

# Bill 194 Assurance Package

## 3Tenets Consulting Inc.

Cybersecurity, privacy and assurance for public sector organizations across Canada

Available through OECM's Vulnerability Assessment and Penetration Testing Services agreement

Bill 194 changed what your organization has to be able to prove. Not that you intended to protect personal information, but that you tested it, scored it, and wrote it down.

Most organizations meet that demand in fragments: a penetration test one year, a privacy review the next, a framework assessment when the auditor asks. The findings never reference each other. This package replaces the fragments with one engagement built on a single evidence base.

**Built for** school boards, colleges and universities, municipalities, hospitals and health agencies, children's aid societies, provincial agencies and Crown corporations.

**Assessed against** NIST CSF 2.0, CIS Controls v8, NIST AI RMF, OWASP LLM Top 10, MITRE ATT&CK and ATLAS, ISO 27001, PHIPA and FIPPA.

## Four deliverables, one engagement

### 1 Penetration Testing

Manual adversarial testing of the external perimeter, internal network and priority web applications. Logic flaws, access control bypasses and chained exploit paths that scanners do not find.

**You receive:** risk ranked findings mapped to MITRE ATT&CK and OWASP, proof of concept evidence, remediation guidance for the team that has to action it, and one verification retest of critical and high findings.

### 2 Bill 194 Readiness Assessment

Your security program scored against all six NIST CSF 2.0 functions, with every gap traced to a named CIS Controls v8 safeguard. Covers the safeguarding duty, breach assessment and reporting, incident response readiness, and governance ownership.

**You receive:** an overall maturity score with component scores, a severity rated gap register, a remediation roadmap sequenced into quick wins and longer term work, and a summary your board can read.

### 3 Privacy Impact Assessment

A complete written PIA on one priority system, whether that is a core records or case management platform, a student or client information system, an HR system or a newly deployed AI tool. Built to the IPC's guide and containing every element the legislation requires.

**You receive:** the completed PIA, a reusable template configured to your environment, and a working session so your staff can run the next one without us.

### 4 AI Security and Governance

Exploit focused assessment of deployed AI and LLM systems covering prompt injection, data leakage, model misuse and agent risk, paired with a governance review of how AI is approved, procured and overseen.

**You receive:** an inventory of AI systems in use, risk rated findings, and a governance framework covering acceptable use, vendor review and human oversight, positioning you ahead of the AI requirements expected under EDSTA.

**They connect.** Testing runs first and its findings become the evidence base, populating the scoring in the readiness assessment and the safeguards sections of the PIA and AI review. Bought separately, that evidence is gathered and written up four times.

Scope

Test

Score

Document

Readout

Each stage feeds the next. Testing evidence carries into the scoring, and the scoring carries into the written record.

**Scoped before it is quoted.** You receive a written scope and proposed approach before any commitment.

## What you walk away with

### Evidence, not assertion

Safeguards validated by someone trying to defeat them, not confirmed by a questionnaire.

### A score that travels

Assessed to NIST CSF 2.0 with component scores and named improvement areas, so the output carries into your other reporting without being rebuilt.

### A defensible budget ask

Remediation sequenced by risk and cost, giving your funding request an order of operations behind it.

### Capability you keep

A configured PIA template and the training to use it.

## Why it costs less than the parts

### No institutional RFP

Pre competed rates through OECM, with BPS Procurement Directive and trade agreement compliance already established.

### One discovery phase

The saving is structural. Bundling removes duplicated scoping, duplicated documentation and the work of stitching three vendors' outputs into one narrative.

## Also available

Additional privacy impact assessments on further systems

Incident response tabletop exercise

Scheduled advisory days through the year

## Why 3Tenets

Every engagement is senior led. Scoping, testing and reporting are handled by senior, certified consultants, with no junior handoffs.

Canadian consultants holding CISSP, OSCP and equivalent certifications

Delivering to public sector organizations throughout Canada

Proven inside school boards, health agencies and municipal bodies

Reporting built to survive audit and executive challenge

## Book a 30 minute scoping call

We confirm your objectives, outline the right approach and set out clear next steps. No obligation, and a senior consultant responds within one business day.

info@3tenets.ca  
226.790.4225  
3tenets.ca