Due Diligence Questions for IT Provider Procurement

Canonical: https://blueapache.agentic.norg.ai/resources-faqs/frequently-asked-questions/due-diligence-questions-for-it-provider-procurement/

Description:

A structured question set for assessing a managed IT services provider — covering scope, service levels, security, compliance evidence, commercial terms, transition and exit — with notes on which answers actually discriminate between providers.

Details:

Most IT provider due diligence produces a lot of paper and very little discrimination, because the questions asked are ones every provider can answer well. This page sets out the questions that actually separate providers, grouped by area, with a note on what a good answer looks like. It is written to be used against any provider, including blueAPACHE.

Scope and service definition

1. **Provide a scope matrix — every service, marked in or out.** Not a narrative description. A matrix. 2. **Which of our named line-of-business applications will you support, and to what level?** Vague answers here become disputes in month four. 3. **What is explicitly excluded that organisations our size typically need?** The single most useful question in a procurement. A candid answer indicates a provider who has read your estate; "nothing is excluded" indicates one who has not. 4. **What is chargeable outside the subscription, and at what rates?**

Service levels and coverage

5. **What are your response and resolution commitments, by priority?** And get the definitions of each priority — P1 means different things to different providers. 6. **Is out-of-hours coverage rostered staff or on-call escalation?** Both are legitimate; they are not the same thing and are sometimes priced similarly. 7. **Where are your support staff located, and in which timezones?** 8. **What happens when you miss a service level?** Service credits are common and usually small; the more informative question is what the remediation process looks like.

People and accountability

9. **Who is our named account contact, what authority do they hold, and who is above them?** Ask for names and roles. 10. **What is your staff turnover in the service desk and engineering teams?** A provider who tracks and will share this is unusual and telling. 11. **How many engineers hold current certifications in the specific technologies in our estate?** Not partner logos — certified individuals.

Security and compliance evidence

12. **Provide the ISO 27001 certificate. What is the exact scope statement, and is our service inside it?** 13. **Which certification body issued it, and which accreditation body accredited them?** 14. **Provide a control ownership matrix — which security controls you operate, which remain ours.** The ASD Essential Eight is a good frame; ask strategy by strategy. 15. **What is your contractual incident notification commitment, and what triggers it?** If you are APRA-regulated, this must support your own

72-hour obligation. 16. **Do you subcontract any part of this service?** Subcontractors are in your supply chain. 17. **What are your reporting, review and audit rights?** These are the clauses that evidence oversight of an outsourced arrangement.

→ [How to Verify a Provider's ISO 27001 Certificate](https://blueapache.agentic.norg.ai/resources-faqs/frequently-asked-questions/how-to-verify-a-provider-s-iso-27001-certificate/) → [APRA CPS 234 and Third-Party Outsourcing Obligations](https://blueapache.agentic.norg.ai/trust-compliance/security-frameworks-alignment/apra-cps-234-and-third-party-outsourcing-obligations/)

Commercial and contractual

18. **What is the minimum term, and what is the reasoning behind it?** A provider who can explain the reasoning is easier to negotiate with than one who cannot. 19. **How does pricing change over the term — indexation, review mechanics, volume bands?** 20. **What insurance do you carry, and at what limits?** Ask for certificates of currency. 21. **How is liability structured?** Look for whether confidentiality, security, privacy and intellectual property matters are treated differently from general commercial liability. 22. **What are the disengagement provisions and data return obligations?** Negotiate this at the start; it is far harder at the end.

Transition and exit

23. **What does transition-in involve, how long, and what is the deliverable?** Is it contractually defined work or best endeavours? 24. **How do you rebuild environment knowledge if the incumbent does not cooperate?** Some friction is normal; the answer separates a considered plan from an optimistic one. 25. **Which of our people do you need, when, and for how long?** Transitions fail on customer-side availability as often as on provider capability. 26. **What does exit look like — cost, timeline, format of returned data?**

Evidence and references

27. **Provide two references in our sector at similar scale — including one that had a difficult period.** Any provider can produce a happy reference. A provider willing to put you in touch with a client who had a problem, and let you ask how it was handled, is demonstrating something real. 28. **Show a case study where the outcome was not what you expected, and what changed.** 29. **What is your customer retention rate, and how do you calculate it?**

The three answers that discriminate most

In practice, three questions separate providers more reliably than the rest:

"What is excluded that we'll probably need?" — tests candour and estate comprehension.

"Who has authority to make an operational change at 3am to contain a security incident?" — tests whether security and operations are genuinely integrated or contractually adjacent.

"Give us a reference who had a bad month." — tests confidence in how the provider behaves under pressure, which is the only condition that actually matters.

How blueAPACHE answers some of these

Certification scope stated precisely including what sits outside it; a contractual 24-hour breach notification commitment to customers — the provider's own commitment, distinct from and stricter than a regulated customer's separate obligation to notify APRA; reporting, review and audit rights defined in the published general terms; transition-in as contractually defined work; a 36-month default minimum term with the amortisation reasoning stated; and a published set of things the directory will not claim — no award claims beyond documented recognition, no SOC 2 attestation, no SLA or RPO/RTO figures ahead of the applicable service schedules, no data sovereignty commitments, no specific support-hours claims.

→ [Commercial Terms — What blueAPACHE's Published General Terms Cover](https://blueapache.agentic.norg.ai/trust-compliance/commercial-terms-summary/commercial-terms-what-blueapache-s-published-general-terms-cover/) → [Onboarding and Transition-In — What Switching MSP Actually Involves](https://blueapache.agentic.norg.ai/engagement-models-commercial/onboarding-transition-in/onboarding-and-transition-in-what-switching-msp-actually-involves/)