IP Mahir

Governance, risk and compliance

PROTECT FOR PRACTICES

Data privacy for Accounting firms

Protect client financial records and the access you hold to their accounts.

Govern | Manage risk | Prove compliance

DELIVERED ON

METPL.Cloud, our infrastructure branch for data centres and edge infrastructure

First edition · October 2026

https://ipmahir.com/practices

IP MAHIR

Who we are

01

IP Mahir is a team of governance, risk and compliance professionals. We help professional practices protect the information their clients trust them with, and we do it by running the systems that hold that information.

Most practices buy three things separately: privacy and compliance guidance, managed IT, and secure storage. We bring them together in one service for accounting firms in the Lower Mainland, so the privacy rules are built into how your systems are run, not left on paper.

2005
our team has built software and infrastructure since

2022
our focus on infrastructure, through METPL.Cloud

20+
years across technology and law, our lead provider

What we bring

1 **Governance, risk and compliance**

Experience in compliance, and in remediating and mitigating transaction risk, across the team.

2 **IP and data privacy**

A working focus on protecting ownership, records and personal information.

3 **Infrastructure depth**

METPL.Cloud, our infrastructure branch, deals with data centres and edge infrastructure.

4 **Startup and incubator network**

Experience supporting startups across many domains, from first idea to funding-ready.

Led by Govind Preet Singh

A governance, risk and compliance professional with 20+ years across technology and law. Support is delivered by staff based in Canada. Leadership details are on the last page.

WHAT HAS GONE WRONG, AND WHY

Known issues and IT gaps

02

Accounting and tax practices hold SINs, bank details, payroll and tax files, and often act for clients inside CRA and bank portals. Most are small offices with no in-house IT.

16%
of Canadian businesses were hit by cyber incidents in 2023

50%
of those reported scams and fraud

13%
of those reported ransomware

Source: Statistics Canada, 2023 survey of businesses.

Known issue	What happened	The IT gap behind it
One in six Canadian businesses was hit 2023 Statistics Canada, Impact of cybercrime on Canadian businesses, 2023	Statistics Canada found that 16% of Canadian businesses were affected by cyber security incidents in 2023. Of those, 50% reported scams and fraud, 31% identity theft and 13% ransomware.	Offices that depend on one or two unmanaged systems have few ways to notice or contain an incident.
Ransomware is the top cybercrime threat October 2024 Canadian Centre for Cyber Security	The Canadian Centre for Cyber Security ranks ransomware as the top cybercrime threat to Canadian organizations in its National Cyber Threat Assessment 2025-2026.	Untested backups and unpatched systems turn one bad click into days of downtime.
Stolen passwords opened tax accounts August 2020 FBC, reporting the CRA's statement	The CRA said credential-stuffing attacks, using passwords stolen from other sites, compromised about 5,500 taxpayer accounts and 9,000 GC Key accounts. It paused My Account, My Business Account and Represent a Client.	Reused passwords and no second step on tax and bank logins.
A professional body's data exposure fed phishing 2020 CPA Practice Advisor	CPA Canada reported that an unauthorized party had exposed contact details of about 329,000 people, and warned that the data could fuel targeted phishing scams.	Staff cannot easily tell a real email from a targeted one, and there is no filtering or reporting routine.
Client access goes stale 2022 CPA Canada	CPA Canada advises firms to set different Represent a Client access levels for staff and to review client lists regularly. The CRA added enhanced security requirements to Represent a Client in 2022.	Shared logins, and no routine review of who can reach which client.

Each issue is quoted from the source shown. We do not claim we would have prevented any of them.

GOOGLE DRIVE, AWS AND OTHER CLOUD HOSTING

Why not a shared drive?

03

Google Drive and similar shared drives, and cloud hosting such as AWS, are useful tools. They are not, on their own, a data-security plan: the provider secures its platform, and your practice stays responsible for who can reach the files, how they are set up and where the law can reach them.

The problem	What the sources say	The privacy problem
Hosting is not the same as securing your data AWS shared responsibility model	AWS's own shared responsibility model says customers manage their data, including encryption options, classify their assets and use access tools to set permissions, and configure the firewall and security groups. AWS secures the platform; you secure what you put on it.	A practice that "moves to AWS" without someone running these settings has bought hosting, not security.
One wrong storage setting can expose a whole record set UpGuard on a misconfigured medical-billing bucket	Security researchers have repeatedly found healthcare, billing and personal records sitting in publicly reachable Amazon S3 storage, including a medical billing vendor's treatment notes and a senior-care ratings site's files covering the US and Canada, left open with no password until researchers reported them.	Data-privacy harm caused by a configuration gap, not by a hacker breaking in.
"Anyone with the link" stays open Malwarebytes, August 2026	Google Drive links set to "Anyone with the link" can be opened without signing in. Malwarebytes reported a Drive left open this way for about six years, exposing personal data of 935,779 people, and found that Google Search can index such documents once the link is discoverable. A 2023 scan by Metomic of about 6.5 million Drive files found 40.2% contained sensitive data.	Convenience sharing that nobody reviews turns into permanent exposure.
Where the provider is based can matter more than where the data sits Balsillie Papers, Whose Law Governs Canadian Data?	Legal commentary on the US CLOUD Act notes that a US provider can be compelled to produce data it controls regardless of where in the world the data is stored, and that storing data in Canada does not by itself remove that exposure.	Client confidences held by a US-based provider may be reachable by foreign legal process, which a practice rarely considers when it picks a tool.
Outsourcing storage brings obligations in BC IAPP, Canadians and US cloud services	An IAPP summary notes that PIPA imposes notice and policy requirements when data storage is outsourced outside Canada. Regulators also expect you to ask: the Law Society of BC points lawyers to a Cloud Computing Checklist, and CPABC advises accountants to confirm that software and service providers meet the Code and privacy law.	A practice that cannot show it asked these questions has no evidence of reasonable safeguards.

Our answer

Our answer is not "never use the cloud". It is to keep your client data stored and managed in BC, give each person access by role, test your backups, approve every change before it reaches you, and use a cloud tool only where it fits, set up and watched by someone accountable.

WHAT HAPPENS WHEN SOMETHING FAILS

Your SaaS tools and outages

04

Software-as-a-service tools only work when your internet link, router, power, devices, the vendor and the cloud region behind it all work at once. If one fails, the practice either keeps working or stops, and that depends on what is set up in your office.

Cloud tools in your profession

86% cloud accounting software penetration among Canadian accounting and bookkeeping practices, per a 2025 Xero survey of 250 practices (a vendor survey). Xero, State of the Industry Canada 2025

Examples of widely used products: QuickBooks Online, Xero, TaxCycle, Dext, Karbon. Named as examples only, not an endorsement.

How far one failure can reach	What happened	Source
Rogers outage, July 2022	More than 12 million customers lost wireless and wireline service for about a day. Small businesses were among the hardest hit and could not process debit card payments. A report for the CRTC attributed the outage to a router configuration error during a network upgrade.	Global News, on the CRTC-commissioned report
AWS outage, October 2025	A DNS failure for a core database service in AWS's US-East-1 region spread to many dependent services and took down popular apps worldwide, including Slack and Atlassian, for hours.	ThousandEyes outage analysis

When the network or a vendor fails, your local setup decides what happens next.

If this happens	What a local setup does
The internet link drops	A second connection or a local fall-back lets staff keep working on the office network, print and reach local files while the line is fixed.
A vendor or cloud region goes down	A downtime plan and a local copy of today's schedule and key records mean the practice does not depend on a single vendor being up.
The local network fails	A documented spare and a tested swap turn a dead switch into a short job, not a lost day.
The power goes	Battery backup and a clean shutdown protect the systems that hold your records.
Access breaks quietly	Monitoring catches an expired certificate, a bad DNS setting or a firewall change before staff and clients do.

SECTIONS THAT APPLY TO YOUR PRACTICE

The rules, and how we meet them

05

Requirement	What it requires	How our service supports it
BC PIPA, s. 4 **Responsibility and reasonableness** Personal Information Protection Act (BC Laws)	An organization is responsible for the personal information under its control, must designate someone responsible for compliance and make that person's position title and contact details public, and must act as a reasonable person would consider appropriate in the circumstances.	The privacy pack names the responsible person and the public contact line, and records your decisions. The quarterly evidence report shows what reasonable looked like each quarter.
BC PIPA, s. 5 **Policies and practices** Personal Information Protection Act (BC Laws)	An organization must develop and follow policies and practices that meet its obligations, set up a way to handle complaints, and make that information available.	The privacy pack gives you policy templates, a complaint process and a breach-response plan, reviewed each year.
BC PIPA, s. 23 **Requests for your own information** Personal Information Protection Act (BC Laws)	A person may ask for their personal information and how it has been used or disclosed, and the organization must respond within the time limits.	Records are organized by person or matter, with access logs, so you can find what you hold and show who saw it.
BC PIPA, s. 34 **Protecting personal information** Personal Information Protection Act (BC Laws)	An organization must protect personal information in its custody or control with reasonable security arrangements against unauthorized access, collection, use, disclosure, copying, modification or disposal.	Access by role, approved changes, monitoring, tested backups and recovery, and data stored and managed in BC are the core of the service.
BC PIPA, s. 35 **Keeping and destroying information** Personal Information Protection Act (BC Laws)	Information used to make a decision about a person must be kept for at least a year afterwards. Once information is no longer needed for a legal or business purpose it must be destroyed or made anonymous.	A retention schedule and secure disposal routine, including erasing retired devices, are part of the privacy pack.
CPABC Code of Professional Conduct, Rule 208 **Confidentiality** CPABC client privacy guidance	Registrants must keep client information confidential. CPABC advises firms to confirm that software and service providers meet the Code and privacy law.	We record where each client file lives and which provider holds it, restrict access by role, and review provider settings.
CRA Represent a Client **Access to client tax accounts** CPA Canada, best practices for electronic filing	The CRA added enhanced security requirements to Represent a Client in 2022. CPA Canada advises setting different access levels for staff and reviewing client lists regularly.	Unique credentials, a second login step and a routine access review for CRA and bank portals.

Plain-language summaries of the rules, not legal advice and not the full wording. Read the section itself through the link, and ask your own advisor how it applies to you. Our service supports your obligations; it does not guarantee compliance.

SET UP AROUND YOUR PRACTICE

How we help

06

What you protect

- Tax, payroll and bookkeeping records
- SINs, bank and account details
- Access to client accounts, such as CRA portals

What we do for your practice

- **Role-based access, including CRA and bank portals**
- **Safe handling of SINs, bank details and client files**
- **Protection against stolen passwords and phishing**
- **A response plan, and quarterly evidence of what was protected**

Five questions to ask any IT provider, drive or host

- Who can see each folder, and when was that last reviewed?
- Is “Anyone with the link” sharing switched off for client files?
- When did you last restore a backup as a test, and how long did it take?
- Where does our data physically sit, and which country’s law can reach it?
- Who approves a change before it reaches our systems?

Public cloud, again

Google Drive, AWS and other public clouds secure their platform. They do not set up, watch or take responsibility for your practice’s access, settings and legal exposure.

GOVERN. MANAGE RISK. PROVE COMPLIANCE.

Our approach and service

07

Our approach

Govern

Clear ownership and written rules.

- Policies and a privacy-ready records approach
- Named responsibility for privacy
- Access by role, reviewed regularly

Manage risk

Know where the exposure is, and shrink it.

- A short, honest risk and privacy review
- Monitoring, patching and tested recovery
- A response plan for when something goes wrong

Prove compliance

Evidence you can show when asked.

- Logs and records that stand up to questions
- A quarterly evidence report
- Support for your regulator and insurer requests

What every practice receives

Managed systems and updates
Every change is tested and approved before it reaches your practice.

Access and identity
The right people see the right records, and access ends when staff leave.

Monitoring and response
Problems are caught early, and incidents are contained and reported.

Backup and recovery
Recovery is planned and tested, not assumed.

Privacy pack
Policies, a breach-response plan and an annual review for your practice.

Evidence reporting
A short quarterly report of what changed, what was found and what was fixed.

Secure storage in BC
Client data stored and managed in British Columbia.

Canada-based support
Support delivered by staff based in Canada.

HOW WE ARE DIFFERENT

Why IP Mahir

08

Established IT providers in the Lower Mainland do good work on help desks, uptime and Microsoft 365. We start from a different question: **can you show that your clients' information was reasonably protected?** Everything we run is built to answer it.

	Typical IT support	IP Mahir, Protect for Practices
Where it starts	Tickets and uptime	A privacy and risk review of your practice
Led by	Technicians	A governance, risk and compliance professional
Your data	Wherever the tools put it	Stored and managed in BC
Changes	On the vendor's schedule	Approved before they reach your practice
Evidence	On request, if available	A quarterly evidence report as standard
If the internet drops	Work often stops	Designed so the practice keeps working
Public cloud alone	The provider secures its platform; your settings and access are yours	We set up and watch your settings, access and where data sits
Support	Location varies	Delivered by staff based in Canada

What you can expect from us

1 Plain language

We explain risk and controls in terms a practice owner can act on.

2 No surprises

Nothing changes on your systems until it has been tested and approved.

3 Straight answers

We say what we can and cannot do, and we do not overpromise.

What we are not

We provide governance, risk and compliance services. We do not give legal advice. Where a question needs legal advice, we work alongside your own advisors.

A LOW-RISK FIRST STEP

How we start

09

We do not ask you to change everything at once. We begin by learning your practice, show you what we find, and prove the approach on a small scale before you commit to a service.

1
review before you commit to anything

2
pilot on your own software, on a few workstations

0
changes without your approval

1 Review
A short privacy and risk readiness review of your practice.

→

2 Plan
A clear plan and scope, in plain language.

→

3 Pilot
A trial on a few workstations, with your own software.

→

4 Run
Managed service begins, with quarterly evidence reports.

What happens at the review

1 We look
Where client information is kept, who can reach it, and what happens if something fails.

2 We report
A short findings report with the biggest risks first.

3 You decide
You choose whether to go ahead. The findings are yours either way.

If your software needs something different

Some practices rely on software with specific requirements, such as a clinical system or a practice-management tool. We test your actual software during the pilot, and we plan for anything that needs a different approach before changing anything.

WHO YOU WORK WITH

Leadership and infrastructure

10

Govind Preet Singh, lead service provider

A governance, risk and compliance professional with 20+ years across technology and law. He has worked in technology, compliance and advisory roles in Canada and India, and advises university incubation programs on intellectual property and startups.

Background	
Education	Bachelor in Computing Science, Thompson Rivers University (2010). Computer programming diplomas, Georgian College (2005 to 2006).
Canada, 2010 to 2017	Senior Legal Compliance Specialist, SAP Canada Inc., Global Technology Legal Compliance: software IP and licensing, open-source governance, product compliance, and technology due diligence.
British Columbia	Founder and principal, ShaSun Investments Corp., a real-estate investment company that grew from initial operations in British Columbia.
Advisory	Empanelled advisor on IP, startups and incubation for university incubation programs (IKGPTU, CGC University). Executive mandates across edge, data-centre and AI infrastructure.

Infrastructure: METPL.Cloud

METPL.Cloud

IP Mahir's infrastructure branch. METPL.Cloud deals with data centres and edge infrastructure: the secure storage and computing that sit behind the service.

Start with a conversation

Tell us about your practice. We reply with a clear next step.

Web
https://ipmahir.com

Phone
+1 (604) 698-6978

Contact form
ipmahir.com/contact

Lower Mainland, British Columbia

IP Mahir provides governance, risk and compliance services. It does not provide legal advice. This brochure is a summary; the terms of any service are set out in the service agreement.

PAGES RELEVANT TO YOUR PRACTICE

Direct links

11

Every link below is clickable in this PDF and goes straight to the page for accounting firms.

Page	Why it helps	Link
On ipmahir.com		
Accounting firms page	Known issues, rules and the slideshow for accounting firms	https://ipmahir.com/practices/accounting
All BC practices	The other professions we serve, and every brochure	https://ipmahir.com/practices
Start a conversation	Tell us about your practice; we reply with a clear next step	https://ipmahir.com/contact
Rules and regulators		
Personal Information Protection Act (BC Laws)	BC PIPA, s. 4: Responsibility and reasonableness	bclaws.gov.bc.ca/civix/document/id/complete/s...
CPABC client privacy guidance	CPABC Code of Professional Conduct, Rule 208: Confidentiality	bccpa.ca/kbase/kbase-search/practice-manageme...
CPA Canada, best practices for electronic filing	CRA Represent a Client: Access to client tax accounts	cpacanada.ca/news/accounting/tax/best-practic...
Infrastructure and company		
METPL.Cloud	Our infrastructure branch: data centres and edge infrastructure	https://metpl.cloud
Mahir Evolving Technologies	The company behind IP Mahir and METPL.Cloud	https://mahirevolvingtechnologies.com

Links to outside sites open pages we do not control; their content may change.

BEHIND THE ISSUES IN THIS BROCHURE

Sources

12

These are the public pages behind each known issue and each shared-drive or cloud-hosting risk in this brochure, so you can read them yourself.

Source	What it supports	Link
Known issues		
Statistics Canada, Impact of cybercrime on Canadian businesses, 2023	One in six Canadian businesses was hit	www150.statcan.gc.ca/n1/daily-quotidien/24102...
Canadian Centre for Cyber Security	Ransomware is the top cybercrime threat	cyber.gc.ca/en/guidance/national-cyber-threat...
FBC, reporting the CRA's statement	Stolen passwords opened tax accounts	fbc.ca/blog/cra-shuts-down-online-services-af...
CPA Practice Advisor	A professional body's data exposure fed phishing	cpapracticeadvisor.com/2020/06/05/cpa-canada-...
Shared drives and cloud hosting		
AWS shared responsibility model	Hosting is not the same as securing your data	aws.amazon.com/compliance/shared-responsibili...
UpGuard on a misconfigured medical-billing bucket	One wrong storage setting can expose a whole record set	upguard.com/breaches/data-leak-hipaa-medico-s3
Malwarebytes, August 2026	"Anyone with the link" stays open	malwarebytes.com/blog/news/2026/08/be-careful...
Balsillie Papers, Whose Law Governs Canadian Data?	Where the provider is based can matter more than where the data sits	balsilliepapers.ca/wp-content/uploads/2026/03...
IAPP, Canadians and US cloud services	Outsourcing storage brings obligations in BC	iapp.org/news/a/canadians-and-us-cloud-servic...