Cloud and SaaS review

Test shared responsibility against actual settings, data paths and recovery evidence.

Printable workpaper. The detailed guide and all scenario branches are in the Markdown file.

IaaS, PaaS and SaaS; responsibilities vary by service. All example data is fictional.

Process and expected evidence

1. Allocate responsibility

Service-specific responsibility matrix

2. Inspect effective settings

Resource scope and effective configuration

3. Test logging and recovery

Test-event trail and restore result

4. Monitor drift

Drift action and scoped retest

Work record

Scope / date:
Business / technical owner:
Decision and rationale:
Evidence reference / retest:

Example and closure

Fictional example; not evidence of actual work.

Resource: Example project

Owner: Cloud service owner

Expected control: No anonymous sharing

Effective setting: Legacy-link exception

Test: Synthetic guest test

Action: Remove old link and verify

Closure checklist

[ ] Responsibilities explicit.

[ ] Exceptions linked to inventory.

[ ] Logging and recovery tested.

[ ] Drift monitoring has an owner.

Official sources

Microsoft — Protect identities and secrets

https://learn.microsoft.com/en-us/entra/fundamentals/zero-trust-protect-identities

NIST Cybersecurity Framework 2.0

https://csrc.nist.gov/pubs/cswp/29/the-nist-cybersecurity-framework-csf-20/final