FUSION COMPUTING FIELD GUIDE

Claude Cowork for accounting firms: secure books, close, and tax work for Canadian CPAs

Mike Pearlstein, CISSP, MSc Computer Science (AI)

Published May 26, 2026; Updated August 12, 2026

WHAT'S INSIDE

TRUSTED BY **Toronto law firms** **Hamilton manufacturers**

Vancouver clinics **GTA accounting firms** **Ontario non-profits**

British Columbia professional services

Accountants are asking whether Claude Cowork can touch client books without putting confidential financial data at risk. According to Statistics Canada, finance and insurance firms lead AI use at 40.4%, with professional, scientific and technical services at 32.4%. These are sector-level figures, not Cowork or firm-level adoption figures. The duty to keep client information confidential stays with the firm.

Mike Pearlstein, CISSP, MSc Computer Science (AI), founder of Fusion Computing, which has secured IT for Canadian accounting and finance firms across Toronto, Hamilton, and Metro Vancouver since 2012.

Key takeaways

- An accounting firm can use Claude Cowork on a Team or Enterprise plan with access scoped to one client folder and a written policy.
- Cowork connects to QuickBooks, so reconciliation and month-end prep are a strong fit. Scope it to one client, not the whole drive.
- Cowork keeps local-session history on the user's own computer, so the firm builds its own record of AI-assisted work. For CPA file documentation and CRA audits, you build that record yourself.
- For this pilot, a designated CPA reviews anything filed. That is a firm control, not a universal CRA rule; CRA authorization requirements such as Form T183 still apply. Never put client tax data on a personal account.

Plan a Safe Cowork Pilot

Can accounting firms use Claude Cowork with client financial data?

Yes, an accounting firm can use Claude Cowork on a Team or Enterprise plan, with access scoped to one client's working folder and a written usage policy. Confidentiality binds the firm, not the software. It is your professional obligation under your provincial CPA code, and the applicable privacy law depends on the engagement and the data flow — PIPEDA where it applies, and provincial private-sector statutes such as BC PIPA. On the business plans, your content is not used to train Anthropic's models by default, which is one reason client work belongs on a business plan and never on a personal account.

The point is that confidentiality is the firm's obligation under the provincial CPA code of professional conduct, and no vendor setting removes it. What a practice controls is the scope: which files the agent opens, which plan governs the data, and who reviews the numbers before filing. On the business tiers, Anthropic's privacy commitments keep that data out of model training.

It's the same secure-adoption logic from the pillar guide on using Claude Cowork securely in your business, applied to a CPA practice, and it sits alongside our broader IT for accounting firms work. The law-firm version of this guide covers the parallel duties for law firms using Cowork.

A registered investment advisory practice should read the Claude Cowork guide for wealth management firms instead, which works through CIRO record-keeping and supervision rather than CPA rules.

A client that is a brokerage, MGA, or lender rather than a CPA practice belongs in the Claude Cowork guide for financial services firms, which covers CIRO bulletin 26-0034 and FSRAO oversight instead of CPA rules.

What does Claude Cowork actually do for an accounting firm?

> Claude Cowork completes multi-step financial work rather than answering a single question. Because Claude for Small Business connects natively to QuickBooks, the workflows to test first are reconciliation, month-end close prep, first-draft financial statements, organizing tax documents, and cleaning up accounts payable and receivable. Each output is a draft for a CPA to verify, not a filing.

Here's how those jobs map to the work, with the guardrail that keeps each one safe. Fusion Computing walks firms through this before any pilot, the same way we scope any AI services engagement.

Book a 30-minute call to scope Claude Cowork for your practice safely →

Task	What to test	The guardrail
QuickBooks reconciliation	Matches transactions and flags discrepancies	Scope to one client; the accountant reviews
Month-end close prep	Reconciles accounts and drafts a plain-English variance summary	One client folder, not the whole drive
First-draft financial statements	Assembles statements from the trial balance and working papers	A CPA reviews and signs; never auto-filed
Tax-document organization	Sorts and renames T-slips, receipts, and source documents	No SIN or tax data on a personal plan
AP and AR cleanup	Deduplicates and categorizes invoices and payments	Treated as a draft for review

Treat these as pilot hypotheses to validate in your own tenant, not vendor-guaranteed capabilities. Anthropic documents a subset of them directly; the rest are workflows to test before a firm relies on them.

How do the confidentiality and client-data guardrails work?

> According to Anthropic's deployment guidance, the core guardrail is least privilege: scope Cowork to one client's working folder, never the whole client drive. Classify what is allowed in (working documents for the active engagement) and what stays out (tax identifiers and client data beyond the scoped folder). Keep a CPA reviewing anything filed. Cowork runs in an isolated environment on Anthropic's servers for remote sessions, or in an isolated virtual machine on the member's device for local sessions, but prompts still reach Anthropic, so scope is one control among several: also disable unneeded web, connector and MCP access, and require approval for consequential write actions.

The first thing I check is scope. When a firm connects the agent to the entire client drive, a single task can read every client's books. Scope it to the active engagement and the file-exposure risk drops sharply, though prompt-injection, connector and web-access risk remain.

> **Field note.** The first thing I change is access. I've seen a bookkeeper point an agent at a drive that held every client's working papers. We scoped it to one engagement folder, and the workflow that felt reckless became routine. The work's identical; the exposure isn't.

The policy is the other half. A short rule set, the kind we cover in our guide on what belongs in an AI acceptable use policy, names the approved tool, the data that may go in, and who may run it. I pair the policy with a technical review so the scope survives contact with a real busy season.

Fusion Computing pairs that policy work with a cybersecurity review so the practice has a defensible position.

The oversight gap for CPA file documentation and CRA audits

> According to Anthropic, Claude Cowork stores local-session conversation history on each user's computer, where it is not subject to Anthropic's standard data retention policies and cannot be centrally managed or exported by admins. Cowork activity is captured in the Compliance API, and Enterprise admins can retrieve local-session content through it in beta. For a CPA firm it matters: file documentation standards and CRA audit trails both assume the firm can reconstruct how a number was reached. Team and Enterprise owners can stream Cowork events to a SIEM through OpenTelemetry, which Anthropic notes does not replace audit logging for compliance. Cowork exports the full text of user prompts by default, along with tool parameters, file paths and user email addresses, so configure filtering or redaction at the collector and set SIEM access and retention before enabling export.

According to Anthropic's guidance on using Cowork on Team and Enterprise plans, the local history "is not subject to Anthropic's standard data retention policies and cannot be centrally managed or exported by admins."

> **Field note.** When I walk a partner through the oversight gap, I open the local Cowork history on the demo machine and ask who else can see it. Nobody can. Few file-documentation procedures contemplate a transcript that lives on one bookkeeper's laptop. CRA requires records detailed enough to recreate the transaction trail from supporting documents through to the summarized accounts, so preserve the AI-assisted working papers the engagement needs.

> *"Partners ask me whether Cowork can run the month-end close. It can draft it. The close still belongs to the CPA who signs it, and the practices that hold that line get the speed without the file-review problem."*
>
> ***Mike Pearlstein**, CISSP, CEO, Fusion Computing*

That doesn't rule Cowork out. It means the firm designs its own record of AI-assisted work.

If the pilot needs centralized monitoring, define the destination, filtering, access and retention before enabling OpenTelemetry. If a working paper could support a filing or a CRA query, the firm keeps that record on purpose.

Plan tier and a setup checklist for an accounting firm

> The plan tier is the first decision: per Anthropic's plan lineup, only Team ($25 USD monthly, $20 USD annual, 2-seat minimum) and Enterprise carry the "not trained on by default" commitment a firm needs. A safe rollout: scope to one client folder, keep "Manually approve" on for client books, write a usage policy, turn on OpenTelemetry monitoring, and have a CPA sign off on filings.

Need the policy first? Use our AI acceptable use policy template.

Cowork runs on Pro, Max, Team, and Enterprise plans per Anthropic's release notes, but only the two business tiers fit client work. Here's the checklist Fusion Computing runs with a firm before the first client file goes near the tool. In our practice the plan-tier fix is the first change we make.

> **Why Canadian firms bring this work to Fusion Computing**
>
> CISSP-led, a Microsoft Solutions Partner and a CompTIA Managed Services Trustmark holder, securing IT for Canadian SMBs across Toronto, Hamilton, and Metro Vancouver since 2012.

1. **Choose Team or Enterprise.** A bookkeeper running client books on a personal account is the first risk to fix.
2. **Scope to one client folder.** Never the whole client drive or every company file. Widen only with a reason.
3. **Default to "Manually approve."** Cowork always asks before deleting files; keep approvals on for client data.
4. **Write an acceptable use policy.** Name the approved tool, the data that may go in, and who may run it.
5. **Turn on OpenTelemetry monitoring only after deciding what may be logged.** It gives the firm a structured visibility stream into what the agent did.
6. **Keep a CPA signing off.** Nothing filed, from statements to returns, ships without review.
7. **Map the terms to your duties.** Check Anthropic's data handling against CPA confidentiality and CRA record-keeping before go-live.

None of it's exotic. The technical setup can be quick; the privacy, logging and approval work is what decides how long the pilot takes.

Fusion Computing sets it up as part of the managed IT work we already do for firms, and the same pattern carries to wealth management firms, real estate brokerages, and healthcare clinics under their own regulators. The review work is CISSP-led at a Microsoft Solutions Partner, the same team that has secured Canadian practices since 2012.

Claude Cowork is worth adopting for the reconciliation and document work that fills a practice. Start with one low-risk workflow. If the controls hold and the numbers are right, expand from there.

Fusion Computing helps Canadian businesses across Toronto and the GTA, Hamilton, and Metro Vancouver with managed IT, cybersecurity, and Microsoft 365.

Frequently Asked Questions

Q. Is Claude Cowork safe for client books? –

Claude Cowork can be safe for client books on a Team or Enterprise plan, with access scoped to one client folder and a CPA reviewing the output. Team and Enterprise do not train on organization content by default, but that alone is not a confidentiality determination: verify the execution mode, Anthropic's current terms and DPA, retention, the applicable privacy law and your professional obligations before client data is used. Cowork sessions run remotely by default on Anthropic's servers. Existing desktop deployments may still run locally, with code in an isolated virtual machine on the member's device. On Team and Enterprise plans, your content is not used to train Anthropic's models by default. Confidentiality stays the firm's duty, so the controls around the tool are what make it safe.

Q. Can Claude Cowork use my QuickBooks? –

Yes. Claude for Small Business, which ships inside Cowork, connects natively to Intuit QuickBooks along with tools like PayPal and Microsoft 365. For a firm that means reconciliation and month-end prep can run against the live books. Scope the connection to one client and keep an accountant reviewing the result before it informs a filing.

Q. Does Claude Cowork breach CPA confidentiality? –

Using Claude Cowork does not breach CPA confidentiality by itself. The risk comes from careless setup. Confidentiality depends on controlling client information, so a firm should run Cowork on a business plan, scope it to one client folder, keep tax identifiers out of unscoped folders, and review anything before filing. The duty sits with the firm, not the tool.

Q. What plan does an accounting firm need for Claude Cowork? –

An accounting firm should use the Team or Enterprise plan, not a personal Pro or Max account. Only the business tiers carry Anthropic's commitment not to train on your content by default, plus the owner and admin controls a firm needs. A bookkeeper running client books on a personal account is the first risk to remediate.

Q. Is client tax data used to train the model? –

On Team and Enterprise plans, your content is not used to train Anthropic's models by default, so client tax data processed under a business plan stays out of training. Personal Pro and Max plans follow individual privacy settings, which differ from the business default. For a CPA firm, that difference is the reason to standardise on a business plan.

Q. How is Claude Cowork different from Intuit Assist or accounting AI? –

Intuit Assist and similar tools are built into specific accounting platforms. Claude Cowork is a general agent that works across your own files and apps on the desktop, and it can connect to QuickBooks through Claude for Small Business. For a firm, the practical differences are where the data lives, the admin and audit controls, and how broadly the agent can reach.

Q. Does Claude Cowork work on Windows or only Mac? –

Claude Cowork works on both macOS and Windows through the Claude desktop app, and it reached general availability on both on April 9, 2026. Cowork is available on paid plans across desktop, web and mobile. Web and mobile remote sessions are in beta and are rolling out gradually across plans, so confirm availability for your plan before launch. Some capabilities, such as computer use, arrived first as research previews, so confirm the current feature list for your platform inside the app.

Q. Who at the firm should run Claude Cowork? –

Start with a small group who understand the engagement and the confidentiality duty, not the whole firm at once. Cowork has an organization-wide enablement switch, and on Enterprise, groups and custom roles can restrict it to selected users or teams while Team remains organization-wide, so a deliberate pilot with named users beats a broad rollout. Pair it with training and a written policy before wider use.

Talk to Fusion

Put this guide to work

Fusion Computing helps Canadian SMBs adopt AI safely. The review work is CISSP-led at a Microsoft Solutions Partner and CompTIA Managed Services Trustmark holder, securing Canadian businesses since 2012.

- Managed IT support with a 1-hour priority response
- Cybersecurity, managed detection and response, and compliance reviews
- AI and Copilot consulting, including safe Claude Cowork pilots
- Microsoft 365 management and licensing

Book a 30-minute scoping call

fusioncomputing.ca/contact-us · 416-566-2845
Toronto · Hamilton · Metro Vancouver