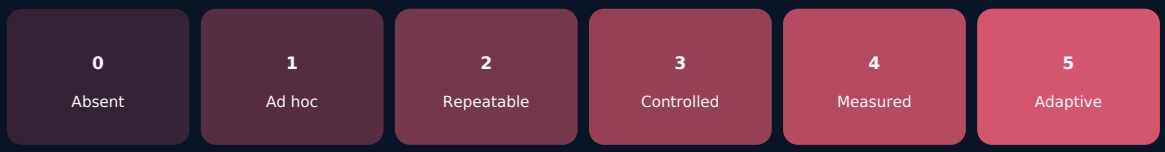
Implementation evidence and review gates

Required assurance chain



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.

Assurance maturity spectrum



Current authority register

Authority	Version / snapshot	Applicability	Review by
TLA+ Foundation: TLA+ Language and Tools Documentation	Rolling documentation snapshot	High	2027-01-24
Kubernetes Project: Kubernetes Documentation	v1.36 current documentation	High	2026-10-22
OpenTelemetry Project: OpenTelemetry Documentation and Specification	Rolling specification snapshot; profiles public alpha and declarative configuration stable in 2026	High	2026-10-22
Cloud Native Computing Foundation: Cloud Native Landscape and Project Documentation	Rolling catalog snapshot	Moderate	2026-08-23
FinOps Foundation: FinOps Framework and FOCUS Specification	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.