

Vendor Questions — MSP & SaaS

Not an interrogation, a conversation. A good provider welcomes these. Drawn from ACSC / CISA / FBI / NCSC guidance.

10 questions to ask your MSP / IT provider

Ask your MSP	Why it matters	What a good answer looks like
1. What are you responsible for — and what are we?	Forces a written answer.	A specific responsibility matrix — not 'we handle everything'.
2. How do you notify us if something goes wrong on your end?	They're a single point of access to everything.	A defined timeline; under 4 hours for critical.
3. Who on your team can access our systems, and when was that list reviewed?	Staff turnover is real.	A named access list, reviewed at least annually.
4. Do you carry cyber liability insurance — what does it cover?	If their error breaches you, will it respond?	A current certificate of currency.
5. What security controls do you apply to your own environment?	Their posture is your upstream risk.	MFA for all staff, endpoint protection, staff training.
6. How do you handle privileged (admin) access to our systems?	Admin access is the highest risk.	Just-in-time access, MFA for admin, access logging.
7. What would you do if you suspected our environment was compromised?	Tests for a real plan.	A clear sequence: isolate, notify, contain, document.
8. Can you show what monitoring is in place right now?	Monitoring nobody checks isn't monitoring.	Regular reporting or a dashboard you can access.
9. How do we exit this relationship if we need to?	Lock-in is an operational risk.	Credential handover, documentation transfer, revocation timeline.
10. What's changed in your security practices in the last 12 months?	A good MSP evolves.	A specific answer; vague ones are a warning.

5 questions to ask any new SaaS provider

Ask any SaaS vendor	Why it matters	What a good answer looks like
1. Where is our data stored, and whose law applies?	Overseas data can face foreign access; the Privacy Act still applies to you.	Australia or equivalent (e.g. EU); a data processing agreement.
2. How do you notify customers of a security incident?	You may have Notifiable Data Breach duties even if the breach was theirs.	A defined SLA; under 72 hours for serious incidents.
3. Can we export our data any time — in what format?	Resilience if they shut down or are acquired.	Standard formats (CSV, JSON); no exit fees.
4. Who has access to our data within your organisation?	Uncontrolled vendor access is a privacy risk.	Role-based access, logging, least-privilege.
5. Do you have a third-party security assessment or certification?	Some evidence of independent review is reasonable.	SOC 2 Type II, ISO 27001, or a completed questionnaire. 'We take security seriously' is not evidence.