Good Security

CHECKLIST WATERMARKED PDF

OPERATIONAL CHECKLIST

Cyber Insurance Readiness Checklist

30 controls NZ insurers commonly require or assess at underwriting. Work through this checklist before applying for or renewing cyber insurance to improve eligibility and reduce premiums.

Branded customer-ready document | Shareable with leadership teams | Generated 12 Mar 2026

Prepare for your cyber insurance application or renewal

Good Security · goodsecurity.co.nz · **hello@goodsecurity.co.nz**

How to use this checklist Work through each control and mark your status using the indicators below. When applying for or renewing cyber insurance, you will be asked about most of these controls. Honest answers are essential — misrepresentation can void your policy when you need it most.

INDICATOR	MEANING
✅ In Place	Control is implemented and effective
⚠️ Partial	Control exists but has gaps or is not consistently applied
❌ Not in Place	Control has not been implemented

Important: This checklist does not replace professional insurance advice. Review your policy wording carefully and engage a NZ broker with cyber insurance experience.

SECTION 1: ACCESS CONTROL

Critical — required by most insurers. Gaps here are the most common reason for declined cover.

Multi-factor authentication (MFA) on email MFA is enabled for all staff email accounts. This is the single most commonly required control. Insurers increasingly refuse cover without it.

☐ Status: ✅ / ⚠️ / ❌ Notes: _____

MFA on all remote access MFA is required for VPN, Remote Desktop, cloud platforms, and any system accessible from outside the office network.

☐ Status: ✅ / ⚠️ / ❌ Notes: _____

MFA on privileged and administrator accounts All administrator accounts have MFA enforced. Admin accounts are used only for administrative tasks — not for day-to-day work.

☐ Status: ✅ / ⚠️ / ❌ Notes: _____

Privileged access is restricted The number of staff with administrator rights is limited to those who genuinely require it. This is reviewed periodically.

☐ Status: ✅ / ⚠️ / ❌ Notes: _____

Offboarding procedure removes access promptly When a staff member leaves, their access is revoked within 24 hours. This process is documented and consistently followed.

☐ Status: ✅ / ⚠️ / ❌ Notes: _____

SECTION 2: ENDPOINT SECURITY

Endpoint detection and response (EDR) on all managed devices Business-grade endpoint protection is installed on all devices used for work. This goes beyond basic antivirus — EDR provides detection and response capabilities.

☐ Status: ✅ / ⚠️ / ❌ Notes: _____

Operating systems and software are patched promptly Critical security patches are applied within 30 days of release. There is a documented patching schedule, or automatic updates are enabled and verified.

☐ Status: ✅ / ⚠️ / ❌ Notes: _____

Full-disk encryption on all laptops All laptops have full-disk encryption enabled — BitLocker on Windows, FileVault on Mac. This prevents data exposure if a device is lost or stolen.

☐ Status: ✅ / ⚠️ / ❌ Notes: _____

Mobile Device Management (MDM) in use If staff use mobile devices for work, an MDM solution — Microsoft Intune, Jamf, or equivalent — manages and secures these devices.

☐ Status: ✅ / ⚠️ / ❌ Notes: _____

SECTION 3: EMAIL SECURITY

Email authentication configured (SPF, DKIM, DMARC) Your domain has SPF, DKIM, and DMARC DNS records correctly configured. DMARC is set to at minimum `p=quarantine`. This is a baseline defence against Business Email Compromise.

☐ Status: ✅ / ⚠️ / ❌ Notes: _____

Anti-phishing and anti-spam filtering is active Email filtering — Microsoft Defender for Office 365, Proofpoint, Mimecast, or equivalent — is enabled to detect and quarantine phishing emails before they reach staff.

☐ Status: ✅ / ⚠️ / ❌ Notes: _____

Business Email Compromise (BEC) controls in place Financial processes require out-of-band verification — a phone call to a known number — before making payments to new or changed payees based on an emailed instruction.

☐ Status: ✅ / ⚠️ / ❌ Notes: _____

SECTION 4: BACKUP & RECOVERY

Business data is backed up at least daily Critical data — financial records, customer data, operational systems — is backed up at minimum daily.

☐ Status: ✅ / ⚠️ / ❌ Notes: _____

Backups are stored offline or immutably Backups are stored in a location that cannot be encrypted by ransomware. Acceptable options: offsite location, cloud with versioning and deletion protection enabled, tape, or air-gapped storage.

☐ Status: ✅ / ⚠️ / ❌ Notes: _____

Backups have been successfully tested A full or partial restore has been tested in the last 12 months and confirmed successful. An untested backup is not a backup.

☐ Status: ✅ / ⚠️ / ❌ Date of last restore test: _____

Recovery Time Objective (RTO) is defined You know how long it would take to restore critical systems from backup and have a plan to achieve this within a tolerable timeframe.

☐ Status: ✅ / ⚠️ / ❌ Notes: _____

SECTION 5: INCIDENT RESPONSE

Incident response plan is documented A written incident response plan exists, covering how to detect, contain, and recover from a cyber incident.

☐ Status: ✅ / ⚠️ / ❌ Notes: _____

The plan has been tested in the last 12 months A tabletop exercise or walk-through has been conducted to test the plan. Insurers increasingly require evidence of testing, not just documentation.

☐ Status: ✅ / ⚠️ / ❌ Date of last test: _____

Staff know what to do if they suspect an incident All staff know who to contact and what not to do — don't turn off devices, don't discuss on potentially compromised systems — if they suspect an incident.

☐ Status: ✅ / ⚠️ / ❌ Notes: _____

Cyber insurer contact details are accessible offline The insurer's incident response hotline is printed and accessible without relying on systems that may be compromised.

☐ Status: ✅ / ⚠️ / ❌ Notes: _____

SECTION 6: SECURITY AWARENESS & TRAINING

All staff have completed security awareness training in the last 12 months Training covers phishing recognition, password hygiene, and how to report suspicious activity. Completion is documented.

☐ Status: ✅ / ⚠️ / ❌ Date: _____ Completion rate: ____

Phishing simulations are conducted Simulated phishing exercises are used to test and reinforce staff awareness. Results are tracked and used to inform targeted training.

□ Status: ✅ / ⚠️ / ❌ Notes: _____

SECTION 7: THIRD-PARTY & SUPPLY CHAIN RISK

Critical vendors have been security assessed Your most important technology and data suppliers have been reviewed for their security practices — cloud providers, IT managed service providers, and any vendor with access to your systems or data.

□ Status: ✅ / ⚠️ / ❌ Notes: _____

Contracts with vendors include data security obligations Agreements with vendors that access or process your data include provisions requiring appropriate security controls and breach notification.

□ Status: ✅ / ⚠️ / ❌ Notes: _____

SECTION 8: DATA GOVERNANCE

Personal data inventory is maintained You know what personal information you hold, where it is stored, who can access it, and how long you retain it. This is required under the Privacy Act 2020.

□ Status: ✅ / ⚠️ / ❌ Notes: _____

Sensitive data is classified and access-controlled Sensitive data — personal information, financial data, intellectual property — is identified and access restricted to those who have a genuine need.

□ Status: ✅ / ⚠️ / ❌ Notes: _____

Data retention policy is in place and followed There is a documented policy for how long different types of data are kept. Data is deleted securely when it is no longer needed.

□ Status: ✅ / ⚠️ / ❌ Notes: _____

SECTION 9: NETWORK SECURITY

Remote Desktop Protocol (RDP) is not exposed to the internet RDP is not accessible directly from the internet. If remote access is required, it is via VPN with MFA.

□ Status: ✅ / ⚠️ / ❌ Notes: _____

Network segmentation separates critical systems If you have on-premises servers or operational technology, critical systems are on a separate network segment from general office traffic.

□ Status: ✅ / ⚠️ / ❌ Notes: _____

Guest Wi-Fi is separate from business Wi-Fi Office Wi-Fi has separate networks for staff and guests. Guests cannot access business systems.

□ Status: ✅ / ⚠️ / ❌ Notes: _____

READINESS SUMMARY

SECTION	CONTROLS IN PLACE	PARTIAL	NOT DONE
Access Control (5 controls)			
Endpoint Security (4 controls)			
Email Security (3 controls)			
Backup & Recovery (4 controls)			
Incident Response (4 controls)			
Awareness & Training (2 controls)			
Third-Party Risk (2 controls)			
Data Governance (3 controls)			
Network Security (3 controls)			
Total (30 controls)			

WHAT YOUR SCORE MEANS

25–30 in place: Strong control environment. You are well-positioned for cyber insurance. Focus on maintaining and evidencing these controls at renewal.

18–24 in place: Moderate readiness. Prioritise the Access Control and Backup sections before applying. You may face higher premiums or specific exclusions for gaps.

Under 18 in place: Significant gaps exist. Many NZ insurers will decline cover or offer very limited cover until foundational controls — particularly MFA and tested backups — are in place. Contact Good Security for a prioritised remediation plan.

PRIORITY ACTIONS BEFORE APPLYING

If you need to improve your position quickly, address these in order:

1. **MFA everywhere** — The single biggest factor in insurer acceptance. Email, remote access, and admin accounts first.
2. **Offsite or immutable backups** — Insurers that pay ransomware claims prioritise this above almost everything else.
3. **Endpoint protection** — Business-grade EDR on all managed devices.
4. **Incident response plan** — Even a basic documented plan demonstrates you have thought through your response.
5. **Staff training** — Documented completion of annual training supports your application.

QUESTIONS YOU WILL LIKELY BE ASKED ON THE APPLICATION

- Do you use MFA for email, remote access, and admin accounts? (Yes/No for each)
- How often are backups taken, and are they stored offline?
- Do you have a documented incident response plan?
- Have you tested your backup restore in the last 12 months?
- How many employees do you have?
- What is your annual revenue?
- What personal information do you hold and how is it protected?
- Have you experienced a cyber incident in the last 3–5 years?
- What industry sector do you operate in?