Cloud Security Readiness Audit Checklist

Score each item:

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

Identity & Access

☐ 1. All cloud admin accounts use multi-factor authentication.
☐ 2. Shared administrator credentials are prohibited.
☐ 3. User permissions are assigned by role, not convenience.
☐ 4. Former employees/vendors are removed promptly from all cloud platforms.
☐ 5. API keys and service credentials are rotated on a schedule.

Configuration & Hardening

☐ 6. Public storage exposure is formally reviewed.
☐ 7. Firewall/security group rules are audited regularly.
☐ 8. Temporary test resources are removed after use.
☐ 9. Encryption is verified for stored and transferred sensitive data.
☐ 10. Default deployment settings are hardened before production use.

Monitoring & Visibility

☐ 11. Administrative actions are comprehensively logged.
☐ 12. Suspicious login behaviour generates alerts.
☐ 13. Critical cloud logs are centrally retained.
☐ 14. Storage access anomalies are monitored.
☐ 15. Cloud alerts are reviewed by assigned personnel.

Backup & Recovery

☐ 16. Backups exist for critical cloud workloads.
☐ 17. Backup restoration is tested periodically.
☐ 18. Backup repositories are protected from live-account compromise.

Governance & Documentation

☐ 19. The organisation maintains a current cloud asset inventory.
☐ 20. Named personnel own cloud security governance tasks.
☐ 21. Major cloud changes are documented.
☐ 22. Third-party SaaS integrations are reviewed for security exposure.
☐ 23. Cloud incident response procedures are documented.
☐ 24. Leadership receives periodic cloud security status reporting.
☐ 25. Cloud platforms are reviewed under a recurring security audit schedule.

SCORING RESULTS

40–50 Points — Strong Maturity

Your organisation demonstrates disciplined cloud security ownership and above-average resilience.

22–39 Points — Moderate Exposure

Important protections exist, but fragmented oversight or inconsistent execution leaves avoidable gaps.

0–21 Points — High Vulnerability

Your cloud infrastructure may be operationally functional but remains materially exposed to preventable incidents, visibility failures, and continuity disruption.