**Compliance Map: Cybersecurity Regulations Impacting Fintesh (Vancouver, Canada)**

This compliance Map is for FinTesh, a premier financial company located in the heart of **Vancouver, BC**. At Fin Tesh, we specialize in providing tailored loan solutions to meet the diverse needs of our clients. Our commitment to excellence and customer satisfaction sets us apart in the financial industry.

**Canadian Federal Regulations**

**1. Personal Information Protection and Electronic Documents Act (PIPEDA)**

**Scope:** Applies to private-sector organizations in Canada that collect, use, or disclose personal information in the course of commercial activity.  
**Cybersecurity Implications:**

* Must implement **reasonable security safeguards** to protect personal data against unauthorized access or loss.
* Requires **breach notification** to affected individuals and the Office of the Privacy Commissioner of Canada (OPC) when a breach poses a real risk of significant harm.
* Fintesh must have a **privacy management program**, including policies, training, and breach response protocols.

**2. Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA)**

**Scope:** Applies to financial services providers to detect and report money laundering and terrorism financing.  
**Cybersecurity Implications:**

* Fintesh must implement **secure systems for transaction monitoring**, **identity verification**, and **reporting suspicious activity** to FINTRAC.
* Enforced access control, **data retention**, and **secure logging/auditing** are critical.
* Cybersecurity must support **data integrity and traceability**.

**3. Bank Act and OSFI Guidelines .**

**Scope:** Since Fintesh is regulated under the Office of the Superintendent of Financial Institutions (OSFI), they must follow these guidelines.  
**Cybersecurity Implications:**

* **OSFI B-13 Guideline** mandates a **Cyber Risk Management Framework**.
* Fintesh must identify, assess, and mitigate cyber risks regularly, and report material incidents.
* Must maintain **incident response and recovery plans**, third-party risk assessments, and **security architecture governance**.

**Provincial Regulations (British Columbia)**

**4. BC Personal Information Protection Act (PIPA)**

**Scope:** Governs how organizations in BC handle personal information.  
**Cybersecurity Implications:**

* Fintesh must ensure personal data is stored and transmitted **securely and with consent**.
* Must employ **physical, administrative, and technical safeguards** to protect customer and employee data.
* Responsible for **third-party data handling security** if outsourcing IT services.

**III. Global and Industry-Specific Standards**

**5. ISO/IEC 27001 (Information Security Management Systems)**

**Scope:** International standard for managing information security.  
**Cybersecurity Implications:**

* Fintesh may pursue ISO 27001 certification to demonstrate **compliance, security maturity, and client trust**.
* Requires establishing a formal **ISMS** with continuous improvement, internal audits, and **risk assessments**.
* Enhances readiness for **regulatory audits and due diligence**.

**6. PCI DSS (Payment Card Industry Data Security Standard)**

**Scope:** Fintesh processes or stores payment card data.  
**Cybersecurity Implications:**

* Must maintain a secure network with **firewalls**, **encryption**, **access controls**, and **logging**.
* Required to conduct **regular vulnerability scans**, **penetration testing**, and **compliance reporting**.

**7. NIST Cybersecurity Framework (CSF)**

**Cybersecurity Implications:**

* Helps Fintesh structure its cyber defenses across **Identify, Protect, Detect, Respond, Recover**.
* Useful for board reporting, aligning controls with **industry-recognized maturity models**, and **gap analysis**.

**8. General Data Protection Regulation (GDPR) *(If serving EU customers)***

**Scope:** Fintesh does not support EU customers and maybe exempt from this.

**Compliance Impact Summary Table**

| **Regulation / Framework** | **Key Impact Areas** | **Required Controls / Practices** |
| --- | --- | --- |
| PIPEDA (Canada) | Personal data protection, breach notification | Access controls, encryption, incident response, training |
| PCMLTFA | AML transaction monitoring | Secure logs, identity verification, audit trails |
| OSFI B-13 | Cyber risk governance | Cybersecurity policies, testing, reporting, recovery plans |
| BC PIPA | Consent, data protection | Safeguards, vendor oversight, breach management |
| ISO 27001 | Security framework, audit readiness | ISMS, documented policies, continuous improvement |
| PCI DSS | Cardholder data security | Network segmentation, logging, vulnerability scans |
| NIST CSF | Cybersecurity program maturity | Baseline assessment, control mapping, reporting |
| GDPR *(if applicable)* | N/A | N/A |