A practical guide for future planning, even if you are not ready to make changes today

Many businesses know that better IT management would be helpful, but the timing is not always right.

Budgets may be focused elsewhere. The current setup may be working well enough. Other priorities may feel more urgent.

That is completely reasonable.

This checklist is designed to help you think through IT readiness at your own pace. It is not meant to push immediate action. Instead, it can help you separate what can wait from what should stay on your radar.

1. What Good IT Management Typically Includes Today

Use this section to confirm whether the major parts of your IT environment are being actively managed.

- Someone is clearly responsible for managing IT decisions.
- Devices, users, software, and systems are documented.
- Security updates are applied consistently.
- Backups are monitored, not just assumed.
- User access is reviewed when employees join, change roles, or leave.
- Email security is in place to reduce phishing and account compromise.
- FAST support is available when employees need help (15 minutes or LESS).
- Technology planning is discussed before there is an emergency.

Why it matters:
Good IT management is not just fixing problems. It is making sure the everyday basics are handled consistently.

2. Areas That Usually Carry Real Risk

These items are worth paying attention to even when everything seems to be working.

- Former employees or vendors may still have access to systems.
- Backups have not been tested recently.
- Passwords are reused, shared, or stored informally.
- Multi-factor authentication is not enabled on key accounts.
- Devices are missing updates or running unsupported software.
- There is no clear process for responding to a security incident.
- Critical knowledge lives with one person and is not documented.
- No one is regularly reviewing security alerts, licenses, or system health.

Why it matters:
Real IT risk often exists quietly. It may not create obvious symptoms until something fails, someone leaves, or an account is compromised.

3. Areas That May Feel Risky but Can Often Wait

Not every IT improvement needs to happen immediately. Some items may be worth planning for later.

- Replacing equipment that is still supported and performing reliably.
- Changing software that employees are comfortable using.
- Redesigning systems that are stable and well-documented.
- Moving to new platforms without a clear business reason.
- Upgrading tools simply because newer options exist.
- Adding advanced security tools before the basics are covered.
- Making large IT changes during a busy operating season.

Why it matters:
Good IT planning does not mean changing everything. It means knowing what is worth addressing now, what can wait, and what should be reviewed later.

4. What Should Not Wait Too Long

These areas are often better handled before there is a visible problem.

- Confirm that backups are working and restorable.
- Remove access for former employees, contractors, and vendors.
- Enable multi-factor authentication on email, finance, and admin accounts.
- Replace unsupported computers, servers, or software.
- Document critical systems, passwords, vendors, and support contacts.
- Review who has administrator-level access.
- Make sure employees know how to report suspicious emails or IT issues.
- Create a basic plan for outages, cyber incidents, or lost devices.

Why it matters:
Some IT items are easy to postpone because they are not urgent today. But when they do become urgent, they are usually harder and more expensive to fix.

5. Questions to Help Prioritize Future IT Decisions

Use these questions when deciding whether an IT issue should be addressed now, planned for later, or simply monitored.

- Would this disrupt daily operations if it failed?
- Would this create a security or compliance concern?
- Would this be difficult to recover from quickly?
- Is this dependent on one person’s knowledge?
- Is the current setup still supported by the vendor?
- Would fixing this now be simpler than fixing it during an emergency?
- Is this issue affecting employee productivity?
- Is there a clear business reason to make a change?

Why it matters:
The goal is not to make every IT improvement at once. The goal is to make informed decisions based on business impact.

6. A Simple Planning Framework

Use the categories below to sort your IT priorities.

Address Soon

These items create meaningful risk or could interrupt the business.

- Security gaps involving email, passwords, or administrator access.
- Untested or unreliable backups.
- Unsupported systems or software.
- Former users who still have access.
- No clear support path for urgent issues.

Plan for Later

These items matter, but may not require immediate action.

- Device replacements.
- Software upgrades.
- Vendor reviews.
- Process improvements.
- Documentation updates.
- Long-term IT budgeting.

Monitor for Now

These items may be acceptable as long as they remain stable.

- Systems that are working and supported.
- Tools employees use effectively.
- Equipment that is reliable and under warranty.
- Processes that are informal but currently manageable.
- Future improvements without a clear deadline.