Managed IT Buyer Guide (Vendor-neutral)

How to compare MSPs in NZ: what to ask, what good looks like, and how to switch safely.

Last updated: 2026-02-21 · **Scope:** Taranaki focus, NZ-wide applicable

Purpose: Evaluate any Managed IT provider fairly. This guide is vendor-neutral and focuses on practical diligence.

How to use this guide:

- Highlight the questions that matter most to your business.
- Ask the same questions to each provider and compare answers side-by-side.
- Use the scorecard at the end to summarise your decision.

18 questions to ask any Managed IT provider

Each question includes why it matters and what a strong answer sounds like.

Commercial clarity & scope

1. What exactly is included vs excluded (in writing)?

Why it matters: So you can compare providers fairly and avoid surprise invoices.

What a good answer sounds like: Clear inclusions/exclusions, examples of what becomes a project, and how changes are approved (SoW/WO with acceptance criteria).

2. What counts as a material change (project) vs day-to-day managed work?

Why it matters: So monthly spend stays predictable and both sides know where the line is.

What a good answer sounds like: Day-to-day = incidents/requests + operational hygiene. Material change = migrations, redesigns, major upgrades, new builds; quoted separately.

3. How does pricing work and how will it scale as we grow?

Why it matters: So you can budget and avoid pricing that only works at one size.

What a good answer sounds like: A transparent model (per-seat/per-site or equivalent), clear thresholds, and a predictable approach when you exceed the included footprint.

Support model & SLAs

4. How do you define response vs resolution?

Why it matters: Because we replied is not the same as you are back up and running.

What a good answer sounds like: Response = triage begins. Resolution = service restored or safe workaround + plan. Separate targets per priority.

5. How do you classify priorities (P1-P4) tied to business impact?

Why it matters: So severity is consistent and you do not fight over urgency.

What a good answer sounds like: Priority definitions tied to impact (outage, degraded service, single user, request), with examples and escalation paths.

6. What are your coverage hours and after-hours pathways?

Why it matters: So you know what happens at 2am or during a weekend outage.

What a good answer sounds like: Business-hours coverage plus defined after-hours response for critical incidents (P1), with clear billing rules if applicable.

Security & resilience

7. How do you handle identity security (MFA, Conditional Access, admin hygiene)?

Why it matters: Identity is the top attack path for most SMB incidents.

What a good answer sounds like: Baseline policies for users/admins, break-glass accounts, regular access reviews, and exceptions tracked with owners and expiry.

8. How do you verify backups (restore testing) and show evidence?

Why it matters: Backups that are never tested are wishful thinking.

What a good answer sounds like: Regular restore tests (at least quarterly), recorded outcomes, and clear RPO/RTO expectations for critical systems.

9. What is your approach to endpoint protection and patching (including rollback)?

Why it matters: Most ransomware and breaches exploit unpatched or unmanaged endpoints.

What a good answer sounds like: Patch cadence, rings, exception handling, rollback awareness, and EDR/AV operations if licensed.

Operations & tooling

10. What monitoring is in place and who watches it?

Why it matters: Monitoring without triage is just noise.

What a good answer sounds like: Defined monitoring stack, alert routing, ownership, and measurable outcomes (reduced repeat incidents).

11. How do you manage documentation (runbooks, diagrams, access register) and keep it current?

Why it matters: Documentation makes support predictable and handover safe.

What a good answer sounds like: Minimum documentation set, updated on a schedule or when changes occur, and provided on exit.

12. How do you manage vendors/ISPs and escalation ownership?

Why it matters: So you do not spend your time chasing telcos and SaaS vendors.

What a good answer sounds like: Provider owns escalation, keeps you informed, documents outcomes, and tracks recurring vendor issues.

Onboarding & change governance

13. What does onboarding look like in the first 30 days and what are milestones?

Why it matters: Switching providers is risky unless there is a structured plan.

What a good answer sounds like: A 30-day baseline plan: access, identity hygiene, backup verification, endpoint baselines, monitoring, plus quick wins.

14. How do you handle risky changes (change control and rollback)?

Why it matters: Unplanned changes cause outages.

What a good answer sounds like: Change approval for high-risk work, maintenance windows, rollback steps, and post-change validation.

15. How do you reduce recurring issues over time?

Why it matters: Managed IT should improve, not just react.

What a good answer sounds like: Root-cause tracking, trend analysis, preventive actions, and a monthly/quarterly improvement cadence.

Exit safety & reporting

16. If we leave, what does offboarding look like and what do we keep?

Why it matters: So you are never held hostage by tooling or credentials.

What a good answer sounds like: Handover pack: access, configs, documentation, asset list, vendor portals, and a transition plan.

17. What reporting do we receive each month (and what decisions does it support)?

Why it matters: Visibility is how you trust the service and plan investment.

What a good answer sounds like: Monthly outcomes: SLA performance, incidents, risks, changes, backup status, and next actions.

18. Who owns incident communication during an outage or security event?

Why it matters: Clear comms reduces business chaos and speeds recovery.

What a good answer sounds like: Named incident manager, comms cadence, stakeholder updates, and a post-incident summary with actions.

Common red flags

- Unlimited everything with no written scope boundaries or examples.
- Backups in place but restore tests are rare or undocumented.
- No change control or rollback thinking for risky work.
- Single-person dependency and no defined coverage model.
- Bundled licensing presented in a way that makes it hard to compare or exit.

Switching providers safely (simple plan)

- Snapshot first: identity, backups, endpoints, network touchpoints, vendor portals.
- Access handover: admin accounts, MFA, break-glass, password vault, ownership clarity.
- Baseline stabilisation: identity hygiene, backup verification, patch cadence, monitoring.
- Improve later: bigger changes after stability (migrations, redesigns, major upgrades).

Scorecard

Category	What to score	Score (1–5)
Scope clarity	Included vs excluded is clear and written	
Support model	SLAs defined; response/resolution measurable	
Security baseline	MFA/CA/admin hygiene + exception tracking	

Backup confidence	Restore tests + evidence	
Operations	Monitoring, patch cadence, documentation	
Governance	Change control + improvement cadence	
Exit safety	Handover pack; no hostage tactics	

Optional help: If you want a second opinion on MSP answers, you can book a free consultation to sanity-check your shortlist.
hello@virtusgroup.biz · virtusgroup.co.nz · 0800 847 887 (VIRTUS)