

FRAMEWORK #163

Your Recovery Plan Passed. The Business Didn't Come Back.

CONTINUITY EXECUTION BOUNDARY

THE DISTINCTION

Recovery Success $\neq$ Continuity

RECOVERY

Infrastructure came back

CONTINUITY?

Is the business operating — untested

Two different claims. Most DR programs treat them as one.

01

Condition

02

Boundary

03

Failure State

04

Consequence

The Condition

Recovery has been designed, executed, isolated, and adversarially validated — D1 through D4.

FRAMEWORK #163 — STAGE 2 OF 4



The Boundary

Continuity depends on dependencies and ownership decisions that don't automatically travel with a successful failover.

FRAMEWORK #163 — STAGE 3 OF 4

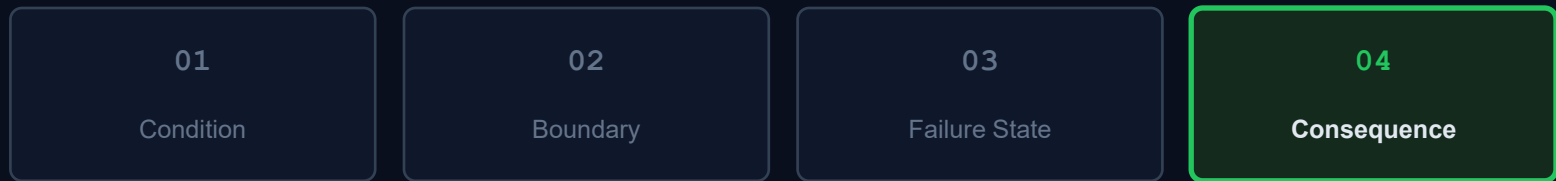


The Failure State

Failover passes every test. The assumptions underneath it were never validated under real conditions.

CONTINUITY THEATER

FRAMEWORK #163 — STAGE 4 OF 4



The Consequence

The gap surfaces mid-incident — discovered live, instead of during design when it would have been cheap to catch.

WHERE THE BOUNDARY ACTUALLY SITS

Six Domains — Part 1 of 2



Does the identity provider, DNS resolution, and certificate chain survive the failover — or just the workload?

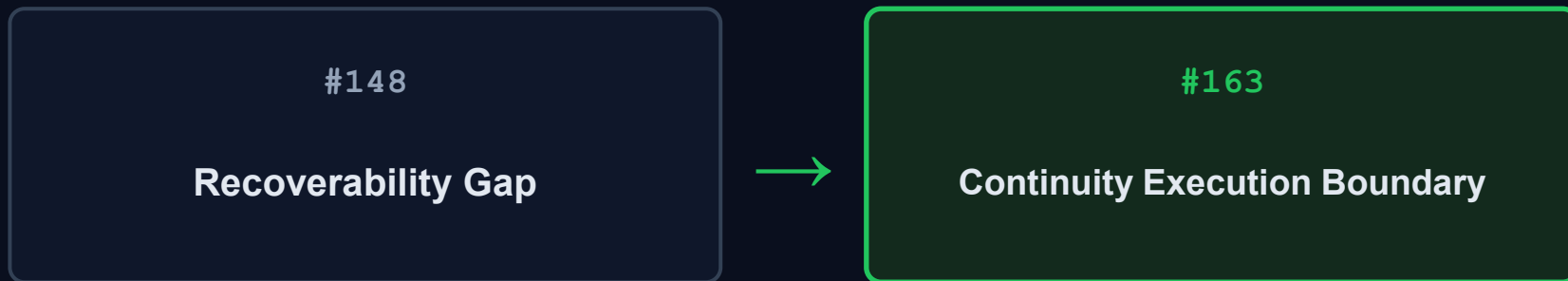
WHERE THE BOUNDARY ACTUALLY SITS

Six Domains — Part 2 of 2



Do routing, control-plane ownership, and the application itself survive — or were they scoped only for steady state?

This Only Matters Once #148 Is Closed



Testing continuity before recovery survives compromise answers a question with no foundation.

A Green Dashboard Isn't a Continuity Test.

Rack2Cloud.com

Follow The Architect for more