DATA PROTECTION · DOWNLOAD ASSET

Adversarial Restore Test Design Checklist

Structuring staged sabotage, blast-radius containment, and cadence when moving a DR program from cooperative to adversarial restore testing.

01 — KILL SWITCH INDEPENDENCE

- [ ] Kill switch sits outside the systems being deliberately degraded
- [ ] Kill switch tested and confirmed functional before the first live drill
- [ ] Kill switch authority assigned to a named role — not "whoever's available"

02 — CADENCE & SCOPE

- [ ] One failure mode targeted per drill, not all failure modes at once
- [ ] Quarterly cadence minimum for adversarial drills
- [ ] Scope bounded explicitly to the restore path — not the full production estate
- [ ] Written scope boundary reviewed and signed off before each drill runs

03 — FAILURE MODES TO COVER

- [ ] Credential revocation mid-restore
- [ ] DNS unavailable during failover
- [ ] Identity provider unavailable
- [ ] Control plane degraded under load
- [ ] Repository under active denial
- [ ] Key operator unavailable / partial context

04 — BEFORE CALLING THE PROGRAM COMPLETE

- [ ] Every row above has been run adversarially at least once — not just planned
- [ ] Findings from each drill fed back into the recovery runbook, not just a report
- [ ] Recovery Readiness Analyzer re-run against updated assumptions post-drill