THE AZURE MANAGED CLOUD
BUYER'S GUIDE

How to evaluate managed Azure services — and the questions that separate real providers from resellers.

The Azure Managed Cloud Buyer's Guide

Microsoft Azure is easy to buy. Accountability for how it runs is not. Anyone with a partner portal can resell you a subscription; far fewer firms will monitor it at 2 a.m., test your restores, and answer for the monthly bill.

Most "managed Azure" offers are resale plus a ticket queue. This guide gives you the inclusion checklist, the real cost drivers, the security baseline, and the twelve questions that separate a provider who runs Azure from one who merely bills for it.

1. Why Buying Managed Azure Is Hard

The platform itself isn't the risk — the gap between what a provider says and what they actually operate is. "Managed" has no standard definition, so two providers quoting similar monthly numbers can be selling completely different services: one is engineering your environment, the other is forwarding alerts.

The Rule:

Evaluate the service behind the word "managed," not the logo on the proposal. Everything in this guide exists to make that service visible before you sign.

2. What "Managed Azure" Must Include

A real managed Azure service covers all eight of these — not a subset. What good looks like:

- **24/7 monitoring and alerting** — issues found by the provider, not reported by your users
- **Patch and update management** — a defined cadence for VMs and services, not "as needed"
- **Monthly cost reviews and right-sizing** — someone accountable for the number on the invoice
- **Identity and access management** — Microsoft Entra ID configured, enforced, and reviewed
- **Backup and disaster recovery testing** — restores actually performed, not assumed
- **Security hardening and threat response** — a documented response path with names on it
- **Performance tuning and scaling** — workloads sized to demand, adjusted as demand changes
- **Architecture guidance and roadmap** — the environment improves over time instead of drifting

The Red Flag:

A proposal that lists Azure products instead of operational responsibilities.

3. The Five Things That Actually Drive Your Azure Bill

Azure spend isn't random — five levers control most of it. A competent provider works all five without being asked.

- **Compute sizing** — most VMs are provisioned larger than their workload needs. Right-sizing plus reserved instances on steady workloads is usually the single biggest saving.
- **Storage tiers** — data that hasn't been touched in months doesn't belong in the hot tier, and old snapshots multiply silently. Tiering policies keep storage honest.
- **Licensing** — Azure Hybrid Benefit lets you apply Windows Server and SQL licenses you already own. It is real money, and it is routinely left unused.
- **Networking and egress** — data leaving Azure costs money. Architecture decides what crosses billable boundaries; a bad design pays that toll forever.
- **Orphaned resources** — unattached disks, idle public IPs, and test environments that outlived their purpose. This "ghost" spend bills every month until someone hunts it down.

The Rule:

Cloud waste is invisible until someone measures it — ask who measures yours, and how often.

4. The Security Baseline — Six Things That Must Be True

Whatever else a provider promises, these six must be true of your environment. No exceptions, no "phase two."

- Multi-factor authentication enforced through Microsoft Entra ID — every account, no legacy exceptions
- Least-privilege role-based access — no standing global administrators
- A defined patching cadence for VMs, services, and dependencies
- Backups isolated from production credentials — and restore-tested on a schedule
- Centralized logging with alerting someone actually watches
- A written incident-response path with named people and response times

The Red Flag:

Default settings are not a security posture.

5. Twelve Questions to Ask Any Managed Azure Provider

Ask all twelve. The answers — and the hesitations — tell you who you're dealing with.

1. **Who owns the Azure subscription?** — It should be you. Provider-owned subscriptions are a lock-in mechanism.
2. **What's included in the monthly fee, and what bills separately?** — Surprises live in this gap.
3. **Who responds at 2 a.m., and how fast?** — "24/7 monitoring" means nothing without a response commitment.
4. **What is your patching cadence?** — A real answer has days and windows in it.
5. **How often do you test restores — not just run backups?** — An untested backup is a hope, not a plan.
6. **How do you handle identity — MFA, conditional access, least privilege?** — This is where most breaches start.
7. **What cost-optimization work happens monthly, and where is it reported?** — Optimization that isn't reported isn't happening.
8. **Can we talk directly to the engineers on our account?** — A named team beats an anonymous queue.
9. **What does onboarding look like, and when are you accountable?** — The handoff date should be in writing.
10. **Do we get the documentation of our own environment?** — Your environment, your documentation.
11. **What happens if we leave?** — A confident provider has an offboarding process; a captor doesn't.
12. **What Microsoft partner status and certifications do you hold?** — Verify, don't assume.

6. Red Flags

Any one of these is a reason to slow down. Two or more is a reason to walk away.

- Pricing they won't put in writing
- A provider-owned subscription "for your convenience"
- Backups that have never been restore-tested
- Ticket-queue-only access with no named engineers
- Long contracts required before any trust is earned

7. How QOS MSP Runs Azure

We built our managed Azure service to pass this guide's own test. QOS MSP has engineered and maintained business infrastructure since 2007 — founder-led, security-first on Microsoft Entra ID, with a flat monthly fee and no long-term contract required. You own your Azure subscription and your documentation; we're accountable for how the environment performs, what it costs, and how fast it recovers.

The Final Word

The cheapest proposal and the most expensive one often describe the same Azure products. The difference is who carries the operational responsibility — and whether you can verify it before you sign.

Next Step:

Put your current provider — or your shortlist — against the twelve questions in section 5. If you'd like a second opinion, QOS MSP will assess your Azure environment at no cost: call +1 (877) 800-7672 or visit www.qosmsp.com.