How I Run a Technology Assessment

An assessment tells you where your technology stands against your own targets, what each gap would cost to close, and which ones are worth closing first. The output is a ranked list with numbers attached, not a verdict.

Measured against your targets

Your RTO, RPO, availability and SLA commitments, including what you have already promised customers in writing.

Ranked, not listed

Every gap carries cost and benefit. I supply the order; the decision stays yours.

One view across teams

Hosting, architecture, backup, database, application and security described as a single system, which nobody inside is positioned to do.

Five lenses, three questions each

People
Ownership, depth of cover, key-person risk

Process
Change control, incident response, DR testing

Tools
What is licensed, what is used, spend, renewals

Technology
Topology, redundancy, patch and hardening state

Organization
Structure across sites and teams, and the seams

How it works today → **Industry benchmark** → **The gap**

Every finding is labeled by how I know it: *verified* when I have seen the artifact or watched the test; *asserted, not verified* when I was told and could not confirm it. Both go in the report; the label never drops.

Timeline: focused assessment of one problem area, 2 to 3 weeks. Full assessment, 4 to 5 weeks, including a second interview pass to close what the first pass left open.

Documents on day one; people by name

Artifacts I request

- Network, server and data-center configuration, as built
- Backup schedules, retention, 90 days of job results
- Last disaster-recovery test and what was left open
- Written RTO, RPO, availability and SLA targets
- Vendor contracts, current spend, renewal dates
- Latest pen-test and vulnerability reports
- Customer security questionnaire responses; 12-month incident log

Who I interview, and for how long

- Hosting and infrastructure: 90 min, then 45
- Architecture: 90 min, then 45
- Backup and recovery: 90 min, then 45
- Database; application and release: 60 min, then 30
- Security tooling owner: 90 min, then 45
- Key vendors: 45 min each
- Executive sponsor: at kickoff and at draft

If something on the list does not exist, that absence is itself a finding. It is not a reason to delay.

What I measure against

Standards, cited against each finding

- Your own targets and customer commitments, first
- SOC 2 trust services criteria
- ISO 27001 control areas
- NIST Cybersecurity Framework
- Your customers' security questionnaires

Failure scenarios, always walked through

- Total power or connectivity loss at one site
- Ransomware encrypting primary and backup together
- Silent backup corruption discovered late
- Vendor or SaaS outage
- Key-person loss for two weeks

Gap ranking: each finding carries exposure, likelihood, cost to fix, cost of not fixing, and effort to benefit. Findings sort into four bands: fix now, fix this quarter, plan for the year, accept and document with a named owner.

What you hold at the end

Deliverables

- Current-state and target-state architecture diagrams
- RPO and RTO gap analysis, per system
- Single-point-of-failure map with blast radius
- Security gap register mapped to SOC 2, ISO 27001 or NIST CSF
- Prioritized recommendations with cost and benefit
- 360-degree cost-of-ownership view, current and recommended
- One-page executive summary

Terms

- Single fixed fee agreed before work starts
- Half at commencement, half on delivery
- Scope changes re-quoted, never absorbed quietly
- I sign your NDA; findings belong to you
- No vendor fees or commissions; any conflict disclosed

prasad@aggicorp.com | linkedin.com/in/drgolla | aggicorp.com