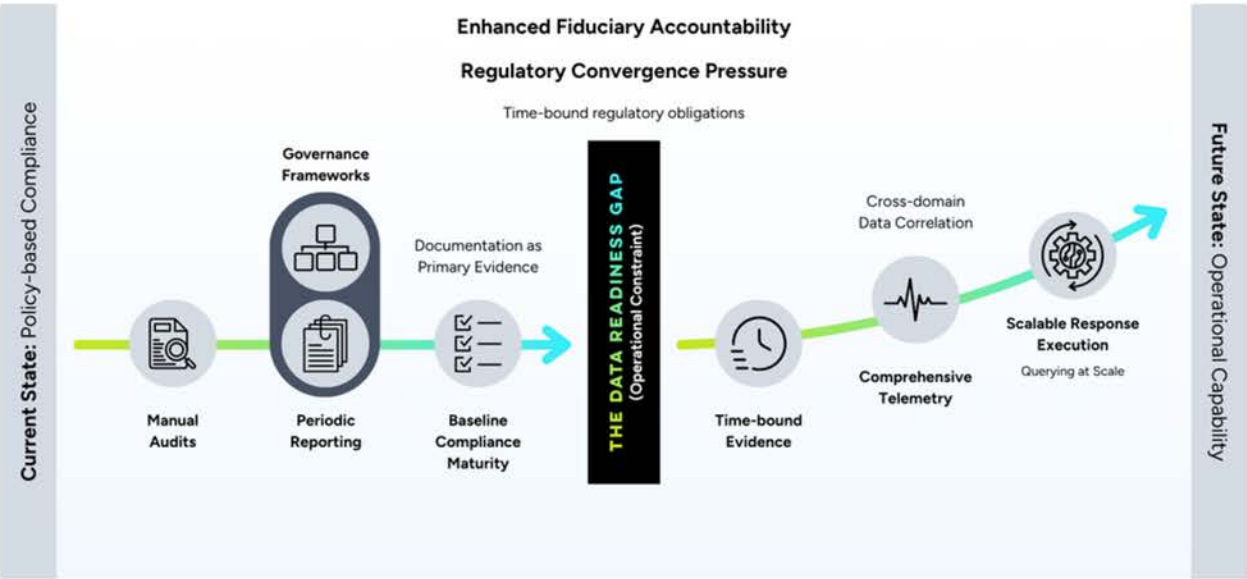
CANADIAN TELECOM REGULATION HAS CROSSED A THRESHOLD

From Compliance Frameworks to Operational Proof

Przemek Tomczak, CPA, CA, CISA
Director of Industry, Partnerships & Alliances



The Operational Maturity Pivot: Strategic Regulatory Transition

EXECUTIVE SUMMARY

The Canadian telecommunications sector is moving beyond policy-based compliance toward a model where operational execution is increasingly central.

Operators are entering a regulatory environment where certain compliance obligations are increasingly time-bound, with expectations measured in minutes or hours rather than months.

With the introduction of **Bill C-22** (which was in its second reading in the House as of March 2026) and the pending **Critical Cyber Systems Protection Act (CCSPA) through Bill C-8** (which passed the House and was under Senate review as of March 2026) the burden of proof is shifting from documented processes to **real-time operational execution**, with many of the specific obligations to be defined through forthcoming regulations.

This shift extends beyond corporate balance sheets. Under the CCSPA, directors and officers may face personal liability if they are found to have directed, authorized, or acquiesced in violation of the Act.

At the same time, evolving **Canadian Radio-television and Telecommunications Commission (CRTC) outage and resilience requirements** are imposing strict, time-bound obligations that require immediate response and auditable evidence.

These forces are converging toward a new regulatory reality: The next generation of compliance risk is less likely to stem from gaps in policy, and more from limitations in the ability to access, correlate, and evidence data at scale and speed.

1. THE THREE PILLARS OF OPERATIONAL ACCOUNTABILITY

The current regulatory shift is defined by three converging forces, each reinforcing the need for **technical execution under real-world conditions.**

Regulatory Convergence Overview

REGULATORY DRIVER	LEGISLATIVE/REGULATORY REQUIREMENTS	OPERATIONAL IMPACT
Bill C-22 (Lawful Access)	Potential regulatory requirements around extracting and delivering transmission data; structured response to judicial orders; metadata retention up to one year	New requirements may necessitate real-time, scalable data retrieval capabilities
Bill C-8 / CCSPA (Cybersecurity)	Mandatory cybersecurity programs; 72-hour incident reporting; supply chain risk controls; binding Cyber Security Directions	Establishes cybersecurity as a **regulated, enforceable operational function**
CRTC (Resilience & Outages)	30-minute notification for 9-1-1 outages; 2-hour reporting for major outages (as defined under CRTC 2025-225 thresholds); 30-day detailed audit reporting.	Requires **immediate visibility and high-fidelity, auditable evidence**

Lawful Access Modernization (Bill C-22)

Bill C-22 represents a structural evolution in lawful access.

- **Mandatory capability:** Regulations may require designated 'core providers' to maintain the ability to extract, organize, and deliver communications and transmission data (scope subject to regulations)
- **Metadata retention:** Regulations may require retention of transmission and location data (potentially up to one year)
- **Structured response:** Processes will be expected to support timely and standardized responses to authorized requests
- **Rapid verification:** Time-sensitive handling of Confirmation of Service Demands (CSDs) is expected under the proposed frameworks, requiring rapid cross-referencing of subscriber and network data
- **Confidentiality obligations:** Requests must be handled without disclosure, which can add operational complexity
- **Security guardrails:** Providers are not required to introduce systemic vulnerabilities, but must still demonstrate capability at scale

Legal Consideration: The proposed framework introduces a lower evidentiary threshold ("reasonable grounds to suspect") for certain subscriber information requests. This has raised potential Charter considerations, particularly in light of Supreme Court decisions such as R. v. Spencer and R. v. Bykovets, and may be subject to future judicial scrutiny.

→ **Implication**

Lawful access is no longer primarily a legal obligation—it is a **performance and data architecture challenge.**

Cybersecurity as a Regulated Capability (Bill C-8 / CCSPA)

The CCSPA would move cybersecurity from best practice to **enforceable regulation.**

- **72-hour reporting requirement** to the Communications Security Establishment (CSE)
- **Mandatory Cyber Security Programs (CSPs)** within defined timelines
- **Supply chain risk mitigation**, including controls over high-risk vendors
- **Binding Cyber Security Directions (CSDs)** with legal force

→ **Implication**

Cybersecurity becomes a **regulated production capability**, requiring demonstrable execution, traceability, and responsiveness.

Cybersecurity as a Regulated Capability (Bill C-8 / CCSPA)

CRTC requirements are already operationalizing compliance expectations:

- **30-minute notification window** for 9-1-1 service outages
- **2-hour reporting window** for major outages (e.g., >600,000 user-minutes)
- **30-day post-incident reporting**, requiring detailed root cause and evidence

→ **Implication**

Resilience is no longer measured by recovery alone—it is measured by **speed, visibility, and auditability of response.**

2. THE HIDDEN CONSTRAINT: DATA ARCHITECTURE

There is a growing disconnect between **regulatory expectations and technical reality.**

Most telecom environments were not designed to support:

- Real-time retrieval across **petabyte-scale datasets**
- Correlation across **network, subscriber, security, and location data**
- Reproducible, auditable responses under regulatory scrutiny

The Structural Gaps

DATA CONSTRAINT	OPERATIONAL IMPACT
The Sampling Trap	Cost-driven sampling creates indefensible blind spots during audits and investigations
Siloed Intelligence	Disconnected systems prevent rapid correlation required for lawful access and cyber response
Query Latency	Traditional architectures struggle to deliver sub-second performance at scale
Retention Constraints	Limited retention windows reduce investigative depth and compliance defensibility

The Core Insight

Emerging regulations increasingly assume timely, reliable access to and retrieval of data across systems, yet most telecom architectures fall short—exposing operators to increasing risk.

3. STRATEGIC IMPERATIVES FOR 2026

To meet these demands, telecom leaders must shift from **governance-led compliance to execution-driven capability.**

Priority Actions

IMPERATIVE	DESCRIPTION
Treat Data as a Regulatory Capability	Elevate data architecture to a core compliance function
Unify Domain Telemetry	Integrate network, subscriber, security, and geospatial data
Eliminate Sampling	Move toward full-fidelity data retention to remove blind spots
Enable High-Speed Access	Ensure seconds-level query performance across large datasets
Design for Auditability	Ensure responses are traceable, reproducible, and defensible
Automate Compliance Workflows	Reduce manual intervention in regulatory response processes

4. ENABLING EXECUTION AT SCALE

Addressing these requirements requires a new class of data capability. Organizations that have successfully adapted—particularly in jurisdictions with mature lawful access and cyber regimes—have invested in platforms designed for:

- Petabyte-scale, full-fidelity data retention
- High-speed analytics across trillions of records
- Cross-domain correlation (network, subscriber, security, geospatial)
- Integrated governance, auditability, and access control
- Deployment models aligned with sovereignty and regulatory constraints
- Response time to requests in seconds versus hours

This is not merely a tooling upgrade; it reflects a broader shift in data architecture needed to support executable compliance. It requires a more integrated data foundation – one that embeds privacy-by-design and aligns with evolving regulations such as Bill C-27 and Quebec's Law 25.

5. THE RISK OF INACTION

The consequences of failing to adapt are material and immediate.

RISK CATEGORY	IMPACT
Regulatory Exposure	The Act introduces significant administrative monetary penalties—up to $15 million per violation for organizations—with continuing non-compliance treated as separate daily violations.
Operational Disruption	Binding directions may require rapid removal of critical infrastructure
Compliance Failure	Inability to meet lawful access or reporting SLAs
Reputational Damage	Public disclosure of outages and cyber incidents erodes trust and valuation

CONCLUSION

Canadian telecom regulation appears to be crossing a significant threshold.

Compliance is increasingly defined not only by policies and frameworks, but by the ability to demonstrate execution in practice. This includes accessing and correlating data at scale, and producing auditable, defensible evidence.

The most successful organizations that succeed will have more than mature governance frameworks. They will have the operational capability to demonstrate compliance under real-world conditions.

REFERENCES

1. Parliament of Canada.
Bill C-8 (45-1): An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts.
https://www.parl.ca/legisinfo/en/bill/45-1/c-8

2. Parliament of Canada.
Bill C-22 (45-1): Lawful Access Act, 2026.
https://www.parl.ca/legisinfo/en/bill/45-1/c-22

3. Canadian Radio-television and Telecommunications Commission (CRTC).
Telecom Decision CRTC 2025-225.
https://crtc.gc.ca/eng/archive/2025/2025-225.htm

4. Canadian Radio-television and Telecommunications Commission (CRTC).
Notification of Major Service Outages.
https://crtc.gc.ca/eng/comm/telecom/notifresilienc.htm

5. Public Safety Canada.
Backgrounder: Supporting Authorized Access to Information Act (Bill C-22 – Part 2).
https://www.canada.ca/en/public-safety-canada/news/2026/03/backgrounder--securing-access-to-information-in-bill-c-22.html