Australian SME
IT Security Checklist

A hands-on assessment for business owners with 5–100 staff.
Work through this with your IT provider. Tick what's in place, mark what needs help.

Company name:	
Completed by:	
Date:	
Number of staff / computer users:	
Number of offices / branches:	
Annual turnover:	*Under $3m / $3m or over*
Current IT provider:	*Internal / Outsourced / Ad-hoc*

Why the $3m question matters: Under the Privacy Act 1988, businesses with annual turnover of $3 million or more must notify the OAIC and affected individuals of eligible data breaches. From May 2025, the mandatory ransomware reporting regime also applies to businesses above this threshold. Even if you're under $3m, health, finance and education sectors are covered regardless of size.

Prepared by Zeno IT — ISO 27001:2022-certified managed IT provider, St Leonards, Sydney.

zeno.au | 1300 559 366 | info@zenoit.com.au

Section 1: Your Current Environment

Before assessing security controls, we need to understand what you're working with. This section identifies your platforms, data types and current setup.

Email & Collaboration Platform

	Yes	No	Help Me
Microsoft 365 (Exchange, Teams, SharePoint, OneDrive) *This is the platform most Australian SMEs run on. If you're on M365, the rest of this checklist is directly applicable.*			
Google Workspace (Gmail, Drive, Meet)			
Other / unsure — please specify: _____			

Sensitive Data You Handle

Tick all categories of sensitive information your business stores or processes. This determines your obligations under the Privacy Act and what controls you need.

	Yes	No	Help Me
Personal ID and contact details (driver's licences, emails, phone numbers)			
Financial records and commercial-in-confidence data			
Payment information (credit card, bank details)			
Legal, HR and employment records			
Health or medical records *Health records trigger additional obligations under the Privacy Act regardless of your turnover.*			
Children's or education data			
Intellectual property (patents, trade secrets, source code)			
Client data held on their behalf (you are a data processor)			

Business Systems

	Yes	No	Help Me
CRM (HubSpot, Salesforce, Zoho, industry-specific)			
ERP or accounting system (Xero, MYOB, NetSuite)			
Industry-specific line-of-business application			
Custom software or databases			
Website or e-commerce platform			
VoIP / phone system			

Section 2: Identity & Access Controls

Why this matters: Credential theft and business email compromise (BEC) are the #1 and #2 most reported cybercrimes in Australia (ASD, 2025). The average BEC loss is over $55,000 per incident. MFA alone blocks 99.9% of automated credential attacks (Microsoft).

	Yes	No	Help Me
MFA enabled on all company email accounts *Non-negotiable for cyber insurance. If you only do one thing on this list, do this.*			
MFA enabled on remote access (VPN, RDP, web portals)			
MFA enabled on all admin / privileged accounts			
MFA method is authenticator app or hardware key (not SMS only) *SMS-based MFA is vulnerable to SIM-swapping attacks. Insurers are starting to require phishing-resistant methods.*			
Separate admin accounts used for admin tasks (not daily email/browsing) *If your admin uses the same account for email and for managing servers, a single compromised password gives an attacker everything.*			
Admin access reviewed quarterly — unused accounts removed			
Standard users cannot install software without approval			
Users can only run company-approved applications			
USB ports restricted or blocked on company devices *Prevents data exfiltration and malware via removable media. Especially important for offshore or contract staff.*			
Company data access restricted by role-based permissions *Not everyone needs access to everything. Sales shouldn't see HR files. Finance data should be limited.*			
Password manager deployed for the team *Eliminates password reuse — the single biggest cause of credential compromise after phishing.*			
Leavers have all access revoked within 24 hours of departure *Former employees with active credentials are a documented attack vector. Requires an IT offboarding checklist.*			

Section 3: Devices, Patching & Network Security

Why this matters: Unpatched software and unmanaged devices are the most common entry points for ransomware in Australia. The ASD Essential Eight requires critical patches within 48 hours. Cyber insurers now ask for evidence of patching compliance.

	Yes	No	Help Me
Managed antivirus / EDR on all company devices *Free or consumer antivirus (Windows Defender alone, AVG Free) is not sufficient. Insurers want managed, centrally-reported endpoint detection.*			
Please specify your current AV/EDR product: _____			
All devices enrolled in a device management platform (e.g. Microsoft Intune) *Allows remote wipe if a device is lost or stolen. Required for conditional access policies.*			
Operating systems patched at least weekly *Windows, macOS. Critical patches within 48 hours per Essential Eight ML1.*			
Applications patched at least weekly *Browsers, PDF readers, Java, Zoom, Teams. These are the most exploited entry points.*			
No devices running unsupported operating systems *Windows 10 reaches end of support October 2025. Unsupported OS = unpatched = high risk.*			
All laptops encrypted (BitLocker on Windows, FileVault on Mac)			
Firewall in place and maintained (hardware or cloud-based) *Not just the Windows firewall — a properly configured network firewall with current firmware.*			
Wi-Fi network segregated (guest network separate from corporate)			
Email advanced threat protection enabled *Beyond basic spam filtering — catches impersonation, malicious links and weaponised attachments. Built into M365 Business Premium.*			
Dark web monitoring for company email credentials *Checks if any of your staff's login credentials have been leaked in known data breaches.*			

Section 4: Backup & Disaster Recovery

Critical: Microsoft 365 retains deleted emails for 30 days and SharePoint files for 93 days. This is NOT a backup. It does not protect against ransomware that encrypts files in place, and it does not meet Essential Eight backup requirements (3-month retention, independent storage, tested restores).

	Yes	No	Help Me
Third-party backup of Microsoft 365 data (email, SharePoint, OneDrive, Teams) *Separate from Microsoft's built-in retention. Stored independently of your M365 tenant.*			
Backup retention period is at least 3 months *Essential Eight requirement. Some businesses retain 12 months for compliance or legal reasons.*			
At least one backup copy is offline or immutable *Ransomware targets backups. If your backup is connected to the same network, it can be encrypted too.*			
Backup restores have been tested in the last 12 months *A backup you've never tested is not a backup. When was the last time you actually restored something?*			
Server / on-premise data backed up with same rigour (if applicable)			
Documented disaster recovery plan exists *What happens if your entire M365 tenant is compromised? Who do you call? What's the sequence? How long until you're operational?*			
Recovery time objective (RTO) defined and communicated *How long can your business survive without email? Without files? Without your line-of-business app?*			

Section 5: Policies, People & Cyber Insurance

HR & IT Policies

	Yes	No	Help Me
New staff IT onboarding checklist *Covers device setup, account creation, MFA enrolment, security training, acceptable use acknowledgement.*			
Staff termination IT checklist *Covers account disabling, device collection, access revocation, password changes for shared accounts.*			
Acceptable use policy signed by all staff			
Remote working / work-from-home policy			
E-banking and payment request verification process *Protects against invoice fraud and BEC scams. Should include phone verification for any payment changes or new bank details.*			
Employee / contractor confidentiality agreement			
Supplier / third-party security assessment process			

Security Awareness & Training

	Yes	No	Help Me
Staff complete cybersecurity awareness training at least annually			
Monthly phishing simulations with tracked results *Measures your team's click rate over time. Insurers increasingly ask for this data.*			
New starters receive security induction on day one			
Staff know how to report a suspected security incident *Is there a clear, documented process? Or do they just "tell someone"?*			

Incident Response & Compliance

	Yes	No	Help Me
Written incident response plan exists and has been tested			
Data breach notification process documented *Required under the Notifiable Data Breaches scheme for businesses over $3m turnover or in regulated sectors.*			
Business continuity plan (BCP) exists and has been tested			
Data privacy policy published (website and internal)			
Security logs retained for at least 90 days			
Annual security review or penetration test conducted			

Cyber Insurance

	Yes	No	Help Me
Current standalone cyber insurance policy in place *Not just a cyber add-on to your general business insurance — a standalone policy with specific coverage for breach costs, ransomware and business interruption.*			
All controls declared on the proposal form are actually implemented *Claims can be denied if you declared MFA was in place and it wasn't at the time of the incident.*			
Evidence packs ready for next renewal (MFA status, patch reports, backup logs)			
Policy reviewed in the last 12 months with your broker			

How to Read Your Results

Count your **"Yes"** ticks across all sections. This gives you a rough picture of where you sit.

Yes Count	Where You Sit	What To Do
0–15	**Significant gaps**	Your business has major exposure to common attacks and will likely struggle with cyber insurance. Priority: MFA on all accounts, managed antivirus/EDR, and a third-party M365 backup. These three changes alone will materially reduce your risk.
16–30	**Partial coverage**	You have some controls but gaps remain. Look at the "No" and "Help Me" columns — those are your priorities. You're likely below Essential Eight Maturity Level 1 in some areas. A structured assessment will show you exactly where.
31–40	**Solid foundation**	Core controls are mostly in place. Your gaps are likely in governance, documentation or training rather than technical controls. Focus on formalising policies, testing backups and getting evidence packs ready for your next insurance renewal.
41+	**Strong posture**	You're well ahead of most Australian SMEs. Consider formalising your position with Essential Eight ML2 alignment or ISO 27001 certification. This gives you a competitive advantage in tenders, insurance and client confidence.

This is not a formal audit. It's a practical starting point to identify gaps and have a more informed conversation with your IT provider. If any section has more "No" or "Help Me" ticks than "Yes", that section needs attention before your next cyber insurance renewal.

Next Step

If you'd like help working through this checklist or want a full security baseline assessment mapped to the Essential Eight and ISO 27001, the Zeno IT team can walk you through it. No lock-in, no pitch deck — just an honest look at where your IT and security is at.

Book a free IT & security review:

zeno.au/contact-us | 1300 559 366 | info@zenoit.com.au

Zeno IT is an ISO 27001:2022-certified managed IT and cybersecurity provider based in St Leonards, Sydney. We work with Australian businesses between 5 and 100 staff.