AUSTRALIA-FIRST | GLOBAL DELIVERY | ABN 59 870 881 596

Security Assurance Readiness Checklist

Use this checklist before a cyber insurance renewal, customer security questionnaire, tender, board review, ISO27001 or ISO42001 readiness push, ASD Essential Eight uplift, or AI governance review.

This document is a preparation guide. It is not legal advice, certification advice, insurance underwriting advice, or a guarantee that an auditor, insurer, or customer will accept your controls.

The trust rule

Do not give anyone keys to the kingdom before trust exists. Before sharing credentials, tenant access, evidence exports, or production data, confirm authority, scope, least privilege, access expiry, and the evidence purpose.

Quick scoring

Score	Meaning
0	No evidence exists or owner is unknown.
1	Control exists informally, but evidence is weak or stale.
2	Control exists and has usable evidence, but gaps remain.
3	Control is owned, current, tested, and shareable with reviewers.

1. Authority and scope

Check	Evidence to collect	Why it matters
Authorized representative is named	Requester role, work email, approval record.	Prevents unauthorized testing or evidence sharing.
Business trigger is clear	Insurer, customer, tender, board, audit, ISO, Essential Eight, or AI review request.	Controls effort around a real commercial outcome.
Rules of Engagement exist for testing	Signed scope, assets, dates, contacts, exclusions.	Active testing without scope creates legal and operational risk.
Access expiry is recorded	Access request, owner, approval, expiry, revocation evidence.	Reviewers expect least privilege and accountability.

2. Identity, access, and MFA

Check	Evidence to collect	Why it matters
MFA covers critical accounts	Screenshots or policy export for email, admin, finance, cloud, VPN.	Insurers and customers treat MFA as a baseline.
Admin accounts are separate	Admin role list, named accounts, break-glass process.	Reduces blast radius from everyday account compromise.
Joiner mover leaver process exists	Onboarding/offboarding checklist and recent access removal evidence.	Departed users are a common unmanaged risk.
Access reviews are periodic	Review calendar, last review output, owner sign-off.	Shows access decisions are maintained, not one-off.

3. Backup, recovery, and resilience

Check	Evidence to collect	Why it matters
Critical data is backed up	Backup policy, job status, protected system list.	Ransomware readiness starts with recoverability.
Restores are tested	Restore test date, result, issues, owner.	Untested backups are not evidence of recovery.
Backups are protected	Offline, immutable, or separate-admin evidence.	Attackers often target backups first.
Incident contacts are known	Escalation list and after-hours contact method.	Shortens confusion during the first hour.

4. Email, DNS, and customer trust

Check	Evidence to collect	Why it matters
SPF, DKIM, and DMARC are configured	DNS records and DMARC policy evidence.	Supports brand trust and reduces spoofing risk.
Payment-change process exists	Verification script and approval record.	Business email compromise usually turns into invoice fraud.
Security headers are reviewed	Header scan or Cloudflare/export evidence.	Shows basic web hardening for customer-facing systems.
Privacy notice matches actual data use	Current privacy page and data-flow notes.	Customers notice inconsistent privacy claims.

5. Endpoint, patching, and logging

Check	Evidence to collect	Why it matters
Device inventory exists	Endpoint list with owner, OS, protection status.	You cannot secure devices you cannot name.
Patch cadence is defined	Patch policy and recent compliance report.	Patching is a core Essential Eight and insurer expectation.
Endpoint protection is deployed	Coverage report and alert review evidence.	Antivirus alone rarely satisfies serious assurance reviews.
Security logs are collected	Log sources, retention, review process.	Evidence and investigation both depend on logs.

6. Vendor and SaaS risk

Check	Evidence to collect	Why it matters
Critical vendors are listed	Vendor register and data sensitivity notes.	Your risk includes supplier access and data handling.
Vendor security is reviewed	Questionnaire, SOC report, ISO certificate, or risk note.	Customers increasingly ask about third-party dependencies.
Contracts address security	Security clauses, breach notice, data location, support contacts.	Commercial terms matter during incidents.
OAuth and integrations are reviewed	Connected app export and owner review.	Shadow integrations can bypass normal access controls.

7. AI governance

Check	Evidence to collect	Why it matters
AI register exists	Tool, owner, use case, data type, approval state.	You cannot govern AI use you cannot see.
AI acceptable-use policy exists	Policy and staff acknowledgement evidence.	Sets boundaries for customer, health, finance, and confidential data.
AI suppliers are assessed	Vendor review and data-retention notes.	AI tools often create new supplier and privacy risk.
AI incidents are covered	Incident response playbook with AI data leakage scenario.	AI governance is only credible if incidents are planned.

8. Evidence pack readiness

Check	Evidence to collect	Why it matters
Evidence is mapped to the request	Control-to-evidence index.	Reviewers need a clear path, not a folder dump.
Evidence is redacted	Redaction checklist and clean copies.	Never leak secrets while proving security.
Executive summary is current	One-page status, blockers, decisions, owner.	Boards and customers need a decision-ready view.
Next 90 days are prioritized	Risk-ranked roadmap with owner and due date.	Assurance work should create action, not just a score.

Reviewer-specific prompts

Reviewer	Readiness question
Cyber insurance	Can we prove MFA, backups, patching, endpoint protection, email controls, incident response, vendor risk, and logging?
Customer questionnaire	Can we answer with evidence instead of promises?
Tender	Can we show ownership, policy, implementation, and review cadence?
Board	Can we explain risk, cost, and next decisions in business language?
ISO27001	Can we show an ISMS direction: scope, risk, controls, evidence, improvement?
ISO42001	Can we show AI governance: inventory, accountability, risk, suppliers, monitoring, and human oversight?
ASD Essential Eight	Can we show maturity against the mitigation strategies relevant to our environment?

Need help turning this into evidence?

Start qualified triage at https://consult.lil.business/. We will confirm authority and scope before asking for sensitive access.

lilMONSTER | lil.business | shoutout@lil.business | ABN 59 870 881 596