

FOR ACCOUNTING AND ADVISORY FIRMS

How to answer your cyber insurance renewal without guessing, even if your IT is outsourced

Three IT questions on the form, and how to check your answers yourself

---

With an email you can send your IT provider this week.

THE SITUATION

Someone has to sign it

The email from your broker has the renewal application attached and a date to send it back. One question asks whether multi-factor sign-in is on for email, remote access and administrator accounts. Another asks whether your backups are kept offline. Another asks how you confirm a request to change banking details.

You know two of the answers. For the rest, you'd be guessing, and your name, or a partner's, goes at the bottom.

That isn't a sign the firm is careless. The questions are written for IT people, and they end up on the desk of a partner, a principal or an office manager. This guide covers three of them, what each one is asking and how to check your answer yourself.

This guide draws on two Canadian insurers' current application forms. Yours will be worded a little differently, so pull last year's application out of your email and read it alongside this guide.

WHY IT MATTERS

Why the answers matter

Your answers on the application are what the insurer relies on when it decides to cover you. If an answer turns out to overstate what's in place, it can affect a claim later, and in some cases the whole policy.[1,2]

Give the accurate answer, even when it's partial. A "partly," with a note explaining what's in place, is worth more than a "yes" that doesn't hold up when you need to claim. Your answers can also affect the terms you're offered, so take a partial answer to your broker, or whoever places your policy, before you submit, not after.[6]



QUESTION 1

Is multi-factor sign-in on for every account that needs it?

WHAT THE FORMS ASK

The forms split this into three parts: email, remote access (signing in to the office systems from outside) and administrator accounts, the ones with full control. One also asks about cloud systems that hold sensitive information.[3]

WHAT "ALL" COVERS

Look at the accounts that tend to get exceptions: partners, shared mailboxes, anyone who works from home, and the administrator accounts used to manage your systems.

HOW TO CHECK

Ask your IT provider for a list of accounts that don't have multi-factor sign-in, split into email, remote access and administrator accounts.

When you ask your provider, here's what a solid reply and a weak one sound like.

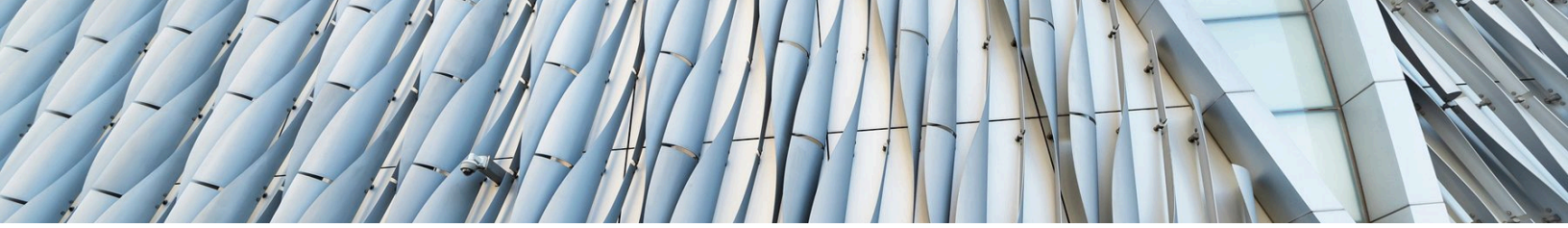
A REPLY YOU CAN RELY ON

"Every email account has it, including the two shared mailboxes. Remote access and the admin accounts have it too. Here's the list, checked last week."

A REPLY TO PUSH BACK ON

"Yes, it's on."

Ask for the list.



QUESTION 2

Are your backups kept offline or on a separate network?

WHAT THE FORMS ASK

The forms ask whether backups of critical data are kept "offline or on a separate network." One also asks how many copies you keep and how often you test a full restore.[3] The Canadian Centre for Cyber Security says long-term backups, such as weekly ones, must be stored offline.[4]

WHAT "OFFLINE" MEANS

A copy that someone with full access to your network couldn't reach or delete. If ransomware could get to your backups, they aren't offline.

WHY A TEST MATTERS

A backup can run every night and still fail when you need it. The Canadian Centre tells organizations to "regularly verify that back-up and restore mechanisms operate as expected," and CPABC tells firms to verify backups "even if IT is outsourced."[4,5] A test restore is how you know your "yes" is true, and one of the forms asks for it directly.

HOW TO CHECK

Ask your IT provider three things: where the offline copy is, how often it's made and the date of the last test restore.

A REPLY YOU CAN RELY ON

"A copy goes offline every night. We restored the client file folder and a full laptop last week. Both opened. Here's the record."

A REPLY TO PUSH BACK ON

"The backups run every night."

Ask when a restore was last tested.



QUESTION 3

How do you confirm a request to change banking details or send money?

WHAT THE FORMS ASK

Both forms ask whether you confirm a payment request another way before you act on it, such as a phone call. One asks about transfers over $25,000. The other asks about requests to change a supplier's or client's account details, and about paying a new account.[3]

WHY IT MATTERS

Most firms do this by habit. The form asks whether it happens every time, and a habit that someone skips on a busy day isn't a yes. AI makes fake requests harder to spot.[7] More on page 7.

HOW TO CHECK

You don't need IT for this one. Ask the people who handle payments what they do when an email asks them to change banking details or pay a new account. Then write the rule down: call back on a number you already have, never one in the email, and have a second person approve.

A REPLY YOU CAN RELY ON

"Every change to banking details and every payment to a new account is confirmed by phone on a number we already have, and a second person approves it. It's in our written payment procedure."

A REPLY TO PUSH BACK ON

"We'd notice if something looked off."

Ask what happens every time, and write it down.

THE REST OF THE FORM

What else the forms ask

This guide covers three questions. The two forms behind it ask more, and the insurer relies on every answer:[3]

- **Who is responsible for IT security, by job title.** Name one person, often the managing partner, principal, office manager or your in-house IT lead, and get your provider's responsibilities in writing.
- Whether you've had a cyber incident or claim in the last three years, or know of anything that could lead to one
- How much personal and sensitive client information you hold
- Whether laptops and desktops are encrypted
- What protects each computer, and who watches it day and night
- Whether email is filtered and staff are tested with practice phishing emails
- Whether staff have administrator rights on their own computers
- Whether you run software that's no longer supported, and how quickly updates go on
- Whether you have a written plan for a cyber incident

Your IT provider can answer most of these. Ask for them in the same email, below.

Then read your policy wording. Some policies set conditions that apply for the whole term. Ask your broker what yours says. Page 7 covers what's changing with AI.



THIS WEEK

What to send your IT provider

Copy this into an email:

Before our cyber insurance renewal, could you send us the following in writing?

1. A list of any accounts without multi-factor sign-in, split into email, remote access and administrator accounts.
2. Where our offline backup copy is kept, how often it's made and the date and result of the last test restore.
3. What you're responsible for on IT security, so we can answer the insurer's question about who owns it.
4. Your answers to the other security questions on the form. I've attached last year's application.

AI AND YOUR RENEWAL

What AI means for your renewal

The cyber forms in this guide don't ask about AI. Some policies now mention it.

CYBER INSURANCE

AI fraud: covered by some

Some cyber insurers now say in writing that they cover fraud that uses AI, such as a cloned voice or a fake video call asking for a payment.[8] One insurer lists it under funds transfer fraud and social engineering coverage.

OTHER POLICIES

Would your policy pay for an AI mistake?

If someone pastes client files into an AI tool and they leak, the answer depends on your policy wording. In the U.S., more than 60 insurance groups have filed AI exclusions, mostly for general liability and umbrella policies, and some won't use them right away.[9] Sources say they haven't really reached Canadian cyber policies.[9]

PAYMENT FRAUD

AI may make a fake call or email from a client, a supplier or a partner at your firm harder to spot.[7] Ask which part of your policy pays for that fraud, and the limit. Then check that your answer to Question 3 still holds up.

YOUR POLICY WORDING

Ask your broker, in writing, whether any of your policies added or removed anything about AI this year, including professional liability.

HAVE IT READY

In the U.S., a risk control lead at a large broker expects professional liability insurers to ask accounting firms about their AI policies and procedures.[10] Have these answers on one page:

- Which AI tools your staff use
- Who approved them
- What client information goes into them
- Your written rules for using them

Tenom Modern finds the AI tools in use and blocks the ones you haven't approved. That answers the first question and backs up your answer to the second. See page 9.

IF AN ANSWER IS NO

Ask what it would take to fix, whether it's covered by your agreement or billed separately, and whether it can be done before your renewal date. Get the price in writing before you approve it. Tell your broker in writing what's in place now and when the rest will be done, and confirm in writing once it's done, before the policy starts.

KEEP A RECORD

Keep it on one page

Keep the answers with the policy. Here's a filled-in example, including an honest "partly":

Multi-factor sign-in	On for all 31 email accounts, including two shared mailboxes, and for remote access. **Partly** for administrator accounts: two of three have it, and the third is booked for next month. Provider's list checked last week.
Offline backup	A nightly copy to a separate cloud account the office network can't reach. On the form we answered "separate network," not "offline," because that's what it is. Last test restore was last week: the client file folder and one laptop. Both opened.
Banking changes	Confirmed by phone on a number we already have, and a second person approves. Written into our payment procedure.
What we told the broker	*"Administrator accounts: partly. Two of three have multi-factor sign-in, and the third will be done before the renewal date."*

Next year, you'll start the form with these answers already in hand.

NOTES

1. Insurance Journal, "Travelers Wants Out of Contract With Insured That Allegedly Misrepresented MFA Use," July 12, 2022, and follow-up, Aug. 30, 2022. A U.S. case.
2. *Travelers Property Casualty Co. of America v. International Control Services Inc.*, No. 2:22-cv-02145 (C.D. Ill., filed July 6, 2022). A U.S. case.
3. Coalition Insurance Solutions Canada, "Questions for Coalition Cyber Insurance and (Optional) Technology Errors & Omissions Insurance," version 202205; CFC Underwriting, "Cyber Private Enterprise Insurance Application Form, CA," 2024.
4. Canadian Centre for Cyber Security, "Baseline Cyber Security Controls for Small and Medium Organizations," version 1.2, control BC.7.2 and section 3.7, last modified Feb. 18, 2020.
5. CPABC Newsroom, "Reducing cyber risk and responding to breaches: a cybersecurity expert's advice for CPA firms," Sept. 15, 2026.
6. Derek May, HUB International, quoted in "Cyber insurers now demanding firms have MFA, says Canadian broker," IT World Canada, May 7, 2021.
7. Insurance Bureau of Canada, "The Canadian Cyber Insurance Market," October 2026, 16.
8. Coalition Canada, "AI Coverage," accessed Nov. 6, 2026; Insurance Business, "CFC folds cyber, AI wording into financial institutions suite," Sept. 17, 2026.
9. The Insurer, "More than 60 P&C insurance groups file to adopt AI exclusions," July 23, 2026. U.S. filings. Jason Contant, "Cyber insurance's next big surprise?" Canadian Underwriter, Oct. 27, 2026.
10. Chris Gaetano, "Insurers eyeing AI risk at CPA firms," Accounting Today, April 21, 2026. U.S. insurers.

WHERE YOU STAND

Know your answers before you submit

After the call, you get a one-page summary of where your firm stands. This sample is for a fictional firm that isn't a Tenom client.

Sample accounting firm · Renewal readiness

IT ASSESSMENT FINDINGS

Three answers are ready, three need a "partly," one is missing and one we couldn't confirm. Fix the admin account and write the incident plan first.

ON THE FORM	STATUS	WHAT TO DO
Multi-factor sign-in: email	READY	All 31 accounts, including two shared mailboxes
Multi-factor sign-in: remote access	READY	On for all remote access
Multi-factor sign-in: admin accounts	PARTLY	Two of three. Ask your provider to finish the third before renewal
Backups offline or on a separate network	READY	Separate cloud account. Answer "separate network"
Last full restore test	UNKNOWN	No record. Ask your provider for the date and result
Encryption on laptops	PARTLY	Four of 22 laptops aren't encrypted
Confirming banking changes	PARTLY	Staff call back by habit. Write the rule down
Written incident plan	MISSING	Write a one-page plan before renewal

WITH TENOM MODERN Several of these answers are built into Tenom's managed service.

- **Multi-factor sign-in on every account**
- **Encrypted disks, protected and watched 24/7**
- **Mailboxes and files backed up**
- **AI tools found, and unapproved ones blocked**

How your firm confirms a banking change, and your written rules for AI, stay your own.

IF YOU'D LIKE HELP

Get a second set of eyes on your form

Bring last year's application and whatever your provider sends back. If you have an in-house IT lead, bring them too. On a 30-minute call, Tenom will go through each answer with you and mark which are ready, which need a "partly" and what to ask your provider next. This isn't a test of your provider. It puts the answers in your hands before the form arrives. There's no charge for the call or the written findings. Nothing on your systems is changed during the review, and you'll get written findings within five business days. You keep them whether or not you work with Tenom.

tenom.ca/assessment/accounting-finance · 613-319-5043

Book at least three weeks before your renewal date, so there's time to fix a "no" before the policy starts.

SCAN TO BOOK

A Canadian IT company with offices in B.C., Ontario and Manitoba