FREE SELF-ASSESSMENT · QUANTUM AUDIT ENGINE

The Audit Readiness Baseline

A 20-point, framework-neutral self-assessment across five control areas — score yourself before you pay for an audit, and find the area that will actually decide your result.

How to use this baseline

Score each of the 20 controls below: **0** = not in place, **1** = partially in place or undocumented, **2** = in place, documented, and someone owns it. Subtotal each area, then read your verdict band. The framework is deliberately neutral — the same fundamentals underlie SOC 2, ISO 27001, and the HIPAA Security Rule, so this baseline works whichever audit you are heading toward.

Area 1 — Governance & ownership (max 8)

1. A named owner exists for security/compliance with real authority (not “everyone’s job”).
2. Written policies exist for security, acceptable use, and data handling — reviewed within the last 12 months.
3. A risk register exists: top risks written down, rated, and revisited on a schedule.
4. Management reviews compliance status at a set cadence (quarterly or better), with minutes.

Area 2 — Access control (max 8)

1. Every system uses unique accounts — no shared logins anywhere that matters.
2. MFA is enforced on email, VPN/remote access, and every admin console.
3. Access follows least privilege, and there is a written joiner/mover/leaver process.
4. Access reviews happen on a schedule: someone re-certifies who can touch what, and departures are deprovisioned within a defined SLA.

Area 3 — Asset & data management (max 8)

1. An asset inventory exists (devices, servers, SaaS apps) and is kept current.
2. Data is classified — you know where sensitive data lives and who touches it.
3. Laptops and mobile devices are encrypted and centrally managed.
4. Vendors with access to your data are listed, risk-rated, and reviewed.

Area 4 — Operations security (max 8)

1. Patching runs on a defined cycle with visibility into what is missing.
2. Endpoint protection/EDR is deployed on all endpoints and monitored.
3. Logs from critical systems are collected centrally and retained; someone would notice anomalous activity.
4. Backups run automatically, are tested by restore at least annually, and at least one copy is offline/immutable.

Area 5 — Resilience & evidence (max 8)

1. A written incident response plan exists and has been exercised (tabletop counts).
2. Security awareness training is delivered at least annually and tracked to completion.
3. Changes to production systems follow a documented change process.
4. Evidence of all the above is collected as you go — screenshots, exports, tickets — not reconstructed at audit time.

Read your score

Total (max 40)	Band	What it means
33–40	Audit-ready	Gaps are cosmetic. Book the audit; spend effort on evidence packaging.
24–32	Near-ready	1–2 areas need real work. A focused 60-day push closes it.
14–23	Foundational gaps	Do not book an audit yet — remediate the lowest-scoring area first.
0–13	Starting point	Build governance and access control before anything else; the rest depends on them.

The constraint rule: your lowest-scoring AREA is your real readiness, whatever the total says. Auditors probe systematically — one hollow area produces findings across the whole report. Fix the floor, not the average.

Your 30-day fix cycle

1. Week 1: rescore with your team in the room — disagreement on a score IS a finding.
2. Week 2: pick the lowest area; write the missing policy or process (short and real beats long and ignored).
3. Week 3: implement the top two technical gaps (MFA and backup-restore tests are the usual quick wins).
4. Week 4: start the evidence habit — one folder per area, dated artifacts as things happen.

What each low-scoring area costs you

Weak area	Typical audit outcome	Typical business outcome
Governance	Scope disputes; findings on policy currency	Decisions stall; compliance lives in one person’s memory
Access control	High-severity findings; sampling expands	Departed users retain access; breach blast radius grows
Assets & data	“Unknown systems” findings	Shadow SaaS holds sensitive data unmanaged
Operations	Evidence requests you cannot fill	Unpatched estate; backups that restore nothing
Resilience	IR plan marked aspirational	Incidents improvised under pressure

Scoring honestly: three traps

- **The aspiration trap:** scoring what you intend to do next quarter. Score only what an auditor could verify today.

- **The hero trap:** “Alex handles that” is a 1, not a 2 — a control living in one person’s head is undocumented by definition.
- **The tool trap:** owning a product is not operating a control. EDR installed-but-unwatched scores 1.

A worked example

A 40-person SaaS company scores 31/40: Governance 7, Access 7, Assets 6, Operations 7, Resilience 4. The total says “near-ready,” but the constraint rule says Resilience is the true state: no exercised IR plan, untracked training. Their 60-day plan: run one tabletop (week 2), move training to a tracked platform (week 3), write the change-management one-pager (week 4), rescore. They book the audit only after Resilience clears 6 — and pass with two minor findings. The team that ignores the floor and books at “31” typically eats a qualified report instead.

What auditors actually sample

- Three recent joiners: was access granted per the written process?
- Three recent leavers: dated proof access was removed.
- One restore: show the test, not the backup job log.
- One incident — or the dated “none occurred this period” statement.
- Policy review dates checked against the calendar.