



The IT Readiness Checklist

25 practical checks across security, infrastructure, software and process — for teams who want to know where they actually stand.

Security

- ☐ **Multi-factor authentication** is enabled on every account with access to production systems or customer data.
- ☐ **Password reuse** across business tools has been checked — no shared logins for critical systems.
- ☐ You know **who has admin access** to every system, and it's been reviewed in the last 6 months.
- ☐ Customer data is **encrypted at rest and in transit** everywhere it's stored.
- ☐ You have a written, if brief, **incident response plan** — who does what if something goes wrong.

Backups & Continuity

- ☐ Backups run **automatically**, not manually, and someone actually checks they complete.
- ☐ A backup has been **test-restored** in the last 12 months — not just taken, but proven to work.
- ☐ Backups are stored **somewhere separate** from the primary system (different provider or region).
- ☐ You know your **recovery time** if a core system went down today — roughly, in hours.

Vendor & Software Audit

Infrastructure & Scale

- ☐ You know what happens to performance if **traffic doubled** tomorrow — tested, not assumed.
- ☐ Deployments happen without **manual, error-prone steps** — there's a repeatable process.
- ☐ **Monitoring and alerting** exist for the systems that would hurt most if they went down.
- ☐ You're not dependent on **one person's knowledge** to keep critical systems running.
- ☐ Cloud costs are **reviewed regularly**, not just paid automatically each month.

Software & Process

- ☐ New features go through **some form of testing** before reaching real users.
- ☐ There's a way to **roll back** a bad release quickly, without a multi-hour scramble.
- ☐ **Technical debt** is tracked somewhere, not just known anecdotally.
- ☐ Onboarding a new engineer takes **days, not weeks**, thanks to reasonable documentation.

Team & Support

- ☐ Customers have a **clear channel** for support, with a real expected response time.
- ☐ Support and bug patterns are **reviewed periodically** to catch recurring issues.

- ☐ You have a **current list** of every paid software tool and who owns each relationship.
- ☐ **Unused subscriptions** have been cancelled in the last quarter.
- ☐ Every vendor with access to customer data has been asked about **their** security practices.
- ☐ There's a named person (even part-time) **accountable** for IT and security decisions.
- ☐ Your team knows **who to call** when something breaks outside business hours.