Professional Cloud Backup & Disaster Recovery Readiness Audit Checklist

Business Continuity Self-Assessment for Cloud-Dependent Organisations

Score each item:

- **Yes = 2 points**
- **Partially = 1 point**
- **No = 0 points**

Cloud Visibility & Asset Mapping

☐ We maintain a documented inventory of all critical cloud workloads and SaaS systems.
☐ Cloud assets are classified by business recovery priority.
☐ Irreplaceable data sets have been specifically identified.

Backup Architecture

☐ We use more than one recovery layer for mission-critical cloud systems.
☐ Independent backups exist beyond native provider retention alone.
☐ Immutable or deletion-protected storage is enabled where appropriate.

SaaS Continuity

☐ Microsoft 365/Google Workspace or equivalent SaaS platforms have dedicated backup coverage.
☐ CRM/accounting/HR SaaS systems have export or independent recovery planning.
☐ SaaS retention assumptions have been formally reviewed.

Administrative Protection

☐ Backup administration uses separate privileged accounts from production administration.
☐ MFA protects cloud administrative and backup control pathways.
☐ Repository deletion rights are restricted.

RTO / RPO Governance

☐ Recovery Time Objectives are defined for major cloud systems.
☐ Recovery Point Objectives are defined for critical data classes.
☐ Leadership understands acceptable downtime and acceptable data loss.

Outage Resilience

☐ Multi-region or alternate continuity options have been evaluated for critical workloads.
☐ Hybrid/off-platform copies exist for high-value systems.
☐ Vendor concentration risk has been reviewed.

Recovery Testing

☐ File-level restore tests are performed regularly.
☐ SaaS object/mailbox restoration has been tested.
☐ VM/application restoration has been validated.
☐ Recovery timing is measured and documented.

Program Governance

☐ Backup scope is reviewed on a scheduled basis.
☐ DR documentation includes ownership and escalation paths.
☐ Major cloud changes trigger continuity impact review.

SCORING RESULTS

38–46 Points — STRONG MATURITY

Your organization demonstrates strong cloud continuity planning and above-average disaster recovery resilience.

20–37 Points — MODERATE EXPOSURE

Important backup measures exist, but continuity gaps may still create prolonged operational disruption during major incidents.

0–19 Points — HIGH VULNERABILITY

Your cloud environment likely depends too heavily on assumptions and may experience severe recovery difficulty during outage, ransomware, or administrative failure.