

Cyber insurance readiness checklist

The controls insurers now ask about on renewal forms, in plain language. Work through it before the form arrives, not after.

Free to use and adapt.

Why the questions got harder

Cyber insurance applications used to be short. They are not anymore. Insurers now ask directly whether specific controls are in place, and the answers affect both your premium and whether a claim gets paid.

Work through this honestly. An accurate "no" is something you can fix. An inaccurate "yes" is the answer that causes trouble at claim time, because an application is a factual declaration and a materially wrong answer can put your cover at risk.

Identity and access

- ☐ Multi-factor authentication on **all** email accounts
- ☐ Multi-factor authentication on remote access and VPN
- ☐ Multi-factor authentication on administrator accounts
- ☐ No shared or generic logins standing in for named individuals
- ☐ Administrator accounts kept separate from day-to-day accounts
- ☐ Access removed the same day someone leaves
- ☐ A password manager in use, rather than reused passwords

Devices

- ☐ Endpoint protection on every computer, centrally monitored
- ☐ Disk encryption enabled on laptops
- ☐ Operating systems and applications patched on a schedule
- ☐ No unsupported operating systems still in use
- ☐ Mobile devices that reach company email are managed
- ☐ **No Remote Desktop (RDP) exposed directly to the internet.** This is a knockout question on most current forms. If you need remote access, it goes behind a VPN or a broker, not straight onto the open internet.

Backups

- ☐ Backups running for email, files, and any server
- ☐ At least one copy ransomware cannot reach

- ☐ Restores tested, with a date you can actually name
- ☐ Retention long enough for your obligations

Email and fraud

- ☐ Spam and phishing filtering in place
- ☐ External sender warnings enabled
- ☐ SPF, DKIM, and DMARC configured on your domain
- ☐ A verification step before any change to payment details
- ☐ Staff have been shown what invoice fraud looks like

Process and documentation

- ☐ You can produce a list of devices and who has them
- ☐ You know where your data lives
- ☐ Someone is named as responsible for IT
- ☐ A written plan for what happens after an incident
- ☐ Evidence you could show an underwriter: reports, screenshots, policies

For each box you tick, note **where the evidence lives**. "Yes" is the answer; being able to show it is what matters if a claim is ever examined.

How to use your answers

Every unchecked box is either a fix or an honest "no" on the form. Most are a few hours of work, not a project.

The two that most often move a premium: **multi-factor authentication everywhere**, and **backups with a tested restore**. If you only do two things, do those.

About this template. Free to use, edit, and share, including commercially. No credit needed and no permission required. It is a starting point built from common practice. It is not legal advice, not a compliance certification, and not a substitute for advice about your situation. Your obligations depend on your industry, your regulator, your insurer, and your contracts. If you are in a regulated field, have someone qualified review this before you rely on it.

Last reviewed: August 2026 · Latest version: brevitytech.ca/templates

Made by **Brevity.Tech**, managed IT and automation for small businesses in Metro Vancouver. We complete this questionnaire with clients and put the controls in place, so renewal becomes an hour of form-filling rather than a scramble. A free 30-minute check will tell you which boxes you can already tick. brevitytech.ca · 778-321-2372