

Microsoft 365 Risk and Cost Checklist for Small Businesses

A practical worksheet for business owners who want clearer licensing, stronger access controls and fewer surprises before the next migration, audit or security incident.

Use this checklist to:

- Identify questions that deserve an answer
- Separate verified controls from assumptions
- Assign an owner and a next action
- Prepare for a focused Microsoft 365 review

Prepared by Pronto Tech | Local IT support across Virginia, Maryland and Washington, DC

How to use this worksheet

Work through the questions with the person who administers Microsoft 365. Mark **Verified** only when you can point to a current setting, report, owner or test result. Mark **Needs review** when the answer relies on memory, an old project or an assumption.

Status	Meaning
Verified	Current evidence supports the answer.
Needs review	The control, ownership or evidence is unclear.
Planned	A named owner and target date have been agreed.

1. Licensing and ownership

- ☐ Every active user has a license matched to their actual role.
- ☐ Unused accounts and licenses are reviewed on a regular schedule.
- ☐ The business owns and can access its Microsoft tenant, domain and subscriptions.
- ☐ Recurring Microsoft charges can be reconciled to users and services.

Watch for: Paying for capabilities nobody uses, or relying on an outside party as the only administrator.

2. Administrator access

- ☐ Administrative roles are limited to people who need them.
- ☐ Daily email accounts are separate from privileged administrator accounts.
- ☐ Strong multifactor authentication protects every administrator.
- ☐ Emergency access is documented and tested.

Watch for: Too many global administrators, shared admin accounts or an account that cannot be recovered.

Identity, email and information

Most Microsoft 365 incidents begin with an account, message or sharing decision. These checks help expose where daily convenience may have created avoidable risk.

3. Identity and email protection

- ☐ Multifactor authentication is enforced for all users, with exceptions documented.
- ☐ Legacy or basic authentication is blocked where possible.
- ☐ Suspicious sign-ins and risky account activity have an assigned response owner.
- ☐ Email impersonation, malicious links and attachments are addressed by configured controls and a response process.

Watch for: MFA that is merely available instead of enforced, or alerts that nobody regularly reviews.

4. Teams, SharePoint and OneDrive sharing

- ☐ External guests are reviewed and removed when no longer needed.
- ☐ Anonymous sharing links are restricted or expire.
- ☐ Sensitive libraries and sites have named business owners.
- ☐ Employee departure procedures cover files, groups, Teams and shared mailboxes.

Watch for: Old guest accounts, links with no expiration and information stored under one employee's personal ownership.

5. Backup and recovery

☐ Leadership has defined which Microsoft 365 data must be recoverable and how quickly.

☐ Retention settings and independent backup are understood as different capabilities.

☐ Backup coverage includes the workloads the business expects.

☐ A representative file, mailbox or site restore has been tested and documented.

Watch for: Assuming Microsoft retention automatically provides every recovery capability the business expects.

Readiness and next actions

6. Change, migration and AI readiness

☐ Identity, permissions and data locations are understood before a migration or acquisition.

☐ Critical integrations, shared mailboxes and business applications have documented owners.

☐ Copilot or other AI tools will not be enabled before permissions and acceptable-use expectations are reviewed.

☐ The business has a clear escalation path for Microsoft, licensing and application vendors.

Watch for:

Starting a project before ownership, permissions and information locations are understood.

Prioritized action plan

Choose no more than five actions. A short list with owners and dates is more useful than a long list nobody can finish.

Priorit y	Finding or question	Owner	Target date
1			
2			
3			
4			
5			

WANT A SECOND SET OF EYES?

Request a focused Microsoft 365 review.

Pronto Tech reviews the agreed scope, distinguishes verified findings from missing evidence and provides a prioritized findings summary.

pronto-tech.com/managed-ms-365/