BreachGuard

AN ALECTECH PRODUCT

AlecTech

A 12-MINUTE SELF-ASSESSMENT

The Canadian privacy breach *readiness checklist.*

Eighty-five questions across eight domains — governance, intake, RROSH, notification, evidence, and everything in between. An honest self-assessment, designed by AlecTech for Privacy Officers, CISOs, and legal counsel at Canadian organizations.

VERSION 1.0

April
2026

INSIDE THIS CHECKLIST

What you'll *find here.*

BEFORE YOU BEGIN

This isn't a certification. It's a mirror.

Every Canadian organization that collects personal information will, at some point, face a privacy breach. The only question is whether your organization is ready. Answer these questions honestly — the value is in finding gaps, not in scoring well. Most organizations doing this for the first time find more gaps than they expected. That's normal. That's the point.

00 · ORIENTATION

How to *use this* checklist.

This is a structured self-assessment across eight domains, mirroring the lifecycle of a Canadian privacy incident response program. Work through it alone, or — better — with your Privacy Officer, CISO, and in-house counsel in the same room.

Three rules for getting value from this

1. Answer honestly. The only wrong answer is a yes that isn't actually true. An unchecked box is useful data; a falsely-checked box is a future surprise when a regulator asks for proof.

2. Treat "no" as information, not failure. Every unchecked item is a specific thing you now know to improve. That's worth more than a perfect score.

3. Bring the right people. Governance items are for leadership. Intake and triage for the Privacy Officer. Technical controls for the CISO. Evidence and retention for legal. Nobody on their own has the full picture.

THE 85-QUESTION TOTAL

Tally your "yes" answers across all eight domains.

At the end, a scoring rubric on page 22 will help you categorize your program's readiness (Strong, Solid, At Risk, or High Risk) and prioritize remediation. We've included a suggested order for fixing gaps when you can't fix everything at once.

What this is not

This is not legal advice. It doesn't replace a gap assessment by qualified privacy counsel, and it doesn't certify compliance with any specific framework. It's a starting point — the kind of self-assessment a mature privacy program would be running

internally every quarter. If you're at the beginning of your program journey, this will tell you where to focus. If you're mature, it'll tell you what's drifted.

The references to PIPEDA, PIPA, HIA, PHIPA, Law 25, POPA, and the provincial and territorial statutes reflect AlecTech's good-faith interpretation as of April 2026. Privacy law is moving fast in Canada — always consult qualified counsel for obligations specific to your organization.

01 · ORIENTATION

The Canadian privacy landscape, *at a glance.*

Before working through the checklist, know which frameworks apply to you. Most Canadian organizations are subject to more than one. Where multiple frameworks apply, the strictest rule controls.

Federal

PIPEDA **Privacy Act**

PIPEDA covers private-sector businesses engaged in commercial activity, federally-regulated works (banks, telecoms, interprovincial transport, airlines), and any organization transferring personal information across borders. **The Privacy Act** covers federal government institutions.

Provincial private sector — *substantially similar to PIPEDA*

PIPA Alberta | **PIPA** British Columbia | **Law 25** Québec

Québec's Law 25 carries penalties up to **4% of global revenue or $25M**, whichever is higher — the most aggressive in Canada.

Health information

HIA Alberta | **PHIPA** Ontario | **PHIPAA** New Brunswick | **PHIA** Manitoba

HIPA Saskatchewan | **PHIA** Nova Scotia | **PHIA** Newfoundland & Labrador

Public sector — *provincial & territorial*

POPA Alberta | **FIPPA** ON · BC · MB | **FOIP** Saskatchewan | **RTIPPA** New Brunswick

FOIPOP Nova Scotia | **FOIPP** PEI | **ATIPPA / ATIPP** NL · YT · NT · NU

A PRACTICAL NOTE ON ALBERTA POPA

The Privacy Management Program deadline is June 11, 2026.

If you are a public body in Alberta, POPA replaces FOIP and requires every institution to stand up a documented Privacy Management Program by the deadline. If you haven't started, this checklist is a fast way to see where you are.

THE STRICTEST-RULE PRINCIPLE

When multiple frameworks apply, follow the strictest.

A healthcare provider in Alberta is subject to HIA (for health data), PIPA Alberta (for other personal information), and may be subject to PIPEDA for cross-border data flows. Each framework imposes its own notification triggers, timelines, and record-keeping duties. You are responsible for satisfying all of them.

DOMAIN 01 · THE FOUNDATION

Governance & *accountability.*

01

The foundation of a defensible breach response program is clear accountability. Regulators want to know who owns this — *and that the owner has real authority.*

DOMAIN 01

Governance & *accountability.*

The most common failure mode in Canadian privacy breach response is not technical — it's structural. A Privacy Officer without authority, or a policy that no one has read.

- [ ] We have designated a **Privacy Officer** with documented authority to lead breach response.
- [ ] The Privacy Officer's contact information is **published internally** and known to staff who might discover an incident.
- [ ] The Privacy Officer has a **direct reporting line** to executive leadership that does not require intermediary approval.
- [ ] We maintain a written **privacy breach response policy**, reviewed within the last 12 months.
- [ ] Our breach response policy **explicitly identifies** which Canadian privacy frameworks apply to our organization.
- [ ] Executive leadership has *read and formally approved* the breach response policy.
- [ ] The Board of Directors (or equivalent) receives a **quarterly report** on privacy incidents and remediation status.
- [ ] We have a documented **escalation path** for breaches likely to trigger regulator notification, including pre-identified external counsel.

For Alberta POPA public bodies specifically

- [ ] We have a **Privacy Management Program (PMP)** that satisfies the POPA Ministerial Regulation requirements by *June 11, 2026*.

- [ ] Our PMP **designates a Privacy Officer**, establishes internal policies, sets a security classification system, mandates training, and defines periodic review timelines.
- [ ] We have documented **PIA procedures** for new or substantially changed programs involving personal information.

DOMAIN 02 · KNOW YOUR HOLDINGS

Data inventory & *classification.*

02

You cannot protect what you do not know you have. Defensible breach response starts with understanding the personal information your organization actually holds — ***where it lives, and who can reach it.***

DOMAIN 02

Data inventory & *classification.*

If your first response to a breach is "where would that data even live?" — you have a gap here.

- [ ] We maintain a **current inventory** of personal information holdings across all business units and systems.
- [ ] The inventory identifies **data types, volumes, systems of record, processors, and retention periods**.
- [ ] We have **classified personal information by sensitivity** — at minimum: sensitive, standard, public.
- [ ] **Health information, financial information, and SINs** are specifically flagged as high-sensitivity data types.
- [ ] The inventory identifies **cross-border data flows**, including processors outside Canada.
- [ ] We document the **legal basis** for each material collection of personal information.
- [ ] **Data processor agreements** exist for every third party handling our personal information, with breach notification obligations to us.
- [ ] The inventory is *reviewed annually* and after any material system or process change.

WHY THIS MATTERS

When a breach happens, you have 72 hours to understand scope.

Organizations without a current inventory spend the first two days of a breach *figuring out what was affected*. That's time you don't have. A good inventory turns the first meeting into "here's what was compromised" rather than "let's find out."

DOMAIN 03 · THE FRONT DOOR

Detection & *intake.*

03

Most breaches are discovered by people, not systems — a staff member, a customer, an external researcher. Your intake process must be designed for ***them.***

DOMAIN 03

Detection & *intake.*

A breach response program is only as fast as its front door. Friction here means breaches go unreported — or, worse, get triaged by someone unqualified.

- [ ] **Any employee** can report a suspected privacy incident through a clear, documented channel.
- [ ] The reporting process *does not* require technical knowledge of what constitutes a "breach" — the Privacy Office makes that determination.
- [ ] We capture a **structured record at intake**: incident category, data types involved, affected population, containment status, narrative description.
- [ ] Our security operations center has a **documented hand-off** to the Privacy Office when security events may have privacy implications.
- [ ] External parties (customers, researchers, regulators) have a **published means** to report concerns to us.
- [ ] The intake channel is monitored during business hours with a **documented after-hours escalation path**.
- [ ] We **preserve evidence at intake** — device images, logs, affected records — before remediation begins.
- [ ] Reporters of potential incidents receive *acknowledgement within one business day*.

DOMAIN 04 · THE FIRST JUDGMENT

Triage & *classification.*

04

Not every security event is a privacy incident. Not every privacy incident meets the threshold for notification. Getting triage right is where most programs ***succeed or fail.***

DOMAIN 04

Triage *& classification.*

The SLA clock starts here. Get this right and you have time to breathe. Get it wrong and you're already late.

- [ ] Within **24 hours of intake**, every reported incident is triaged by a named Privacy Office staff member.
- [ ] Triage assigns a **priority** (low, medium, high, critical) based on documented criteria.
- [ ] Triage identifies **which regulatory frameworks** apply to the incident.
- [ ] An **SLA clock starts** at triage acceptance, tied to the applicable framework's notification timelines.
- [ ] Triage decisions are captured in writing, with *named decision-maker, timestamp, and rationale*.
- [ ] We distinguish between a **security event**, a **breach of safeguards**, and a **privacy breach** — and route each appropriately.
- [ ] Where AI or automated tools assist with classification, results are treated as *suggestions requiring human review* — not determinations.
- [ ] Escalation from triage to full investigation happens **within 72 hours** for high and critical incidents.

DOMAIN 05 · THE CRITICAL JUDGMENT

The RROSH *assessment.*

05

PIPEDA, PIPA Alberta, HIA, and Québec Law 25 all turn on the same determination: ***is there a real risk of significant harm?*** This is the most consequential judgment in Canadian privacy law.

DOMAIN 05 · THE CRITICAL JUDGMENT

Real Risk of *Significant Harm*.

Get it wrong one way, you underreport and face penalties. Get it wrong the other way, you overreport and erode trust. Most organizations get it wrong because they don't have a methodology — just instinct.

- [ ] We have a documented **methodology** for assessing RROSH that goes beyond gut-check judgment.
- [ ] The methodology considers, at minimum: **data sensitivity, probability of harm, affected population, containment**.
- [ ] Each factor is **weighted**, and the weights are documented and approved.
- [ ] The assessment produces a *reproducible score or threshold determination* — not a narrative conclusion.
- [ ] The assessment considers downstream harms: **identity theft, financial loss, physical safety, reputational harm, employment loss, discrimination, humiliation**.
- [ ] "*Significant harm*" is interpreted consistent with OPC guidance — not narrowly.
- [ ] Every RROSH assessment is documented with **named assessor, factors, score, and narrative**.
- [ ] We have a **separate assessment** for Québec Law 25's "serious risk of harm" threshold, which operates distinct from RROSH.
- [ ] For health information breaches, we apply the **heightened sensitivity** treatment the applicable health privacy legislation requires.
- [ ] RROSH assessments are *reviewed by the Privacy Officer* before any regulator notification decision.

A NOTE FROM THE FIELD

Regulators don't second-guess conclusions. They second-guess methods.

Two organizations with the same breach can reach opposite RROSH conclusions and both survive investigation — if their methods were documented, weighted, and applied consistently. An undocumented gut-call, even if technically correct, often doesn't. The lesson: *the method matters more than the answer.*

DOMAIN 06 · THE PUBLIC-FACING WORK

Notification.

06

When notification is required, the standard is "***without unreasonable delay.***" Regulators interpret these phrases strictly. Your notifications must be fast, accurate, and auditable.

DOMAIN 06

Notification — regulators first.

The commissioner's inbox is your first reader. Templates, addresses, and approval flows should be ready before a breach, not drafted during one.

- [ ] We have **pre-prepared notification templates** for each regulator with jurisdiction over our organization.
- [ ] The templates capture the **specific elements each regulator requires**: incident description, affected information, risk assessment, remediation, affected population.
- [ ] We have identified the specific **notification addresses, portals, or forms** for each regulator.
- [ ] We maintain **delivery confirmation records** — read receipts, portal confirmations, registered mail receipts.
- [ ] Drafts are *reviewed and approved by a named authority* before transmission, with drafter and approver logged separately.
- [ ] **French translation** is available for notifications to the Commission d'accès à l'information du Québec.
- [ ] For health breaches requiring multi-party notification, we have separate templates for **privacy commissioner, affected individuals, and professional regulatory bodies**.

Notification — individuals next.

When you write to an affected individual, you are writing to someone who just learned something unsettling about your organization. Plain language, clarity, and usefulness beat corporate formality every time.

- [ ] Our notification uses **plain language** understandable to a non-specialist.
- [ ] The notification **describes the incident**, the information involved, and the potential consequences.
- [ ] The notification **describes remediation** we have taken and recommends steps the individual can take.
- [ ] The notification identifies a **contact** — name and reachable channel — for questions.
- [ ] We have a **mass-notification plan** accounting for reachability: we know the ratio of current versus stale contact information.
- [ ] We **track notification delivery**: sent, bounced, opened where possible, responded.
- [ ] For very large breaches, we have assessed **substitute notification strategies** (press release, website posting) where direct notification is impracticable.

DOMAIN 07 · CLOSE THE LOOP

Remediation & *lessons learned.*

07

A regulator closes a file when they are satisfied the underlying issue is ***fixed*** — not when notification is complete. Remediation is where most programs lose momentum after the crisis.

DOMAIN 07

Remediation & *lessons learned*.

The second a regulator hears you made "policy changes," they want the policy — with a before-and-after diff. Vague remediation is almost worse than no remediation.

- [ ] Every confirmed breach generates one or more **remediation tasks with named owners and due dates**.
- [ ] Remediation tasks are **tracked in a system** that flags overdue items to the Privacy Officer.
- [ ] Common remediation types — policy review, targeted training, access control change, technical control strengthening — have **templated task definitions**.
- [ ] We conduct a **lessons-learned review** within 30 days of every material breach.
- [ ] Lessons-learned findings *feed back into* our policies, training, and technical controls.
- [ ] **Remediation evidence** — updated policies, training rosters, change records, technical verification — is preserved and linked to the parent incident.
- [ ] The Board receives a summary of significant remediation actions **quarterly**.
- [ ] We can demonstrate, for *any historical breach*, that remediation was completed and verified.

DOMAIN 08 · THE RECORD THAT SURVIVES

Evidence, audit & *retention.*

08

The single characteristic that distinguishes a defensible program from a vulnerable one is the quality of the record. *Every action, every decision, every approval — timestamped, attributable, retained.*

DOMAIN 08

Evidence, audit & *retention.*

This is the domain that saves you — or sinks you — during a regulator investigation. A strong record shortens investigations. A weak record prolongs them and invites scope expansion.

- [ ] We maintain a **breach register** for all incidents, regardless of whether they triggered notification.
- [ ] PIPEDA-regulated organizations retain breach records for **at least 24 months**.
- [ ] Health-information custodians retain breach records for **10 years**, consistent with health privacy legislation.
- [ ] Our breach records are **immutable** — edits are captured as amendments, not overwrites.
- [ ] Every action on a breach record (create, modify, approve, export) is *logged with actor and timestamp*.
- [ ] **Access to breach records is role-controlled**: reporters, investigators, privacy officers, and leadership see what they need, and no more.
- [ ] We can produce, on demand, a **complete evidentiary package** for any historical breach.
- [ ] Annual compliance reporting is *generated from the breach register* — not reconstructed manually.
- [ ] Data subject access requests can be fulfilled **without compromising the integrity** of the record.

SCORING

What your *score means.*

Tally your "yes" answers across all eight domains. Out of **85 possible**, where does your program land?

SCORE	READINESS	WHAT IT MEANS
75+	**Strong**	Your program meets or exceeds the requirements of Canadian privacy law across the full lifecycle. Focus on continuous improvement, emerging frameworks (CPPA, modernized health privacy), and keeping pace with regulator guidance.
60 – 74	**Solid**	Your program is defensible but has identified gaps. Prioritize the domains with the lowest scores — RROSH methodology and evidence retention, if those are weak.
45 – 59	**At risk**	A real breach would expose documented gaps. Urgent focus needed on governance, intake, and record-keeping. Consider an external program assessment.
< 45	**High risk**	Your program would not withstand a regulator investigation. This is the most common starting point — the good news is that it's also the most improvable. Treat remediation as urgent.

PRIORITIZATION

When you can't fix *everything at once.*

Most organizations will find gaps in more than one domain. When resources are constrained, the correct prioritization is:

01 Governance & accountability

Without a named Privacy Officer with real authority, nothing else matters. Fix this first.

02 Evidence & retention

Your current breaches are happening now. If you can't record them properly, you're creating future liability every day.

03 RROSH methodology

The single most consequential judgment in Canadian privacy law — and the one most likely to be questioned.

04 Notification readiness

The public-facing mistakes are the most damaging ones. Pre-prepared templates pay for themselves the first time you use them.

05 Everything else

Detection, triage, inventory, remediation — in order of your organization's specific exposure and risk tolerance.

WHERE TO GO FROM HERE

You've found the gaps. *Now what?*

If this assessment surfaced gaps, you are not alone. The vast majority of Canadian organizations operate privacy programs that wouldn't survive scrutiny. The gap is rarely between good programs and great programs — it's between programs that exist on paper and programs that operate in practice.

How BreachGuard closes each domain

BreachGuard is AlecTech's privacy incident management platform, built from the ground up for Canadian organizations. It operationalizes every domain in this checklist:

DOMAIN 01 · GOVERNANCE

Named-role RBAC; Privacy Officer workflows; quarterly board report generator.

DOMAIN 02 · INVENTORY

Data Inventory Kickstart — a two-week structured engagement pairs nicely.

DOMAIN 03 · DETECTION

Structured intake form; AI-assisted classification; SIEM integration.

DOMAIN 04 · TRIAGE

SLA clocks auto-configured by framework; priority scoring; audit trail.

DOMAIN 05 · RROSH

Weighted, configurable RROSH scoring; assessor notes; framework-aware thresholds.

DOMAIN 06 · NOTIFICATION

Jurisdiction-aware templates for every Canadian regulator; approval workflow.

DOMAIN 07 · REMEDIATION

Kanban task board; overdue flagging; lessons-learned template.

DOMAIN 08 · EVIDENCE

Immutable audit log; 10-year retention by default; per-incident evidence export.

BOOK A DEMO

See BreachGuard against your *actual* obligations.

A 30-minute working session with an AlecTech privacy engineer. We'll walk through a real incident end-to-end, configured for your jurisdictions. No slides. No marketing.

✉ breachguard@alectech.ca

☎ +1 (437) 747-0878

CANADIAN-HOSTED · CANADIAN-OWNED · BUILT BY ALECTECH

AlecTech Inc.

CANADIAN MANAGED SECURITY & PRIVACY

FOUNDED	September 2015 — Ontario
HEADQUARTERS	5270 Solar Drive, Unit 11 · Mississauga, ON L4W 0G7
CONTACT	breachguard@alectech.ca · +1 (437) 747-0878
OWNERSHIP	100% Canadian-owned and operated
SERVICES	MSP · MSSP · 24/7 SOC · Managed Detection & Response · Privacy Incident Management · Incident Response

This checklist is provided for informational purposes only and does not constitute legal advice. Readers should consult qualified privacy counsel for obligations specific to their organization and jurisdictions of operation. AlecTech Inc. makes no warranty, express or implied, as to the completeness or current accuracy of the legal references herein. References to PIPEDA, provincial private-sector acts, health privacy statutes, public-sector privacy legislation, and Québec Law 25 reflect AlecTech's good-faith interpretation as of April 2026.