vemo

IT Risk Assessment Worksheet for NZ Businesses

Identify, Assess, and Mitigate Your IT Risks — Before They Become Expensive Problems

For New Zealand SMEs looking to explore where AI can make a difference—without the hype.

Why This Worksheet Matters

Many New Zealand businesses don't discover their IT risks until it's too late — after a cyber attack, outage, data loss, or failed audit. This worksheet is designed to help SMEs proactively assess their IT environment and uncover hidden vulnerabilities across devices, data, access, and systems. Whether you're preparing for a cyber insurance application, complying with Essential 8 or NIST 2.0, or just trying to sleep better at night, this practical tool helps you take stock, take control, and take action.

What You'll Get From This Exercise

- A practical, no-jargon understanding of your IT risk exposure
- A list of high-priority fixes you can action internally or with your IT provider
- Confidence when applying for cyber insurance or tendering for contracts
- A consistent process to repeat annually or after business changes
- A way to show leadership and staff that IT is being managed proactively

---

IT Risk Assessment Scoring Worksheet

Rate each question from 1 to 5.

Score	Meaning
1	No controls in place / Not addressed at all
2	Partially considered, not yet implemented
3	Implemented but not enforced or reviewed
4	Implemented and partially monitored
5	Fully implemented, reviewed, and working well

Question 1: Device & Endpoint Security

How well are your devices protected?

Question	What It Means	Why It Matters	What Could Go Wrong	Your Score (1–5)
Do all company devices have antivirus or endpoint protection (EDR)?	EDR detects and stops malicious activity on devices.	It blocks ransomware, viruses, and unauthorised access.	Malware can spread silently and damage systems.	
Are operating systems and software patched regularly?	Updates fix security holes in Windows/macOS or apps.	Unpatched systems are an easy entry point for attackers.	Hackers can exploit outdated software to take control.	
Are staff using only company-managed devices (no BYOD)?	BYOD = Bring Your Own Device (personal laptops/phones).	Company devices can be secured, monitored, and wiped.	Sensitive data might be exposed or lost on personal devices.	
Are mobile phones used for work protected with PINs or biometrics?	Devices should be locked when idle.	Prevents access to business email or cloud apps if stolen.	A stolen phone could give access to your inbox, files, or apps.	
Are USB drives restricted or encrypted?	USBs can carry malware or leak data.	Limits risky file transfers and data loss.	Data could be stolen, or malware brought in from home.	

Section Score (out of 25): _____

Question 2: Access & Identity Management

Who can access your systems — and how securely?
If someone gets in who shouldn't, the damage can be serious and fast.

Question	What It Means	Why It Matters	What Could Go Wrong	Your Score (1–5)
Are access levels based on job roles (least privilege)?	People should only access what they need to do their job.	Limits accidental damage or exposure of sensitive data.	Junior staff could delete financial records by mistake.	
Are shared logins avoided?	Every user should have their own login.	Allows tracking, auditing, and accountability.	If something goes wrong, you can't see who did it.	
Is MFA enabled for all critical systems?	MFA = Multi-Factor Authentication (password + code).	Stops attackers even if passwords are leaked.	Without MFA, stolen credentials give full access.	
Are ex-staff accounts deactivated immediately?	Disable logins as soon as someone leaves.	Prevents unauthorised access or sabotage.	A former employee could log in and delete data.	
Is access to sensitive data monitored and logged?	Track who accesses critical files and systems.	Helps detect breaches or insider threats.	You won't know who accessed what — or when.	

Section Score (out of 25): _____

Question 3. Backups & Business Continuity

If something goes wrong, can you get your data and systems back quickly?
This is your business insurance when disaster strikes.

Question	What It Means	Why It Matters	What Could Go Wrong	Your Score (1–5)
Do staff receive regular cyber awareness training?	Learn how to spot phishing and scams.	Reduces human error and risky behaviour.	A click on a fake invoice could trigger ransomware.	
Do you have email filtering in place?	Automatically blocks dangerous or spam emails.	Reduces phishing and malware reaching staff.	Risky emails land in inboxes and get clicked.	
Is there an easy way to report suspicious emails?	Staff should be able to flag and get help fast.	Speeds up response and avoids repeat mistakes.	Staff ignore threats, or respond incorrectly.	

Do you use password managers?	Store and autofill secure passwords.	Stops reuse of weak or repeated passwords.	One hacked password can lead to full system access.	
Do you have a process for when someone clicks a bad link?	What happens if someone makes a mistake?	Containment and quick response matter.	Without a plan, infections spread quickly.	

Section Score (out of 25): _____

Question 4. Policy, Governance & Documentation

Is your IT environment structured, documented, and managed properly?
Without visibility, things fall through the cracks.

Question	What It Means	Why It Matters	What Could Go Wrong	Your Score (1–5)
Do you have an IT policy staff must follow?	Covers devices, apps, passwords, and behaviours.	Sets expectations and accountability.	Staff use weak passwords or risky apps without knowing.	
Do you maintain an asset register?	A list of all hardware and software.	You can't protect what you don't track.	Lost laptops, expired licenses, or missed renewals.	
Do you have policies for AI, remote work, and passwords?	Written guidelines for how modern tools are used.	Clarifies what's allowed, what's not.	Staff might unknowingly expose data through apps.	
Are vendor responsibilities documented?	Know who supports what and who to call.	Speeds up support and reduces miscommunication.	Delays and finger-pointing when issues arise.	
Do you track system uptime or recurring IT issues?	Regular metrics or logs.	Helps you spot patterns and fix root causes.	You keep solving symptoms, not causes.	

Section Score (out of 25): _____

Question 5: Email, Phishing & Staff Awareness

Are your people prepared to deal with scams, phishing, and cyber threats?
The #1 cause of breaches isn't tech — it's people.

Question	What It Means	Why It Matters	What Could Go Wrong	Your Score (1–5)
Do staff receive regular cyber awareness training?	Learn how to spot phishing and scams.	Reduces human error and risky behaviour.	A click on a fake invoice could trigger ransomware.	
Do you have email filtering in place?	Automatically blocks dangerous or spam emails.	Reduces phishing and malware reaching staff.	Risky emails land in inboxes and get clicked.	
Is there an easy way to report suspicious emails?	Staff should be able to flag and get help fast.	Speeds up response and avoids repeat mistakes.	Staff ignore threats, or respond incorrectly.	
Do you use password managers?	Store and autofill secure passwords.	Stops reuse of weak or repeated passwords.	One hacked password can lead to full system access.	
Do you have a process for when someone clicks a bad link?	What happens if someone makes a mistake?	Containment and quick response matter.	Without a plan, infections spread quickly.	

Your Results: IT Risk Assessment Scoring Summary

Step 1: Transfer Your Section Scores

Section	Your Score (out of 25)
Device & Endpoint Security	_____
Access & Identity Management	_____

Backups & Business Continuity	_____
Policy, Governance & Documentation	_____
Email, Phishing & Staff Awareness	_____

Step 2: Interpret Each Section

Use the table below to interpret each section's score:

Score Range	What It Means	Action Required
21–25	Excellent	Maintain and monitor. No immediate action needed.
16–20	Good	Small improvements can boost resilience.
11–15	Concerning	Gaps exist — prioritise improvement.
0–10	High Risk	Immediate action required to reduce vulnerability.

Highlight any section **scoring under 15** — this is a key exposure area in your IT environment.

Step 3: Identify Your Weakest Link

Your lowest-scoring section is the one most likely to expose your business to risk.
Start there.

Examples:

- If Device & Endpoint Security is your lowest: Improve antivirus, patching, device control.
- If Access & Identity is lowest: Enforce MFA, disable shared logins, review account removals.
- If Backups & Continuity is lowest: Implement cloud/offsite backups and run restore tests.
- If Email & Phishing is lowest: Train staff, filter email, prepare response steps.
- If Policy & Documentation is lowest: Roll out simple, written IT policies and assign ownership.

Step 4: Review Data & Security

1. Does it store or access sensitive client or business data?
2. Are there data privacy settings or NZ-compliant security options?
3. Do you need an AI Policy in place before rollout?

Use Vemo's AI Policy Template to ensure your use is ethical, compliant, and secure.

Optional: Overall IT Risk Score

Add up all 5 section scores:

Total Score (out of 125): _____

Total Score	Risk Level	Interpretation
110–125	Low Risk	Strong IT posture. Keep up the good work.
90–109	Moderate Risk	Solid base, but several areas need work.
Below 90	High Risk	Significant weaknesses – start resolving top issues immediately.

Step 5: Next Steps

- Focus on your lowest-scoring section first
- Assign ownership and set deadlines for improvements
- Book a 30-min IT Risk Review with Vemo to get tailored recommendations
- Repeat this assessment every 6–12 months, or after major IT/business changes

---

Examples of How To Fix: IT Risk Solutions by Section

Use this table to plan your next steps. Start with your **lowest-scoring section** from the assessment.

Device & Endpoint Security

Risk Identified	Why It's a Problem	Recommended Fix
No antivirus or endpoint protection (EDR)	Malware can spread undetected	Install a modern EDR tool like CrowdStrike or Microsoft Defender for Business.
Devices not patched regularly	Hackers exploit outdated systems	Use automated patch management (e.g. Microsoft Intune or RMM software).

Staff use personal devices (BYOD)	No control or visibility	Issue managed company devices, or enforce BYOD policies with MDM tools.
Mobile devices lack screen lock	Anyone can access business apps	Enforce PIN/Face ID with mobile policies. Use mobile threat protection tools.
USB drives not restricted	Can import malware or leak data	Disable USB access via Group Policy or encrypt company-issued drives.

Access & Identity Management

Risk Identified	Why It's a Problem	Recommended Fix
Users have broad or admin access	Increases breach potential	Apply role-based access control (RBAC). Review user roles quarterly.
Shared logins still used	No accountability or audit trail	Assign unique logins per user. Disable shared service accounts.
No MFA on key systems	Single point of failure if password is stolen	Turn on MFA for Microsoft 365, Google, VPNs, cloud apps.
Ex-staff still have account access	Security backdoor	Automate offboarding checklists. Set 24-hour deactivation rule.
No monitoring of sensitive data access	Breaches go unnoticed	Enable audit logs, review activity monthly. Tools: Microsoft Purview, Google audit logs.

Backups & Business Continuity

Risk Identified	Why It's a Problem	Recommended Fix
Infrequent or manual backups	Recovery might not be possible	Use automated daily or hourly backup software.
Backups stored only onsite	At risk of fire, flood, theft	Use hybrid backup (local + cloud) or fully cloud-based backups.
No encryption on backups	Stolen backup = exposed data	Ensure backup data is encrypted at rest and in transit.
Never tested a restore	Backups might not work	Run quarterly restore tests. Document results.
No disaster recovery plan	Chaos during outages	Create a one-page DR plan with roles, steps, and contacts. Review annually.

Email, Phishing & Staff Awareness

Risk Identified	Why It's a Problem	Recommended Fix
No staff training	Humans remain the weakest link	Run phishing simulations and short workshops (e.g. KnowBe4, Vemo-led sessions).
No email filtering	Malware and spam reach users	Implement Microsoft Defender, Mimecast, or Google spam protection.
Staff can't easily report threats	Slows response and learning	Add a "Report Phishing" button or shared inbox (e.g. report@yourcompany.nz).
Password reuse across systems	Easy entry for attackers	Roll out a password manager like 1Password, Bitwarden, or Keeper.
No incident procedure if a phishing link is clicked	Delays containment and cleanup	Create a short, printed "What to do if you clicked" checklist and train teams.

Policy, Governance & Documentation

Risk Identified	Why It's a Problem	Recommended Fix
No formal IT policy	Staff don't know what's expected	Use Vemo's free IT Policy Template. Tailor for your team.
No asset register	Can't track devices or software	Maintain a live asset list in Excel or RMM system. Include purchase dates.
No password or remote work policy	Confusion or risky behaviour	Create a basic Acceptable Use Policy (AUP) covering both.
No clarity on vendor roles	Support delayed during issues	Document who to call for internet, phones, backups, etc. Include escalation paths.
No visibility on uptime or issues	Trends missed, wasteful fixes	Use a simple IT log or status tracker to spot repeat issues.

Not Sure Where to Start?

Let's make it simple.
We offer a Chief Information officer (CIO) for a day to:

- Review your IT Risk Assessment
- Identify the fastest fixes with the biggest impact
- Build a clear, jargon-free action plan for your business

Contact Vemo | Book Your Free CIO for a Day