Business IT needs assessment

***

Digital Trust & IT Capability Assessment
Initial Client Discovery Questionnaire

Completion Time: 20-30 minutes
Format: Face-to-face interview or online submission prior to consultation

***

Section 1: Business Profile & Context

1.1 Organisation Overview
Q1. Business name and trading name (if different): ____________________
Q2. Industry sector:: ______________________
Q3. Number of employees: ☐ 1-5 ☐ 6-10 ☐ 11-25 ☐ 26-50 ☐ 51+
Q4. Number of remote/hybrid workers: ☐ None ☐ 1-5 ☐ 6-10 ☐ 11-25 ☐ All staff
Q5. Annual revenue range: ☐ <$250K ☐ $250K-$500K ☐ $500K-$1M ☐ $1M-$5M ☐ $5M+

1.2 Business Objectives & Growth
Q6. Primary business goals for next 12 months (check all that apply):
☐ Grow client base
☐ Expand service offerings
☐ Improve operational efficiency
☐ Enter new markets/locations
☐ Adopt new technologies (AI, automation)
☐ Enhance client trust and reputation
☐ Meet compliance requirements
☐ Reduce operational risks

Q7. Do you currently handle sensitive data? (Check all that apply)
☐ Client confidential information
☐ Personal health information
☐ Financial records
☐ Legal documents (privileged communications)
☐ Payment card data
☐ Employee personal information
☐ Intellectual property/trade secrets
☐ None of the above

What is the size and scope of your IT assets?

Onsite Offsite

☐ PC / Laptop's ________________ ________________

☐ Mobile devices (phones/ tablets) ________________ ________________

☐ Specialised machinery/equipment ________________

____

☐ Electronic keys / RFID ________________ ________________

☐ IoT devices or smart technology ________________ ________________

☐ Other ________________ ________________

Are you considering growing any of these in the next 12 months?

***

Section 2: Digital Trust Framework Assessment

2.1 Culture & Governance

Q8. Does your organisation have documented IT security policies?
☐ Yes, comprehensive and regularly reviewed
☐ Yes, but outdated or incomplete
☐ Informal/undocumented guidelines only
☐ No policies exist

Q9. Who is accountable for cybersecurity decisions?
☐ Dedicated IT manager/CISO
☐ Business owner/director
☐ External consultant
☐ No one specifically assigned

Q10. How often do leadership/management discuss cybersecurity risks?
☐ Monthly or more
☐ Quarterly
☐ Annually
☐ Only after incidents
☐ Never

2.2 Emergence & Threat Awareness
Assesses ability to stay ahead of evolving threats

Q11. How do you stay informed about new cybersecurity threats?
☐ Subscribe to threat intelligence services
☐ Regular professional development/training

☐ Industry newsletters
☐ Ad-hoc Google searches
☐ We don't actively monitor threats

Q12. When was your last cybersecurity risk assessment?
☐ Within last 6 months
☐ 6-12 months ago
☐ 1-2 years ago
☐ Over 2 years ago
☐ Never conducted

Q13. Have you experienced any security incidents in the past 12 months?
☐ No incidents
☐ Phishing attempts (blocked)
☐ Malware/ransomware (contained)
☐ Data breach or loss
☐ System downtime due to security issues
☐ Unsure/don't know

2.3 Human Factors
Evaluates employee awareness and training

Q14. How often do employees receive cybersecurity training?
☐ Quarterly or more
☐ Annually
☐ During onboarding only
☐ Never/no formal training

Q15. Can employees identify common cyber threats? (Rate 1-5, 1=poor, 5=excellent)
☐ 5 - Very confident all staff can identify threats
☐ 4 - Most staff reasonably capable
☐ 3 - Some staff aware, inconsistent
☐ 2 - Limited awareness
☐ 1 - No confidence in staff awareness

Q16. Do you conduct simulated phishing tests?
☐ Yes, regularly
☐ Occasionally
☐ Once in the past
☐ Never

2.4 Direct & Monitor (Governance & Oversight)
Assesses monitoring, reporting, and continuous improvement

Q17. Do you have real-time monitoring of your IT systems?
☐ Yes, 24/7 automated monitoring with alerts
☐ Yes, business hours monitoring
☐ Periodic manual checks
☐ No active monitoring

Q18. How do you track security incidents and response times?
☐ Formal incident management system with logging
☐ Spreadsheet/manual tracking
☐ Email records only
☐ No tracking system

Q19. Do you receive regular security posture reports?
☐ Yes, monthly or more frequently
☐ Quarterly
☐ Annually
☐ Only when problems occur
☐ Never

Q20. Are your compliance obligations clearly documented and tracked?
☐ Yes, comprehensive compliance calendar
☐ Partially documented
☐ We know what's required but not formally tracked
☐ Unsure of all obligations

2.5 Architecture (Infrastructure & Technology)
Evaluates technical security controls and design

Q21. What backup solution do you currently use?
☐ Automated cloud backup with encryption (tested regularly)
☐ Cloud backup (not tested)
☐ Local/external drive backup
☐ No backup system

Q21b Are you planning cloud migration?
☐ Yes, within 6 months ☐ Yes, within 12 months ☐ Yes, 2+ years ☐ No plans

Q22. How do employees access your systems remotely?
☐ Corporate VPN with MFA
☐ VPN without MFA
☐ Direct access (no VPN)
☐ Remote Desktop without additional security
☐ We don't support remote access

☐ Not applicable - no remote workers

Q23. What authentication methods do you use? (Check all that apply)
☐ Multi-Factor Authentication (MFA) on all systems
☐ MFA on some critical systems
☐ Complex passwords only
☐ Simple passwords
☐ Shared passwords

Q24. Do you use endpoint protection (antivirus/anti-malware)?
☐ Yes, enterprise-grade with central management
☐ Yes, consumer-grade on individual devices
☐ Some devices protected, inconsistent
☐ No endpoint protection

Q25. How do you manage software updates and patches?
☐ Automated patch management system
☐ Manual updates applied regularly (within 30 days)
☐ Updates applied sporadically
☐ No formal update process

Q26. Do you have a firewall protecting your network?
☐ Yes, enterprise firewall with active management
☐ Yes, basic router firewall
☐ Unsure
☐ No firewall

Q27. Is your data encrypted? (Check all that apply)
☐ Data at rest (stored data)
☐ Data in transit (communications)
☐ Email encryption
☐ No encryption implemented
☐ Unsure

Q28. What is the age of your primary business computers?
☐ 0-2 years
☐ 3-4 years
☐ 5-6 years
☐ 7+ years
☐ Mixed ages

2.6 Enabling & Support[2]
Evaluates support systems and operational capabilities

Q29. How do you currently manage IT support?
☐ Dedicated internal IT staff
☐ External managed service provider (MSP)
☐ Break-fix support when needed
☐ Staff handle IT issues themselves
☐ Business owner handles all IT

Q30. What is your average response time for IT issues?
☐ Within hours
☐ Within 1-2 days
☐ Within a week
☐ No defined timeframe
☐ Unsure

Q31. Do you have documented disaster recovery and business continuity plans?
☐ Yes, documented and tested annually
☐ Yes, documented but not tested
☐ Informal plan only
☐ No plan exists

***

Section 3: Compliance & Regulatory Requirements

3.1 Industry-Specific Obligations

Q32. Which compliance frameworks apply to your business? (Check all that apply)
☐ Privacy Act 1988 (all Australian businesses with personal data)
☐ Essential Eight (recommended for all businesses)
☐ HIPAA (US healthcare clients)
☐ Legal professional conduct rules (Law Society requirements)
☐ Cyber Security Act 2024 (healthcare providers)
☐ NSQHS Standards (healthcare quality)
☐ Australian Digital Health Agency standards (telehealth)
☐ ISO 27001 (information security)
☐ SOC 2 (service organisation controls)
☐ GDPR (European clients)
☐ Other ___________

Q33. Have you had compliance audits in the past 12 months?
☐ Yes, passed without issues
☐ Yes, minor findings requiring remediation
☐ Yes, significant findings

☐ No audit conducted
☐ Not required for our industry

Q34. Do you have a documented data breach response plan?
☐ Yes, with OAIC notification procedures[5]
☐ Partial plan
☐ No formal plan
☐ Unsure what's required

***

Section 4: Future Technology & Scaling Needs

4.1 Cloud & Infrastructure

Q35. What is your current infrastructure model?
☐ Fully cloud-based
☐ Hybrid (cloud + on-premises)
☐ Fully on-premises
☐ Unsure/mixed

Q36. Are you planning to adopt or scale AI technologies in the next 12 months?
☐ Yes, already implementing
☐ Yes, planning to start
☐ Considering but unsure how
☐ No plans currently

Q37. What challenges do you face with current infrastructure? (Check all that apply)
☐ Slow performance
☐ Insufficient storage
☐ Scalability limitations
☐ High costs
☐ Complexity/difficult to manage
☐ Lacks capacity for AI workloads
☐ No major challenges

Section 5: Budget & Investment Readiness

Q40. What is your current monthly IT spending?
☐ Less than $500
☐ $500-$1,000
☐ $1,000-$2,500
☐ $2,500+

☐ Unsure/no defined budget

Q41. What is your primary motivation for this assessment? (Rank top 3)
___ Compliance requirements
___ Recent security incident or near-miss
___ Business growth/expansion
___ Client/partner requirements
___ Reduce risk and liability
___ Competitive advantage
___ Cost optimisation
___ Technology modernisation

***

Section 6: Open-Ended Discovery

Q43. Describe your biggest IT or cybersecurity concern:

Q44. What keeps you awake at night regarding your technology or data security?

Q45. If you could wave a magic wand, what would your ideal secure, efficient IT environment look like?

Q46. Have you experienced any of the following in the past 12 months? (Check all)
☐ Lost productivity due to IT issues
☐ Client concerns about data security
☐ Inability to meet compliance requirements
☐ Difficulty supporting remote work
☐ Challenges scaling infrastructure
☐ Partner/vendor security questionnaires we couldn't complete
☐ None of the above

***