Microsoft Cloud Readiness Checklist

A practical planning guide for Microsoft 365, Azure, security, licensing, and managed operations

Guava Systems
Microsoft Cloud Solution Provider

How to use this checklist

Cloud readiness is not a single technical score. It is the ability to make informed Microsoft technology decisions without introducing unnecessary cost, security gaps, operational friction, or adoption risk.

Use this checklist before a Microsoft 365 rollout, Azure migration, security review, Copilot pilot, licensing renewal, or managed-services conversation. Mark each item as **Ready**, **Needs work**, or **Not applicable**. Any item marked Needs work becomes an input to your technology roadmap.

1. Business outcomes and ownership

- [ ] We can state the business outcome of the project in one sentence.
- [ ] An executive sponsor owns the business result, not only the technology launch.
- [ ] A technical owner is accountable for architecture and delivery decisions.
- [ ] Department leaders have identified the workflows or services that must improve.
- [ ] Success measures have a baseline and a target.
- [ ] The organization has agreed on priorities when cost, speed, and risk conflict.
- [ ] Project decisions and responsibilities are documented.

Questions to discuss: What must become faster, safer, simpler, or less expensive? Which result would make the project worthwhile twelve months from now?

2. Microsoft licensing and commercial governance

- [ ] Every active user has an identified role and licence requirement.
- [ ] Inactive, duplicate, shared, and departed-user accounts are reviewed regularly.

- [ ] Premium plans and add-ons are assigned only where the included capabilities are needed.
- [ ] Licence changes are connected to onboarding, role changes, and offboarding.
- [ ] Renewal dates, billing owners, and approval thresholds are documented.
- [ ] The business can explain significant month-to-month cost changes.
- [ ] Current licensing supports the security and compliance controls the organization expects.
- [ ] A quarterly licence-utilization review is scheduled.

Warning signs: Employees receive the same plan regardless of role; add-ons are purchased without adoption measures; departed users retain licences; finance cannot reconcile licences to headcount.

3. Identity and access

- [ ] Multifactor authentication is required for users and administrators.
- [ ] Administrative accounts are separate from everyday user accounts.
- [ ] Global administrator privileges are limited and reviewed.
- [ ] Conditional Access or an appropriate baseline policy protects sign-ins.
- [ ] Legacy authentication is disabled where possible.
- [ ] Guest users and external collaborators have an owner and review date.
- [ ] Emergency access accounts are documented and monitored.
- [ ] Joiner, mover, and leaver procedures are defined.
- [ ] Risky sign-ins and privilege changes generate actionable alerts.

Questions to discuss: Who can grant access? How quickly is access removed when a person leaves? Which sign-ins would the organization consider suspicious?

4. Devices, applications, and data

- [ ] Corporate and personal-device access requirements are documented.
- [ ] Supported devices are enrolled in an appropriate management platform.
- [ ] Encryption, screen lock, update, and endpoint-protection policies are enforced.
- [ ] Business-critical applications and their owners are inventoried.

- [ ] Data locations, sensitivity, and sharing requirements are understood.
- [ ] Teams, SharePoint, and OneDrive ownership rules are defined.
- [ ] External sharing settings match the organization’s risk tolerance.
- [ ] Data retention and deletion requirements are documented.
- [ ] Recovery requirements are defined independently from service availability.

Warning signs: Files are stored across personal drives and unmanaged Teams; no one owns inactive workspaces; sensitive data is discoverable more broadly than intended.

5. Azure migration readiness

- [ ] Workloads, dependencies, data flows, and current costs are inventoried.
- [ ] Each workload has a business owner and technical owner.
- [ ] The migration approach is selected per workload rather than for the estate as a whole.
- [ ] Identity, networking, governance, security, and monitoring requirements are designed before migration.
- [ ] Subscription, resource-group, naming, tagging, and access standards are documented.
- [ ] Recovery objectives and backup responsibilities are defined.
- [ ] Migration waves include testing, rollback, and acceptance criteria.
- [ ] Cost budgets and alerts are configured before production consumption grows.
- [ ] Post-migration optimization is included in the plan.

Questions to discuss: What should move first and why? Which dependencies could stop a cutover? How will the organization know that the migrated workload performs better?

6. Cybersecurity and resilience

- [ ] The organization has a prioritized Microsoft security baseline.
- [ ] Email protection settings are reviewed and tested.
- [ ] Endpoint alerts have an owner and response procedure.
- [ ] Security incidents have severity levels, escalation contacts, and communication steps.
- [ ] Backup coverage includes the data and scenarios the business expects.
- [ ] Restore procedures are tested on a scheduled basis.

- [ ] Logs are retained long enough to support investigation requirements.
- [ ] Vendors and partners have defined access boundaries.
- [ ] Security improvements are tracked as operational work, not only as an annual project.

Warning signs: The organization assumes cloud availability is the same as backup; alerts are enabled but no one reviews them; administrative access is shared; incident contacts are outdated.

7. Teams, SharePoint, and collaboration governance

- [ ] Workspace naming and ownership standards are defined.
- [ ] New Teams and sites follow an approved creation process.
- [ ] Owners review membership and guest access.
- [ ] Inactive workspaces have an archive or deletion lifecycle.
- [ ] Employees know where different types of files should be stored.
- [ ] Sensitive information has appropriate access and sharing controls.
- [ ] Search, metadata, and navigation support common employee tasks.
- [ ] Governance requirements do not create unnecessary barriers to collaboration.

Questions to discuss: Can employees find the current version of a document? Who owns a Team after its project ends? What should happen to external access after a contract closes?

8. Copilot and AI readiness

- [ ] The organization has selected specific, measurable Copilot use cases.
- [ ] SharePoint, Teams, OneDrive, and mailbox permissions are reviewed before the pilot.
- [ ] Sensitive and overshared content has an improvement plan.
- [ ] Acceptable-use and human-review guidance is documented.
- [ ] Pilot users represent real workflows and departments.
- [ ] Training includes prompt skills, verification, and responsible use.
- [ ] Adoption and business-value measures are defined.
- [ ] Licence expansion depends on pilot evidence rather than enthusiasm alone.

Warning signs: The pilot begins before permissions are understood; licences are assigned without a use-case plan; success is measured only by activation or login counts.

9. Support and managed operations

- [ ] Users know where to request support and what information to provide.
- [ ] Incidents, requests, changes, and recurring problems are tracked consistently.
- [ ] Onboarding and offboarding tasks have owners and service targets.
- [ ] Licence, identity, device, and security reviews occur on a defined schedule.
- [ ] Monitoring alerts route to a person or team that can act.
- [ ] Escalation paths to vendors and Microsoft are documented.
- [ ] The internal team and external partner have clear responsibility boundaries.
- [ ] A quarterly technology roadmap review is scheduled.

Questions to discuss: Which tasks consume internal IT time without creating strategic value? Where would a partner improve continuity, expertise, or response time?

10. Your next-step scorecard

Area	Ready	Needs work	Owner	Target date
Business outcomes				
Licensing				
Identity and access				
Devices and data				
Azure migration				
Cybersecurity				
Collaboration governance				
Copilot readiness				
Support operations				

Choose no more than **three priority actions** for the next 30 days. Assign one accountable owner and a realistic completion date to each action.

Turn the checklist into a roadmap

Guava Systems helps organizations connect Microsoft licensing, cloud architecture, security, productivity, and ongoing support to measurable business priorities.

To discuss the findings from this checklist, visit **library.guava.pro/cloud-assessment/** and request a cloud assessment conversation.

Guava Systems
Technology that works for you.
Explore Guava’s Microsoft product catalogue