CLIENT PRACTICUM

Professional Networking Platform — GRC & Compliance Review

Context

A professional networking and community-events platform preparing for growth needed a clear read on its privacy and security posture. The work was carried out as a supervised practicum engagement, scoped and authorized under a defined rules-of-engagement document.

Objective

Establish a defensible baseline across three areas: privacy compliance under Canadian law, a foundation of security policy the platform could operate against, and a compliance scoping position for payment handling.

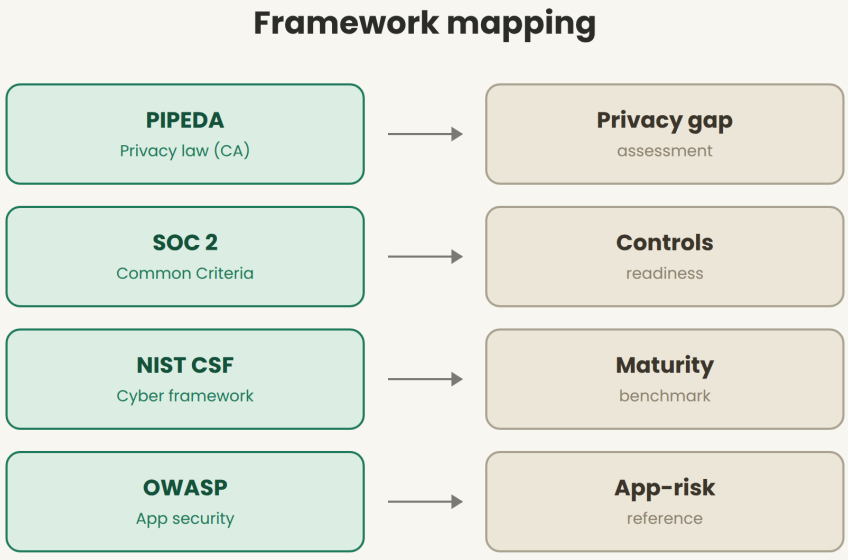
Scope

The engagement was bounded to GRC work — privacy assessment, policy development, and compliance scoping. Authorization was verified before any work began, and specified systems and payment flows were explicitly excluded. Scope boundaries were respected throughout rather than expanded on ambiguous signals.

Approach

Work was sequenced deliberately: a privacy gap assessment first, then controls readiness, then a maturity benchmark. Each area was mapped against an established framework rather than assessed ad hoc, so conclusions traced back to a named standard.

Frameworks



PIPEDA — privacy gap assessment against the fair information principles. SOC 2 Common Criteria — existing and needed controls mapped to the Trust Services Criteria to gauge audit readiness. NIST CSF — an internal maturity

benchmark across the core functions. OWASP — a reference point for application-layer risk informing policy and scope.

Deliverables

A PIPEDA-based privacy gap assessment; a foundational security policy suite; a compliance scoping baseline for payment handling (provisional, pending acquirer confirmation); and a business continuity and disaster recovery plan.

Outcomes

The client received a documented privacy and controls baseline and a policy foundation to build on. Deliverables were reviewed and accepted by the supervising engagement lead. Two follow-on items were identified for the next stage rather than glossed over.

Evidence

- Privacy Gap Assessment (PIPEDA) — v1.0
- Security Policy Suite — v1.0
- PCI DSS Scoping Statement — provisional (pending acquirer confirmation)
- Business Continuity & Disaster Recovery Plan — v1.0
- Framework Mapping Matrix — v1.0

Full artifacts available on request under appropriate confidentiality.

Lessons / Next Stage

An independent review of the policy deliverables caught real corrections before they were finalized. Rather than treat that as a setback, I built the review into the process as a quality-control step — a reminder that GRC deliverables benefit from a second set of eyes. Next stage: complete recovery-test validation, confirm payment scope, and continue the compliance program from PIPEDA gap assessment through SOC 2 readiness.

Related Content

LinkedIn engagement post · Blog: what an external review taught me · Other portfolio projects — see the live case study page at sholahassan.com for links.

Building out a privacy or compliance program?
Let's talk — shola@sholahassan.com