IT Audit Readiness Checklist

For business owners and leadership teams at organizations with about 10 to 250 employees. What a real IT audit reviews, and what you can document today.

How to use this checklist

A lender, an investor, a cyber insurance carrier, a client security questionnaire, or a buyer will eventually ask how your technology is managed. This checklist covers what a real IT audit reviews. Work through each section and check off only what you can prove with current documentation, not what you assume is in place. Every unchecked box is a question worth answering before someone else asks it.

> **What we usually find.** In the environments we review, the same gaps come up again and again: a few accounts missing MFA, some devices missing security protection, patching missing on a few devices, former employees with active accounts, backups that have never been restored, devices on the network nobody can identify, and no history to show what happened last week because nothing was being logged. None of these are exotic. They are what happens when nobody is assigned to check.

1. Inventory

You cannot manage or protect what you do not know is there.

- [ ] We have a current list of every laptop, desktop, server, phone, and network device, including who uses it and where it is.
- [ ] We have a current list of the software and cloud applications the business uses, including free tools staff signed up for on their own.
- [ ] The inventory is updated when devices are added, replaced, or retired, not rebuilt once a year.
- [ ] We can account for every device on the network. Nothing unknown is connected.

2. Accounts and access

- [ ] Every person has their own account. No shared logins are used for business systems.
- [ ] Accounts are disabled the same day someone leaves, and we can show when it happened.
- [ ] Access matches the job. People can reach what they need and nothing more.
- [ ] Admin rights are limited to the few people who need them, using separate admin accounts.
- [ ] We review who has access to what at least twice a year.

3. Multi-factor authentication

- [ ] MFA is enforced on every user account, not just most of them.
- [ ] MFA is enforced on admin, service, and shared accounts, including ones set up before MFA was required.
- [ ] Remote access and vendor access require MFA.
- [ ] We have a way to check which accounts do not have MFA, and nobody is on that list.

4. Backup and recovery

- [ ] Backups run on a schedule and we are alerted when one fails.
- [ ] We have restored from backup in the last six months to confirm it actually works.
- [ ] Backups are encrypted, and at least one copy is protected from being changed or deleted.
- [ ] Microsoft 365 or Google Workspace data is backed up separately, not just left in the service.
- [ ] We know how long a restore would take and how much data we could lose, and leadership has agreed that is acceptable.

5. Security baseline

- [ ] Every device has endpoint protection installed, current, and reporting in.
- [ ] Operating systems and applications are patched on a defined schedule, and we can see which devices are behind.
- [ ] Devices that are rarely rebooted or often off the network are checked so they do not fall behind on patches.
- [ ] Email security is in place, including SPF, DKIM, and DMARC, and external email is tagged.
- [ ] Security awareness training happens more than once a year, and completion is tracked.
- [ ] Security alerts are monitored and someone is responsible for responding to them.

6. Monitoring and history

Having monitoring tools is not the same as monitoring. Each tool reports what it was built to report, and the gaps between them are where problems hide. What matters is whether every layer is watched, whether the history is kept, and whether someone looks.

- [ ] Network devices (firewalls, switches, and access points) are monitored, not just installed.
- [ ] Every endpoint reports its health, security status, and patch level on an ongoing basis.
- [ ] Microsoft 365 sign-ins are monitored, including risky users and conditional access results.
- [ ] Your domain's public DNS records for email (SPF, DKIM, and DMARC) are monitored, so a change or misconfiguration gets caught.
- [ ] DNS activity on devices is monitored for connections to known malicious or suspicious sites.
- [ ] Backup results are tracked, and a failed backup triggers an alert someone acts on.
- [ ] Wi-Fi health is monitored, so slow or dropped connections can be traced to a cause.
- [ ] Internet speed and connection quality are monitored at each location, so a slowdown is caught before staff have to report it.
- [ ] The data from all of the above is kept long enough to look back, at least 90 days.
- [ ] If a problem started three weeks ago, we could see when it began and what changed.
- [ ] Someone reviews the data and acts on alerts. It is not just collected.

7. Microsoft 365

- [ ] Our licensing supports the security features we rely on, such as conditional access.
- [ ] External sharing settings have been reviewed and match how the business works.
- [ ] Mailbox forwarding to outside addresses is blocked or monitored.
- [ ] Audit logging is turned on and retained.

8. AI tools

Most businesses have more AI running than leadership knows about: standalone chat tools, AI features switched on inside software you already pay for, and browser extensions. That is shadow AI, and it is the fastest-growing kind of shadow IT.

- [ ] We know which AI tools staff are using for work, including AI features built into software we already pay for and browser extensions.
- [ ] We have a written AI acceptable use policy that names approved tools and the data that must never go into them, and staff have been trained on it.
- [ ] Staff use approved AI tools on business accounts, not personal ones.
- [ ] Client information, personal data, financial records, and credentials never go into unapproved AI tools.
- [ ] Before adopting an AI tool, we check how it handles our data, including whether the vendor retains it or trains on it.
- [ ] One named person approves new AI tools, and there is a simple way for staff to request one.
- [ ] If we use Microsoft 365 Copilot, file sharing and permissions have been reviewed first, since Copilot can surface anything a user already has access to.
- [ ] A person reviews AI-generated content before it goes to a client, into a file, or into a decision.

9. Vendors and contracts

- [ ] We have a list of every IT vendor and service provider, what they support, and who to call.
- [ ] We know what each contract includes, what it excludes, and when it renews.
- [ ] Vendors with access to our systems use their own named accounts, with MFA, and their access is reviewed.
- [ ] We know who owns our domain, our Microsoft 365 tenant, and our admin credentials. It is the business, not a vendor or former employee.

10. Lifecycle

- [ ] We know the age and warranty status of our devices, servers, and network equipment.
- [ ] Nothing in use is past the point of receiving security updates, or it has a replacement date.
- [ ] Upcoming replacements and renewals are in next year's budget.

11. Policies and documentation

- [ ] We have written IT and security policies, and staff have seen them.
- [ ] Day-to-day practice matches what the policies say.
- [ ] We have a written incident response plan that names who does what.
- [ ] Our network, systems, and key procedures are documented well enough that someone new could take over.

12. Questions to ask your IT provider

- [ ] Can you show me which accounts do not have MFA today?
- [ ] Which devices are behind on patches or missing security protection right now?
- [ ] When did we last restore from backup, and how long did it take?
- [ ] What does your monthly or quarterly reporting actually show, and what does it leave out?
- [ ] Which of these do you monitor for us today: network devices, endpoints, Microsoft 365 sign-ins, email DNS records, backups, Wi-Fi, internet speed, and logs?
- [ ] If something started going wrong three weeks ago, could you show me when and what changed?
- [ ] Do you find out about slow internet or Wi-Fi before our staff call you, or after?
- [ ] Can you show us which AI tools are in use in our environment today?
- [ ] If you left tomorrow, what documentation would we have?

We don't guess. We look it up. 3rd Element monitors every layer of the environments we manage, from network devices and endpoints to Microsoft 365 sign-ins, email DNS records, backups, Wi-Fi health, and internet speed, and keeps 90 days of history across all of it. Many problems, like a slow internet connection, get caught before anyone has to report them. When something does go wrong, we can show you when it started and why. An IT Environment Review is free and takes about 30 minutes by video or phone. We ask a set list of questions about your environment, answer yours, and send you a written summary afterward. Schedule it at **3rdelementconsulting.com/schedule**.

This checklist is a readiness aid, not a formal audit or a compliance determination. Industry regulations such as HIPAA, the FTC Safeguards Rule, or CJIS may require additional controls and documentation. Current as of September 2026.