Professional API & Saas Security Readiness Audit Checklist

Connected Cloud Application Governance Self-Assessment

Score each item:

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

Visibility & Inventory

☐ We maintain a documented inventory of all SaaS integrations and third-party app connections.
☐ API keys, OAuth grants, and tokens are inventoried as managed assets.
☐ Each integration has a documented owner and business purpose.

Authentication Governance

☐ OAuth app approvals are formally reviewed before authorization.
☐ API keys and service tokens are rotated on a defined schedule.
☐ Unused or stale credentials are revoked regularly.

Least Privilege Controls

☐ Third-party apps receive only minimum necessary permissions.
☐ Tenant-wide permissions are restricted where avoidable.
☐ Read-only access is used where full write access is unnecessary.

Vendor Security

☐ SaaS vendors undergo basic security due diligence before broad trust is granted.
☐ Existing vendors are periodically re-evaluated for continued necessity and risk.
☐ Vendor security contacts and breach notification procedures are documented.

Monitoring & Detection

☐ New app authorisations and permission changes are monitored.
☐ API usage anomalies are reviewed.
☐ Suspicious export or abnormal data movement can be detected.

Sync & Data Resilience

☐ Critical SaaS-to-SaaS write pathways are reviewed for propagated damage risk.
☐ Retention windows are sufficient to recover from delayed discovery incidents.
☐ Important integrations are segmented or restricted where possible.

Automation Governance

☐ No-code workflows and automation connectors are inventoried.
☐ Abandoned or consultant-built workflows are reviewed and removed when unnecessary.
☐ Automation permissions are periodically revalidated.

Incident Readiness

☐ SaaS/API incident response procedures include token revocation steps.
☐ Connected downstream systems are included in compromise investigation plans.
☐ Vendor escalation procedures are pre-documented.

SCORING RESULTS

38–46 Points — STRONG MATURITY

Your organisation demonstrates strong governance over connected cloud trust relationships and above-average SaaS security resilience.

20–37 Points — MODERATE EXPOSURE

Important controls exist, but integration sprawl and incomplete governance may still create hidden compromise pathways.

0–19 Points — HIGH VULNERABILITY

Your business likely operates with significant unseen SaaS trust exposure, stale credentials, and poorly governed application permissions.