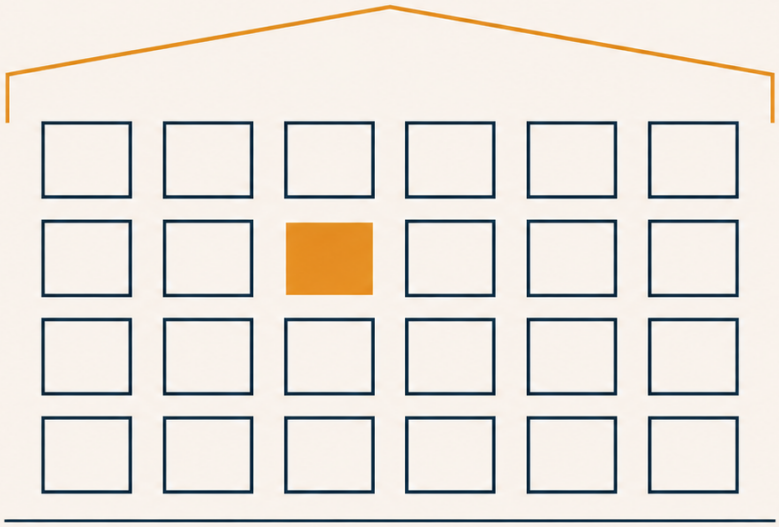
FOR AUSTRALIAN SMES · 2025–26 EDITION

Cyber Baseline & SaaS Audit

Sixty minutes of work that stops most cyber incidents. Plus the audit template that turns "we use a few tools" into a defendable inventory.



EDITION	FORMAT	PAIRS WITH
2025–26 (Australia)	6-page toolkit	Pillar 5 article

SECTION ONE · 18% OF AUSSIE BUSINESSES HAD A CYBER LOSS LAST YEAR. MOST MISSED ONE OF THESE.

The 60-minute cyber baseline

Print. Tick. Don't skip any.

IDENTITY (DO THIS FIRST)

- ☐ **Multi-factor authentication (MFA)** enabled on every business email account — for you and every staff member. Use an authenticator app (Microsoft, Google, Authy), not SMS.
- ☐ **MFA on every banking and credit-card login**. Most banks now require it but check secondary cards and merchant accounts.
- ☐ **MFA on accounting** (Xero, MYOB, QuickBooks) for every user. This is where the money lives.
- ☐ **MFA on cloud storage** (Google Drive, OneDrive, Dropbox) — for every user, including contractors.
- ☐ **Password manager deployed** (1Password, Bitwarden, LastPass). Every staff member gets an account. Unique generated passwords for every login.

DEVICES

- ☐ Operating system updates set to automatic on every laptop, desktop, and phone used for work.
- ☐ Disk encryption enabled (BitLocker on Windows, FileVault on Mac) on every laptop. Catastrophic if a laptop is stolen and isn't encrypted.
- ☐ Screen lock (auto-lock after 5 minutes) on every laptop and phone.
- ☐ Reputable antivirus / endpoint protection installed on every Windows machine (built-in Defender is acceptable for most SMEs).

BACKUPS (THE RECOVERY LAYER)

- ☐ Automated daily backups of accounting file to an off-site location (cloud or external service). Local-only backups die with the ransomware.
- ☐ Customer database and CRM exported regularly to a location separate from the live system.
- ☐ Critical documents (contracts, invoices, signed quotes) backed up to cloud storage with version history (Google Drive, OneDrive, Dropbox all do this).
- ☐ **Restore test conducted in the last 90 days**. A backup you've never restored is hope, not insurance.

ACCESS & OFFBOARDING

- ☐ Every staff member and contractor has their own individual login for every system (no shared accounts).
- ☐ Written offboarding checklist exists: when someone leaves, every access is revoked the same day.
- ☐ Quarterly review of who has access to what — surprise people often still have access months after they should.

SECTION TWO · FILL ONE ROW PER TOOL. THE LIST IS ALSO YOUR INCIDENT-RESPONSE PLAYBOOK.

The SaaS audit template

TOOL NAME	PURPOSE	$/YEAR	OWNER / ADMIN	DATA HELD	CRITICALITY (H/M/L)

*Pull your last 12 months of bank statements and credit-card statements to find every recurring software charge. Cross-check against your accounting software's payee list. Criticality: **H** = business stops if this goes down (accounting, banking, customer database); **M** = significant disruption (CRM, email marketing); **L** = inconvenient but workable (one-off design tools, niche utilities).*

> *The list is also your incident-response playbook. The morning your accounting login is locked is not the morning to be wondering "what else might be affected by the same compromised password".*
>
> — LK EDITORIAL STANDARDS · 2025–26 FRAMEWORK

SECTION THREE · THREE CADENCES. A BACKUP YOU'VE NEVER RESTORED IS A THEORY.

The backup verification routine

W
WEEKLY

Confirm the backup ran

Open your backup service dashboard (Xero file backup, cloud-storage version history, whatever you use). Confirm yesterday's backup completed successfully and that the file size is roughly what you'd expect. 60 seconds of work. Catches the silent failures that build up over months.

M
MONTHLY

Spot-restore one file

Pick any one document from your backup that you haven't touched in a few weeks. Restore it to a test location. Open it. Confirm it works. Five minutes of work. Catches the cases where backups appear to be running but contain corrupted or empty data.

Q
QUARTERLY

Full restore drill on the critical system

Once a quarter, simulate losing your most critical system (usually accounting). Restore the full backup to a fresh location, log in, run a balance check. The first time you do this you will find at least one thing that doesn't work as expected. That's the point — better to find it now than during a real incident.

IF THE WORST HAPPENS

Your first 60 minutes after a breach

0–5 min — **Contain**

Disconnect the affected device from the network (unplug ethernet, switch off Wi-Fi). Do not power it down — forensics may need the memory state.

5–15 min — **Lock the doors**

Change passwords on your most critical accounts from a clean device: email first (because email controls password resets for everything else), then banking, then accounting.

15–30 min — **Document**

Write down everything you know: when you first noticed, what you saw, what actions you've taken. Take screenshots. You'll need this for your insurer and possibly the police.

30–60 min — **Notify and engage**

Contact your cyber insurer (if you have one — most don't and should). Report to the Australian Cyber Security Centre at cyber.gov.au. If customer data was exposed, you may have notification obligations under the Notifiable Data Breaches scheme — talk to a lawyer fast.

SECTION FOUR · FIVE CATEGORIES. SET UP ONCE.

The minimum SME cyber stack

CATEGORY	WHY IT MATTERS	COMMON SME OPTIONS (2025–26)	TYPICAL $/YR
Password manager	Unique strong password per login, shared securely with the team.	1Password Business · Bitwarden Teams · Dashlane Business	$60–$120 / user
Authenticator app (MFA)	Stops 99%+ of credential-theft attacks.	Microsoft Authenticator · Google Authenticator · Authy · Duo	Free–$36 / user
Cloud backup with version history	Recoverable copies of every file, surviving ransomware.	Microsoft 365 / OneDrive Business · Google Workspace · Dropbox Business · Backupify	$144–$300 / user
Endpoint protection	Detects and blocks malware on every device.	Microsoft Defender (built in) · Bitdefender · CrowdStrike Falcon Go · SentinelOne	$60–$240 / device
Email security & phishing filter	Blocks the phishing emails that start most SME breaches.	Microsoft 365 Defender · Google Workspace · Mimecast · Proofpoint Essentials	$48–$180 / user

Most SMEs running Microsoft 365 Business Premium or Google Workspace Business Plus already have four of these five categories built in. Audit what your existing subscription includes before buying anything new — you may have paid for protection you never enabled.

> *You don't have an IT problem. You have a habits problem with an IT vocabulary. The owners who never get breached aren't the technical ones. They're the ones who treated cyber baseline like locking the front door at night — boring, daily, non-negotiable.*
>
> — LK EDITORIAL STANDARDS · 2025–26 FRAMEWORK

WHERE TO GO FROM HERE

Next steps & further reading

The baseline above is the floor. The pillar article goes further: choosing the right accounting platform, AI usage policies, vendor risk, and what good incident-response planning looks like for SMEs.

COMPANION ARTICLE

Australian SME tech & software (2025–26)

The full pillar article: cloud accounting choice, security stack for SMEs, AI in operations, vendor risk, and the rise of SME-targeted ransomware.

Read on lkbusinessadvisory.com.au →

OFFICIAL GUIDANCE

Australian Cyber Security Centre — Small Business Hub

Free, government-backed guidance, alerts, and the Small Business Cyber Security Guide. Worth bookmarking; subscribe to their alerts.

Visit cyber.gov.au →

DIAGNOSTIC

Business Health Score

Two of the 12 questions sit in Tech Infrastructure: MFA coverage and backup resilience. Take five minutes for the full diagnostic across all six dimensions.

Take the assessment →

RESOURCE

The 13-Week Cash Flow Pack

The companion pack for Pillar 4. The Excel template assumes you've done the baseline above — because the file lives in cloud storage that's properly backed up.

Download →

General information only, not personal cyber, legal, or insurance advice. Specific product recommendations reflect common 2025–26 options; evaluate against your own threat model and budget. For meaningful breach exposure, engage a qualified cyber security professional or MSP.