**1) BCP/DR & RTO/RPO — “Failover That Proves Itself”**

**Intent**  
Guarantee business continuity with verifiable backups, regional failover, and rehearsed recovery that does not corrupt compliance lineage.

**Actors**  
BCP Orchestrator • Storage Snapshotter • DR Region • Ops Pilot • Audit Vault

**Preconditions**

* Data domains tagged: Config, Hot Paths (gatecache), Operational (queues), Cold Stores (snapshots, audit).
* KMS keys in multi-region HSM with dual custody.
* Runbooks templated (Game Day scripts).

**Flow (happy path)**

1. **Continuous Snapshots**: hourly object-store versions for Cold Stores; 5-min WAL for Operational DBs.
2. **Integrity Stamps**: each backup batch includes a **Backup Trust Stamp** (dataset + hash + signer + time).
3. **Warm DR Region**: infra standing by; data replicated async; **readiness probes** green.
4. **Game Day Drill (automated)**: quarterly, Orchestrator simulates region loss → flips DNS, promotes DR DB, warms gatecache, replays last WAL.
5. **Lineage Verifier**: replays a random sample of historic **decisions** using restored snapshots/rules; outcomes must match bit-for-bit.
6. **Cut Back**: once primary stable, perform controlled failback with delta compare and stamp.
7. **Evidence Pack**: drill produces a **BCP Proof Bundle** (RTO, RPO achieved, sampled decisions’ hashes, operator approvals).

**Failure/Alternates**

* Promote blocked? auto-retry with smaller shard sets; manual escalation path.
* Key escrow failure? switch to secondary HSM quorum; log incident.

**Acceptance**

* **RTO** ≤ 60 min; **RPO** ≤ 5 min (configurable per tenant tier).
* 100% of sampled decisions **match** post-restore.
* Drill runs ≥ 1/quarter and generates a signed Proof Bundle.

**Innovations**

* **Backup Trust Stamp** + **Decision Replay Verifier** (not just infra up — correctness proven).
* Push-button Game Day with synthetic traffic.