FSRA's new Operational Risk and Resilience Guidance for Ontario insurers

July 09, 2026

On June 8, 2026, the Financial Services Regulatory Authority of Ontario (FSRA) issued its Operational Risk and Resilience Guidance (PC0050APP) for Ontario-incorporated insurance companies and reciprocal insurance exchanges (collectively, Ontario insurers).

The guidance, which sits under FSRA's Risk-Based Supervisory Framework (RBSF-I), marks an escalation in supervisory focus on cyber threats, data vulnerabilities, third-party dependencies, and climate exposure.

While adoption of the guidance's principles is not mandatory, FSRA has indicated that an insurer's adoption of those principles when determining its supervisory approach may be weighed. Ontario insurers should thus treat this guidance as a strong signal of regulatory expectations and an early prompt to assess gaps.

What Ontario insurers should do now

Ontario insurers should consider a structured gap assessment against PC0050APP's four principles, prioritizing:

- Reviewing Board and Senior Management governance structures, including risk appetite documentation and ORMF approval records;
- Auditing IT and cybersecurity controls against GR0016INT and confirming incident notification procedures align with FSRA's materiality thresholds;
- Reviewing third-party vendor contracts for notification obligations, audit rights, and BCP/DRP integration;
- Testing BCP and DRP adequacy, including scenario-specific stress testing; and
- Beginning to incorporate ESG and climate risk considerations into corporate strategy ahead of anticipated further FSRA guidance.

Background

FSRA supervises both Ontario-incorporated insurers and reciprocal exchanges licensed under the *Insurance Act* (Ontario); PC0050APP supplements the existing Corporate

Governance Guidance (PC0051INT) and FSRA's IT Risk Management Guidance (GR0016INT). However, while GR0016INT applies to all FSRA-regulated entities, including federally incorporated insurers licensed in Ontario, PC0050APP applies to Ontario-incorporated insurers only.

Insurers subject to federal oversight should also note that FSRA's guidance broadly aligns, but remains separate as provincial guidance, with expectations in force for federally regulated financial institutions under OSFI's Guideline B-13 – Technology and Cyber Risk Management, reinforcing that operational and cyber resilience is now a pan-Canadian regulatory priority. Ultimately, both FSRA and OSFI have increased their supervisory focus on operational and cyber resilience, resulting in enhanced oversight expectations for insurers operating in Ontario.

PC0050APP's four principles

PC0050APP is organized around four principles that outline FSRA's intended supervisory outcomes:

(1) Governance

Ultimate accountability for operational risk oversight rests with the Board and Senior Management. FSRA expects Ontario insurers to maintain an Operational Risk Management Framework (ORMF), adopt a three-lines-of-defence structure, and clearly define risk appetite, tolerance, and limits. The Board must periodically review and approve Business Continuity Plans (BCPs) and Disaster Recovery Plans (DRPs).

(2) Risk identification and assessment

Ontario insurers must regularly scan their operating environment, including products, people, processes, systems, and the external environment, to identify and assess inherent operational risks. Information technology is specifically flagged as a significant activity subject to this scan.

(3) Risk management

An effective ORMF should reduce both the frequency and impact of operational risk events. Frameworks and supporting policies must be commensurate with the Ontario insurer's size, complexity, and risk profile, and integrated with enterprise-wide risk management.

(4) Resilience

Ontario insurers must plan for adverse scenarios and demonstrate crisis readiness. BCPs and DRPs must be tested against severe but plausible scenarios, kept current, and produced for FSRA on request during supervision. The guidance also emphasizes learning from past failures as a driver of continuous improvement.

Four sub-risk categories under the lens

FSRA identifies four sub-risks within its definition of operational risk, each with specific supervisory implications:

(1) Third-party risk

As insurers increasingly rely on cloud service providers and other outsourced vendors, FSRA emphasizes that accountability and ownership of all risks remain with the insurer, regardless of the outsourcing arrangements. Ontario insurers should establish a third-party risk management framework, conduct ongoing due diligence, and ensure contracts contain appropriate notification, audits, and performance provisions. Concentration risk (that is, over-reliance on a single dominant provider) warrants specific attention.

(2) Cyber risk

FSRA will assess IT controls across access management, network security, asset classification and disposal, incident monitoring, and cybersecurity awareness training. Insurers must provide FSRA with timely notification of material IT incidents as required under GR0016INT, which sets a 72-hour notification window for Ontario-incorporated insurers and reciprocals. BCPs and DRPs should specifically address technology service disruptions.

(3) Data risk

Inadequate data governance is a distinct operational risk, spanning integrity, availability, and the safeguarding of confidential consumer information. FSRA will evaluate whether clear accountability and governance frameworks are in place, and whether data capabilities hold up under stress.

(4) Climate risk (physical and transition)

Physical climate events can disrupt critical operations and amplify underwriting losses through increased property damage claims. FSRA currently assesses ESG and climate initiatives as part of the Resilience Rating under RBSF-I, and has signalled that further climate-specific guidance may follow.

The broader regulatory and legal landscape

FSRA's PC0050APP emerges amid a broader wave of cybersecurity and operational resilience regulation at both federal and provincial levels.

At the federal level, Bill C-8 received Royal Assent on June 15, 2026, thereby completing the legislative process for the *Critical Cyber Systems Protection Act* (CCSPA) and establishing Canada's first mandatory cybersecurity regime for designated operators in sectors, including telecommunications, banking, and clearing systems. Its provisions will come into force gradually, on a day or days to be fixed by order of the Governor-in-Council; read BLG's in-depth Insight on the topic, *Critical Cyber Systems Protection Act*: Bill C-8 is adopted.

While in its current form the CCSPA does not capture federally regulated insurers, insurers that rely on vendors that are designated operators, such as large bank-affiliated cloud providers, may face downstream contractual cybersecurity requirements as those vendors implement their own CCSPA obligations.

Provincially, Ontario's *Enhancing Digital Security and Trust Act*, 2024 (EDSTA) and its accompanying regulations, *O. Reg. 51/26* (Cyber Security) and *O. Reg. 52/26* (Digital Technology Affecting Individuals Under Age 18), both in force as of July 1, 2026, impose mandatory cybersecurity programs, biennial cyber maturity assessments, and 72-hour critical incident reporting on prescribed broader public sector entities.

Ontario's *Plan to Protect Ontario Act (Budget Measures), 2026* (Bill 97) further modernizes the province's access-to-information and privacy framework by extending privacy impact assessment, breach reporting, and cybersecurity safeguard requirements to municipalities.

Although private insurers are not captured by EDSTA, its regulations, or Bill 97, insurers serving public-sector clients may encounter more rigorous cybersecurity expectations as those organizations strengthen vendor oversight obligations.

Takeaways for Ontario insurers

Together with OSFI Guideline B-13 (Technology and Cyber Risk Management), OSFI Guideline B-10 (Third-Party Risk Management), and FSRA's GR0016INT (IT Risk Management Guidance), PC0050APP reinforces a consistent regulatory expectation: boards are accountable for operational risk, risk management frameworks must be documented and proportionate, third-party accountability cannot be outsourced, and resilience must be demonstrated through tested plans rather than asserted. For Ontario-incorporated insurers, PC0050APP provides the framework through which FSRA will assess operational risk and resilience during supervisory reviews.

Key takeaways include:

(1) Governance accountability cannot be delegated.

- The Board bears ultimate responsibility.
- Risk appetite statements, ORMF approval, and BCP/DRP oversight must be demonstrably Board-level activities.
- Ontario insurers should assess their governance structures against Principle 1 and document any gaps.

(2) Cyber and IT controls will face direct scrutiny from FSRA.

- FSRA will assess the full lifecycle of IT risk management from access controls and network security through to incident reporting and staff training.
- Insurers should benchmark their programs against GR0016INT. The 72-hour material incident notification window for Ontario insurers under GR0016INT is a compliance tripwire worth confirming in internal procedures.

(3) Outsourcing does not outsource the risk.

- Accountability for third-party risks stays with the insurer.
- Vendor contracts, particularly with cloud service providers, should be reviewed for incident notification obligations, audit rights, concentration risk provisions, and BCP/DRP integration.

(4) BCPs and DRPs must be tested and producible on demand.

- FSRA may require insurers to present BCPs, DRPS, and scenario testing results during supervisory monitoring.
- Plans must be current, scenario-tested, and capable of being produced promptly.

(5) Climate is a growing supervisory priority, and should be acted upon before the next guidance is anticipated to come out (2031).

- FSRA has signalled that additional climate and ESG guidance is coming, and already factors ESG initiatives into the Resilience Rating.
- Ontario insurers that have not yet begun embedding climate risk into corporate strategy should start now.

By

Laura M. Day, Eric S. Charleston, Olivia Xu

Expertise

Cybersecurity, Privacy & Data Protection, Insurance, Financial Services

---

Montréal

1000 De La Gauchetière Street West
Suite 900
Montréal, QC, Canada
H3B 5H4

T 514.954.2555
F 514.879.9015

Toronto

Bay Adelaide Centre, East Tower
22 Adelaide Street West
Toronto, ON, Canada
M5H 4E3

T 416.367.6000
F 416.367.6749