

The Dentons logo consists of the word "DENTONS" in a bold, white, sans-serif font, enclosed within a white arrow-shaped graphic pointing to the right. The background of the slide is a dark purple gradient with a faint, repeating pattern of a mountain range. On the right side, there is a vertical strip of a photograph showing a rocky riverbed with turquoise water and green vegetation.

# Federal Regulatory Update for Insurers

July 9, 2024

Grow | Protect | Operate | Finance

# Moderator and speaker:



**Laurie LaPalme**  
Partner & Lead, National Corporate  
& Regulatory Insurance practice  
Toronto, Canada  
+1 416 863 4627  
laurie.lapalme@dentons.com

# Speakers:



**Kirsten Thompson**  
Partner & Lead, National Privacy  
& Cybersecurity group  
Toronto, Canada  
+1 416 863 4362  
kirsten.thompson@dentons.com



**Marisa Coggin**  
Partner, Toronto, Canada  
+1 416 863 4633  
marisa.coggin@dentons.com



**Taschina Ashmeade**  
Senior Associate, Toronto, Canada  
+1 416 863 4449  
taschina.ashmeade@dentons.com



**Jaime Cardy**  
Senior Associate, Toronto, Canada  
+1 416 863 4495  
jaime.cardy@dentons.com



**Katie-May O'Donnell**  
Senior Associate, Toronto, Canada  
+1 416 863 4719  
katiemay.odonnell@dentons.com

An aerial photograph of a river flowing through a valley. The river is surrounded by dense green forest. The water is clear and blue, with some white rapids visible. The image is overlaid with a semi-transparent purple shape that covers the left and center portions of the frame.

# OSFI Supervisory Framework

Laurie LaPalme

# Supervisory Framework Renewal

## Fall 2023 OSFI Supervisory Framework Renewal Briefing

- OSFI made comprehensive updates to its Supervisory Framework effective April 1, 2024.
- OSFI stated that the risk environment is changing rapidly, and they modernized their Framework to ensure it remains “Fit for Purpose”.
- OSFI considered other international peer regulators, they held Supervisory roundtables in 2022 on technical risk areas (9 foreign regulatory agencies participated) and held internal focus groups.
- Note that Supervisory Judgement remains a core part of OSFI’s principles-based approach.
- Key Features include:
  - Capturing the impact of systemic and macro centric risks on the risk profile of the FRFI
  - Enabling early corrective action through greater differentiation in risk ratings
  - Building flexibility in the Framework to accommodate new risks and the interplay between financial and non-financial risks
  - Leveraging data and advanced analytics to support a more risk intelligent approach to Supervisory review and application of Supervisory Judgement.
  - Streamlining and simplifying OSFI’s supervisory processes – more timely decisions.

# Framework now includes:

- **Tier Rating** that reflect size, complexity and potential for contagion in the event of failure
- **Overall Risk Rating (ORR)** is assigned which represents the risk of failure (level of overall risk to financial viability):
  - Expanded 8-point rating scale with greater disclosure about risk driver.
  - New Risk Categories including business risk and operational resilience.
  - Umbrella integration of climate risk considerations.
  - Outcome focused.

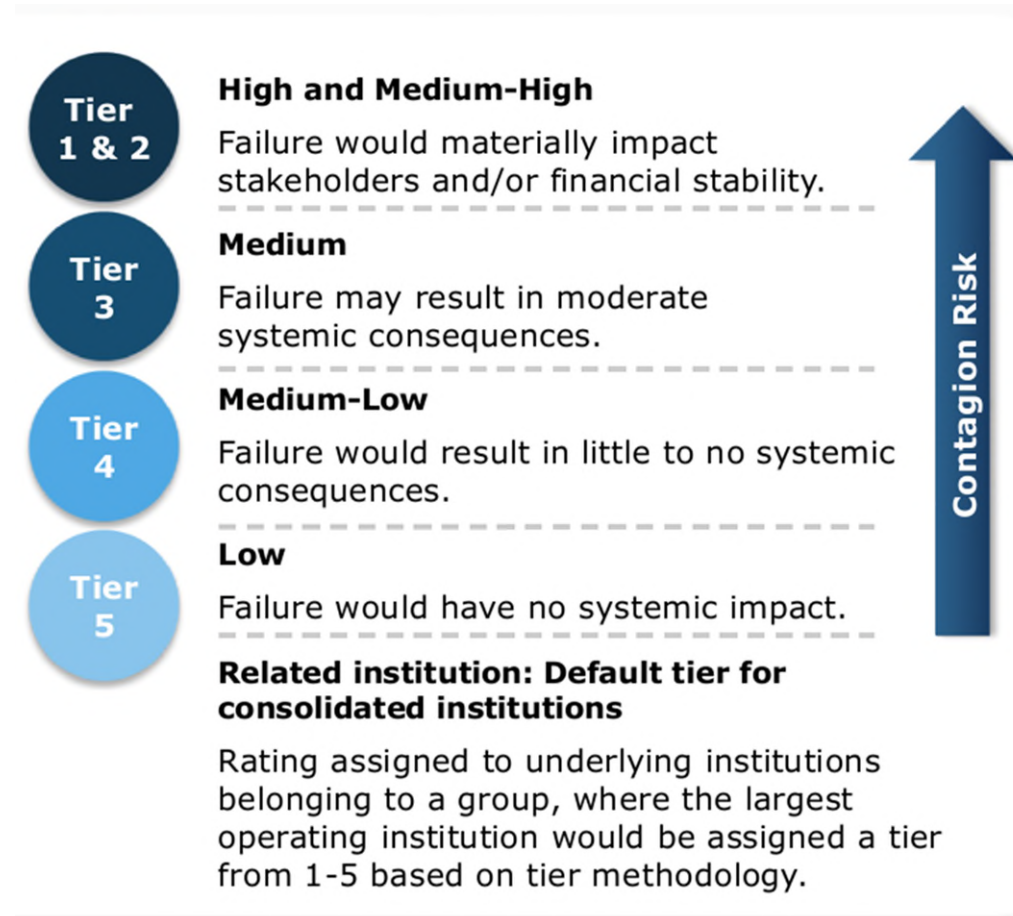
## Framework provides:

Disclosure of rating and the drivers as well as recommendations. This information is to help address supervisory concerns.

Supervisory intensity will be driven by impact of failure (tier rating) and risk of failure (ORR).

# Tier Rating

- Tier Rating reflects size and complexity, with consideration of potential contagion in the event of failure.
- Purpose was to create a consistent risk-based approach to supervision in alignment with OSFI's RISK Appetite.



# Overall Risk Rating

## 4 Risk categories contributing to the ORR




- All categories will drive an outcome.
- The ORR is OSFI's assessment of the safety and soundness of the FRFI. The ORR supports outcome focused engagement with FRFI's.

# ORR Scorecard

Key features:

- Dynamic adjustment and a holistic approach to mitigating risks. There are no fixed weights. Recognition of transverse risks (climate).
- Key findings from supervisory review that assesses safety and soundness of a FRFI and its compliance with Insurance Companies Act and Regulations.
- As a FRFI matures and grows, there is greater supervisory intensity.





		ORR Scorecard												
Disclosed to institutions	All	ORR	Overall Risk Rating											
	1-4	Category	Business Risk	Financial Resilience			Operational Resilience			Risk Governance				
	1-3	Sub-Category		Financial Risk Profile	Capital	Liquidity	Technology	Cyber	Operations	Governance	Business and Central Functions	Risk & Compliance Oversight	Internal Audit	
NOT disclosed to institutions INTERNAL ASSESSMENT ONLY	1 & 2	Detailed Rating		Insurance	Capital Adequacy	Liquidity Adequacy								
				Credit	Capital Management	Liquidity Management								
				Insurers Only	Banks Only									
				Investments	Market (Trading)		Funding Risk							
				Asset/Liability Management	Market (Non-Trading)									
All	Transverse Risk		Climate Risk											

 The number of categories rated depends on the tier and industry



# Rating 8 Point Scale

Maps to Intervention Stages and adds more granularity to Stage Zero.

ORR Rating Scale		Stage
<p>Rating of 1 does not imply perfection</p> 	<b>1 Minimal</b> No significant issues identified	  0
	<b>2 Low</b> Issues are unlikely to impact financial performance or critical operations	
	<b>3 Moderate</b> Issues could impact financial performance or critical operations unless addressed	
	<b>4 Watchlist</b> Issues expected to impact financial performance or critical operations unless addressed promptly	
<p>Ratings of 5-8 include assessment of risk level and velocity</p> 	<b>5 Early warning</b> Issues could impact viability, but this is not expected within two years	1
	<b>6 Material</b> Issues could impact viability within one to two years	2
	<b>7 Serious</b> Issues raise serious doubts about viability within one year	3
	<b>8 Non-viability imminent</b> Non-viability is imminent	4



# Outcome Focused Supervision

- Increased level of timely transparency and disclosure to FRFI to prioritize matters.
- OSFI will share urgent findings as well as recommendations.
- Weakest rating in any category drives the ORR and will drive the required outcome.
- Example below of Summary Supervisory Letter:

Category	Current Rating	Rating Drivers
Tier	Tier 4	
Overall Risk Rating	3	Business Risk
Business Risk	3	New Lines of Business
Financial Resilience	2	Capital Adequacy in New Lines of Business/ Reinsurance Guidelines
Operational Risk	1	No significant issues identified
Risk Governance	1	No significant issues identified
Intervention Stage Rating	Stage 0	ORR that is less than 5

For ratings to improve, FRFI needs to achieve the following:

- Demonstrate the successful execution of business plan, including new lines of business strategy

# What does all this mean? More Time with OSFI!

1. More interaction with Lead Supervisors for “richer dialogue and better assessments”
2. Increased transparency and disclosure in Supervisory Letters:
  - a. Letters were formatted consistently – Ratings, BAAT/ MCT, Specific Themes, Common Themes
  - b. Common Supervisory Themes discussed:
    - ORSA – comprehensiveness of risks assessed, diversification of benefits, breadth of scenarios.
    - Operational resilience – business continuity plans – detailed and documented action plans. Risk scenarios weren’t severe enough.
    - Climate Risk – identifying and quantifying climate related risks and then operationalizing them.
    - Integrity and Security – continued assessment of policies to protect against integrity and security threats.
3. Interim Supervisory letters will be issued. Ratings can change in the year.
4. Increase accountability on FRFI to take action to achieve recommended outcomes. OSFI expecting prompt response.
5. Expect thematic reviews and surveys. Less “On-Sites”.
6. Financial Reporting and Analysis. Questions as to variances and assumption changes.
7. Role of Actuary – appointed actuary and actuarial analysis to play an even greater and prominent role in strategic decisions and day to day operations.
8. Role of Reinsurance may significantly impact ORR.
9. Greater involvement of Senior Management & Board Accountability for effective oversight of risks.
10. More resources and time devoted to regulatory compliance.

# Final Thoughts on OSFI's New Supervisory Framework.

+ It's Flexible, Dynamic, and Proactive



This can only lead to a better Canadian Insurance Industry

+ It's aligned with International Trends



We may be ahead in some areas like Climate Risk Analysis

+ It operationalizes of Risk Management



Better Financial Results and Stronger FRFIs

+ It has increased regulatory burden



Dedicated resources to manage the regulatory requirements

EXPECT frequent and comprehensive involvement with OSFI.

An aerial photograph of a river flowing through a rugged, forested landscape. The river is surrounded by dense green trees and rocky terrain. A large, semi-transparent purple shape is overlaid on the left side of the image, containing the title and author information.

# OSFI Integrity & Security Guideline

Marisa Coggin

# Bill C-47 and Corresponding Changes to Federal Insurance Legislation

- Bill C-47: *An Act to implement certain provisions of the budget tabled in Parliament on March 28, 2023* received Royal Assent in June 2023.
- The *Office of the Superintendent of Financial Institutions Act* was amended to expand OSFI's mandate to include:
- Examining and supervising FRFIs to determine whether they have adequate policies and procedures in place to protect themselves against threats to their integrity and security, including foreign interference; and
- A requirement to report, at least annually, to the Minister of Finance on the adequacy of, and adherence to, the policies and procedures of the FRFIs it regulates.
- In support of these examination duties, the Superintendent has the right to access financial institutions' records and the authority to require financial institutions to provide relevant information.

# Bill C-47 and Corresponding Changes to Federal Insurance Legislation (Cont'd)

- The *Insurance Companies Act* (Canada) was amended to provide that:
  - Canadian insurance companies must establish and adhere to policies and procedures to protect itself against threats to its integrity or security, including foreign interference.
  - Foreign companies must establish and adhere to policies and procedures to protect itself against threats to its integrity or security in relation to its business in Canada.
- A National Security Sector was established and is responsible for helping OSFI ensure that FRFIs address threats from foreign interference and threats to national security that affect FRFIs.
- Integrity and Security Risk Division created to lead integrity and security supervision and policy.

# Regulation of Financial and Non-Financial Risk

## Financial Risks

- Capital
- Liquidity
- Credit

## Non-Financial Risks

- Technology
- Culture
- Regulatory compliance
- Third party risk
- Governance



# Integrity & Security Guideline – Key Definitions

- **Foreign interference** includes activities that are **within or relating to Canada, detrimental to the interests and security of Canada**, and are **clandestine or deceptive** or involve a **threat** to any person, including attempts to **covertly influence, intimidate, manipulate, interfere, corrupt, or discredit** individuals, organizations, and governments to further the **interests** of a **foreign state-or-non-state actor**.
- **Malicious activity** includes actions taken with the **intent** of **causing harm** including **theft, coercion, fraud, manipulation of information or disruptions** that are otherwise **illegal, malicious, clandestine, or deceptive** in nature. Malicious activity can originate from foreign or domestic actors and may have **national security implications**.
- **Undue influence** includes situations where a person or entity engages, with **malicious intent**, in **actions, behaviours, deception** or the use of power to **impact** actions, decisions, or behaviours in their own or another's interests. Undue influence can originate from foreign or domestic actors and may have **national security implications**.

# OSFI Annual Risk Outlook

## 2024-2025 Top risks



Real estate secured lending and mortgage risks



Wholesale credit risks



Funding and liquidity risks



Integrity, security, and foreign interference

# Application, Scope and Outcomes

- The Guideline should be applied on a **risk basis**, having regard to the FRFI's:
  - ownership structure,
  - business arrangements,
  - strategy and risk profile,
  - scope, nature and location of operations.
- The Guideline applies to Canadian insurance companies as well as foreign insurance branches, to the extent it is consistent with applicable requirements and legal obligations related to their business in Canada.
- The Guideline's expectations focus on two overall outcomes:
  1. Actions, behaviours, and decisions should be consistent, and comply, with laws, regulations and codes of conduct.
  2. Operations, physical premises, people, technology assets, and data and information should be resilient and protected against security and other threats.

# Expanded Expectations: Integrity

Principle	Associated OSFI guidelines	Expanded expectations
1. Responsible persons and leaders are of good character and demonstrate integrity through their actions, behaviours, and decisions.	E-17 Background Checks on Directors and Senior Management	Character of responsible persons as demonstrated through their actions, behaviours, and decisions.
2. Culture that demonstrates integrity is deliberately shaped, evaluated, and maintained.	Draft Culture and Behaviour Risk Guideline	Culture reflects a commitment to norms that encourage ethical behaviour.
3. Governance structures subject actions, behaviours, and decisions to appropriate scrutiny and challenge.	Corporate Governance Guideline E-4 Foreign Entities Operating in Canada on a Branch Basis	Governance that provides oversight of actions, behaviours, and decisions. Behavioural expectations are codified in normative documents such as codes of conduct and conflict of interest policies and procedures.
4. Effective mechanisms to identify and verify compliance with regulatory expectations, laws, and codes of conduct exist.	E-13 Regulatory Compliance Management	Compliance that focuses on not just the letter of requirements but also the intent. Effective channels, such as whistleblowing programs, to raise concerns over non-compliance.

# New and Expanded Expectations: Security

Principle	Associated OSFI guidelines	New expectations	Expanded expectations
<b>5. Physical premises are safe and secure and monitored appropriately.</b>	B-13 Technology and Cyber Risk Management Draft E-21 Operational Resilience and Operational Risk Management	Standards and controls for physical buildings, office spaces, physical file storage, and technical security inspections.	Not applicable
<b>6. People should be subject to appropriate background checks, and strategies should be put in place to manage risk.</b>	E-17 Background Checks on Directors and Senior Management	Risk-based background checks on all employees and contractors, as appropriate to the role.	Not applicable
<b>7. Technology assets should be secure, with weaknesses identified and addressed, effective defences in place, and issues identified accurately and promptly.</b>	B-13 Technology and Cyber Risk Management	Not applicable	Enhanced description of what constitutes malicious actions towards IT infrastructure.
<b>8. Data and information should be the subject of appropriate standards and controls ensuring its confidentiality, integrity, and availability.</b>	B-13 Technology and Cyber Risk Management Draft E-21 Operational Resilience and Operational Risk Management	Data classification considers vulnerability to malicious activity, undue influence, or foreign interference.	Personnel access requirements to prevent undue influence and foreign interference.
<b>9. Third parties should be subject to equivalent and proportional measures to protect against threats.</b>	B-10 Third-Party Risk Management	Third-party risk management is conducted through an integrity and security lens and is proportional to the third party's access to the financial institution's physical premises, people, technology assets, and data and information. Transparent and objective procurement processes.	Not applicable
<b>10. Threats stemming from suspected undue influence, foreign interference, and malicious activity should be promptly detected and reported.</b>	E-13 Regulatory Compliance Management	Notification to OSFI when a report is made to RCMP, CSIS, or other authorities regarding undue influence, foreign interference, or malicious activity.	Not applicable

# New and Expanded Expectations

## Background Checks

**Principle 1: Responsible persons and leaders are of good character and demonstrate integrity through their actions, behaviours, and decisions.**

- Where a responsible person is found to lack integrity, they will normally not be suitable for any responsible person position.

**Principle 6: People should be subject to appropriate background checks, and strategies should be put in place to manage risk.**

- **Responsible persons, employees, and contractors** should be subject to appropriate, **risk-based** background checks that are conducted prior to employment, renewed on a regular basis and reviewed off-cycle based on certain criteria.
- Background checks should include, **at a minimum**, education and professional credentials and references.
- Criminal record checks and credit checks should be required for individuals with **higher risk** positions.

# New and Expanded Expectations

## Culture

**Principle 2: Culture that demonstrates integrity is deliberately shaped, evaluated, and maintained.**

- FRFIs should seek to demonstrate that:
  - Culture and behaviour are designed and governed through **accountabilities** and **oversight**; and
  - **Integrity** is **deliberately** shaped, evaluated and maintained.
- FRFIs should **proactively reinforce** desired culture and behaviours and **proactively manage** any risks emerging from **behaviour patterns**.

# New and Expanded Expectations

## Governance

**Principle 3: Governance structures subject actions, behaviours, and decisions to appropriate scrutiny and challenge.**

- Actions, behaviours, and decisions should be subject to appropriate **scrutiny** and **challenge**.
- Important decisions should be subject to **effective governance**.
- Behavioural expectations should be **codified** (in codes of conduct, conflict of interest policies/procedures).
  - Codes of conduct should highlight the importance of (i) adherence to laws, regulations, policies and procedures; (ii) avoiding conflicts of interest (bribery, other unacceptable influences); (iii) maintaining objectivity, avoiding bias in decision-making; and (iv) ensuring security and confidentiality of assets, communications and information.



# New and Expanded Expectations

## Regulatory Compliance Management

**Principle 4: Effective mechanisms to identify and verify compliance with regulatory expectations, laws, and codes of conduct exist.**

- FRFIs should have an effective, enterprise-wide RCM framework.
- Effective channels should exist to **raise concerns** over **non-compliance**, such as whistleblowing programs.
- FRFIs should regularly review, update and remind employees of the existence of internal and external channels available to raise concerns or provide constructive feedback.

**Principle 10: Threats stemming from suspected undue influence, foreign interference, and malicious activity should be promptly detected and reported.**

- **Threats** stemming from suspected undue influence, foreign interference, and malicious activity should be **promptly detected and reported** to OSFI and RCMP or CSIS/other authority.

# New and Expanded Expectations

## Technology/Cyber Risk Management

**Principle 5: Physical premises are safe and secure and monitored appropriately.**

- **Standards and controls** for controlling access to and monitoring of physical buildings, office spaces, physical file storage, and technical security inspections (i.e. access card management and related protocols).

**Principle 7: Technology assets should be secure, with weaknesses identified and addressed, effective defences in place, and issues identified accurately and promptly.**

- Intensity of defences should be **proportional** to the likelihood of threats and severity of impact to the FRFI, its employees, clients and other stakeholders if the technology asset is compromised.

**Principle 8: Data and information should be subject to appropriate standards and controls ensuring its confidentiality, integrity, and availability.**

- **Data classification** should be developed considering vulnerability to malicious activity, undue influence, or foreign interference (i.e. data should have appropriate confidentiality classification – cyber-attacks are a common way to introduce malware to a company’s system to collect information to support foreign interference activities.)
- **Personnel access requirements** should be in place to prevent undue influence and foreign interference.
- FRFIs should implement mechanisms to identify and escalate **unauthorized access** to data by people or systems.

# New and Expanded Expectations

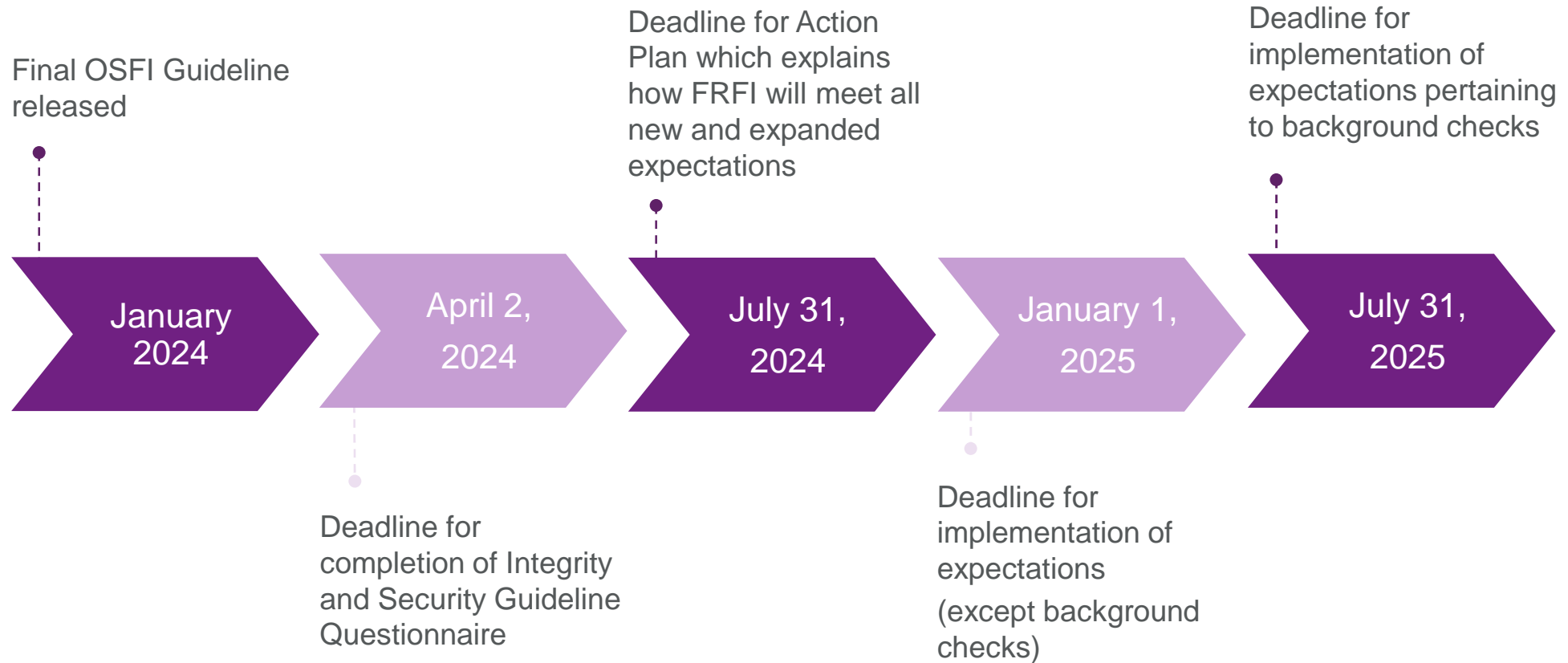
## Third Party Risk Management

**Principle 9: Third parties should be subject to equivalent and proportional measures to protect against threats.**

- Third party risk management should be conducted through an **integrity and security lens** and should be **proportional** to the third party's access to the FRFI's physical premises, people, technology assets, and data and information.
  - Consider the third party (and any subcontractor's) location of operations, location of corporate headquarters, connections to foreign governments and ownership structure.
- FRFIs should ensure that **third party service/other agreements** comply with Guideline B-10.
- **Procurement** processes should be transparent and objective.

# OSFI Integrity and Security Guideline

## Key Dates



# Supporting Compliance with the Integrity & Security Guideline

- Finalizing your Action Plan – specific to your FRFI’s strategy, risk profile and nature of operations.
- Review and/or creation of applicable policies and procedures, including:
  - Regulatory Compliance Management frameworks.
  - Assessment Policies for Responsible Persons.
  - Technology and/or Cyber Risk Policies.
  - Outsourcing Policies.
  - Legal/governance advice.
- Training sessions for personnel.

An aerial photograph of a river flowing through a valley. The river is surrounded by dense green forest and rocky terrain. A large, semi-transparent purple shape is overlaid on the left side of the image, containing the title and author's name.

# Climate Risk Management Guideline

Katie-May O'Donnell

# Summary of Guideline B-15

## Background:

**March 2023:** OSFI issued its first climate sensitive framework.

**March 2024:** OSFI issued updated Guideline-B15 (to align its climate-related disclosure framework with the International Sustainability Standards Board (“ISSB”) standard, IFRS S2 Climate-related Disclosures (“IFRS S2”).

## Purpose:

Outlines OSFI’s expectations for managing climate-related risks in FRFIs.

## Expected Outcomes:

**Risk Mitigation:** FRFIs understand and mitigate potential climate-related impacts on their business model and strategy.

**Governance:** FRFIs implement effective governance and risk management practices for climate risks.

**Resilience:** FRFIs maintain financial and operational resilience during severe climate risk scenarios and disruptions.

# OSFI's Expectations for Guideline B-15

2024 Fiscal Year-End:  
IAIGs are expected to:

- Have governance structures to manage climate risk.
- Incorporate climate risk into their strategy.
- Manage climate risk according to their risk appetite.
- Disclose climate risk metrics, including Scope 1 and 2 emissions.

2025 Fiscal Year-End:  
IAIGs are expected to:

- Disclose Scope 3 emissions.

All Other FRFIs:

- Deadline extended by one year compared to IAIGs.



# Governance

Requirement	FRFIs' Approach	Best Practices	Aligned International Frameworks
<p><i>Describe governance and accountability structure for climate-related risks and opportunities.</i></p>	<ul style="list-style-type: none"> <li>• Large FRFIs have disclosed governance frameworks with roles and responsibilities.</li> <li>• Executive pay tied to climate metrics; Board remuneration not yet included.</li> </ul>	<ul style="list-style-type: none"> <li>• Establish and disclose a climate governance framework with defined roles and accountability at all levels.</li> <li>• Integrate climate framework into existing governance structures with formal reporting and communication.</li> <li>• Include climate-related factors in Board and Executive remuneration and Executive remuneration structures.</li> </ul>	<p>Task Force on Climate-related Financial Disclosures (TCFD), Glasgow Financial Alliance for Net Zero (GFANZ)</p>

# Strategy

Requirement	FRFIs' Approach	Best Practices	Aligned International Frameworks
<i>Describe the impact of climate risks and opportunities on business and strategy.</i>	<ul style="list-style-type: none"><li>• FRFIs assess climate risks with varied disclosures on impacts and financial performance.</li><li>• No standalone Transition Plan yet; most plan to develop one.</li></ul>	<ul style="list-style-type: none"><li>• Develop a transition plan using TCFD and GFANZ frameworks.</li><li>• Disclose how physical and transition risks affect business, strategy, and financial planning.</li></ul>	TCFD, GFANZ

# Risk Management

Requirement	FRFIs' Approach	Best Practices	Aligned International Frameworks
<p><i>Develop climate risk management capabilities.</i></p>	<ul style="list-style-type: none"> <li>• Most FRFIs have processes for identifying and monitoring climate-related risks.</li> <li>• Few comprehensively disclose integration of climate-related opportunities.</li> </ul>	<ul style="list-style-type: none"> <li>• Integrate climate risks into enterprise risk management framework and internal controls, including ORSA.</li> <li>• Use internal reporting mechanisms to monitor and assess climate risks continuously.</li> </ul>	<p>TCFD, NGFS</p>

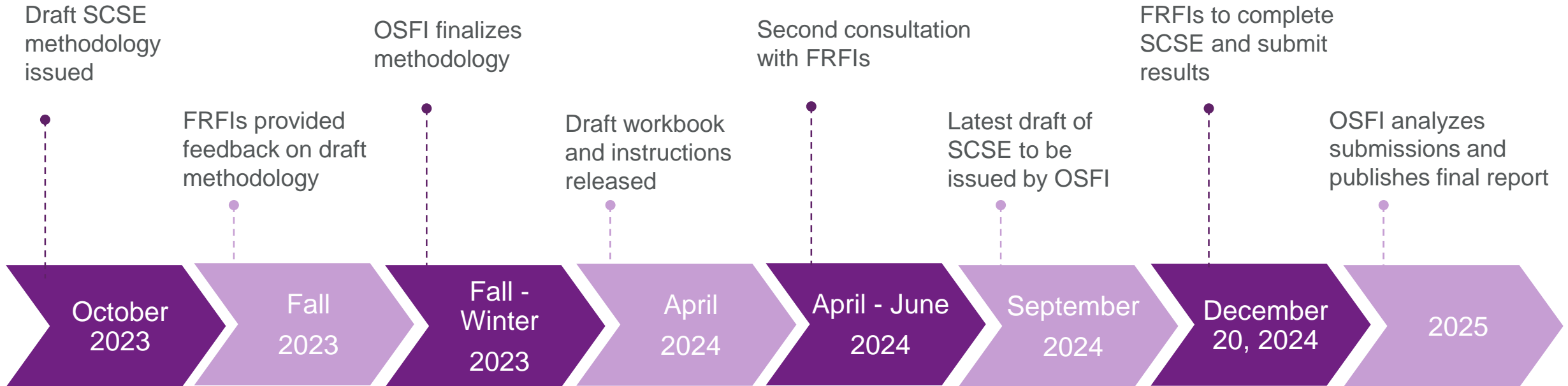
# Metrics and Targets

Requirement	FRFIs' Approach	Best Practices	Aligned International Frameworks
<p><i>Disclose Scope 1, 2, and 3 GHG emissions and net zero targets.</i></p>	<ul style="list-style-type: none"> <li>• Most large FRFIs disclose Scope 1, 2, and at least one Scope 3 category emissions, with interim targets and reporting standards.</li> <li>• Most FRFIs set and report on climate-related targets, with varied disclosure on internal carbon pricing and climate-linked remuneration.</li> </ul>	<ul style="list-style-type: none"> <li>• Calculate financed emissions across relevant portfolios and set interim net-zero targets aligned with key frameworks. Ensure information is reliable and verifiable.</li> <li>• Determine and disclose IFRS S1-aligned industry and cross-industry metrics.</li> </ul>	<p>TCFD, GFANZ</p>

# Overview of Standardized Climate Scenario Exercise (SCSE)

- **Purpose:** Builds on Guideline B-15's climate scenario analysis and stress testing requirements.
- **Scope:** Applies to IAIGs headquartered in Canada and FRFIs.
- **Components:** Includes a comprehensive methodology, instructions, workbook, and industry sector mappings.
- **OSFI's Objectives:**
  - Encourage FRFIs to understand their potential climate risk exposure.
  - Promote assessment of climate risk impacts and scenario analysis.
  - Establish a quantitative assessment of climate-related risks.

# Overview of OSFI's Issuance and Expectations for SCSE



# Ramifications of Non-Compliance with Guideline B-15

- **No Unique Penalties:** Guideline B-15 itself doesn't impose specific penalties for non-compliance.
- **LEFP Framework:** OSFI's Late and Erroneous Filing Penalty Framework applies.
  - **Penalties Apply If:**
    - Disclosures are not made as prescribed.
    - Disclosures are incomplete or contain errors.
    - Disclosures are submitted past the due date.
  - **Per Diem Penalty:** Late or erroneous filings may incur daily penalties.

# What FRFIs Can Do Now to Prepare for the New Requirements?

## Governance and Controls

- Create dedicated committees or roles for overseeing climate risks.
- Embed climate risk considerations into existing governance frameworks and policies.
- Implement controls to ensure the accuracy, completeness and timeliness of internal and external reporting.
- Educate key business partners and provide internal training on their roles and responsibilities regarding climate risk management.

## Data and Analytical Capabilities

- Evaluate appropriate metrics and targets, including the requirements to measure existing metrics and targets.
- Implement processes to collect, validate, and analyze relevant data.
- Develop capabilities to conduct climate scenario analysis to understand and assess potential future impacts on risk profiles and business strategies.
- Integrate climate risk factors into existing risk models and stress testing frameworks.

## Disclosure Readiness

- Establish governance processes to ensure the accuracy and reliability of disclosed information.
- Ensure all disclosure requirements are consistent with OSFI's guidelines and expectations, including accuracy and timeliness.
- Provide a detailed climate transition plan and outline the approach to measure progress.
- Enhance disclosure of climate-related risks and opportunities, including the identification and monitoring of impacts.



An aerial photograph of a river flowing through a forested, rocky landscape. The river is surrounded by dense green trees and rocky terrain. A large, semi-transparent purple shape is overlaid on the left side of the image, containing the title and authors' names.

# Technology and Cyber Risk Management

Kirsten Thompson

Jaime Cardy

# B-13 Introduction

- Establishes OSFI’s expectations for how federally regulated financial institutions (FRFIs) manage technology and cyber risks
- Guideline came into effect on January 1, 2024
- “No one-size-fits-all approach for managing technology and cyber risks”
- Compliance is not a one-time event
- Intended to be read in conjunction with other OSFI guidance, tools, supervisory communications, and guidance from the Canadian Centre for Cyber Security, including:
  - OSFI’s Cyber Security Self-Assessment (issued in 2013; updated in 2021) OSFI’s Advisory on Technology and Cyber Security Incident Reporting (issued in 2019; updated in 2021)
  - The Integrity & Security Guideline
  - OSFI Guideline B-10 – Third-Party Risk Management (released in April 2023)

# Importance of Technology and Cyber Risk Management

- There has been an **increased incidence** of ransomware attacks over the past 5 years coupled with **higher extortion amounts**.
- Due to the increase in incidents in recent years, **cyber insurance providers have started requiring more proactive approaches** from their clients.
  - Examples: Tactics, techniques, and procedures like multi-factor authentication and endpoint detection and response.
- **OSFI** has clearly expressed its **intention to monitor compliance** with the Guidelines over this fiscal year:
  - Based on OSFI's Annual Risk Outlook, it appears that the review process will pay particular attention to third party risk management.
  - Failure to demonstrate compliance with B-13 may negatively impact the institution's Overall Risk Rating and result in escalating supervision and intervention pursuant to OSFI's Supervisory Framework.

# OSFI's Annual Risk Outlook

## Fiscal Year 2024-2025

### Cyber security concerns highlighted in the report:

*“[...] geopolitical tensions, conflicts including state-on-state conflict, political crisis, democratic events, and global power rebalancing efforts continue to create global security and economic uncertainty. Uncertainty and tension can lead to activities, such as special economic sanctions, cyber attacks, foreign interference, or money laundering, that intensify integrity and security risks at institutions and eventually can manifest as financial risks.”*

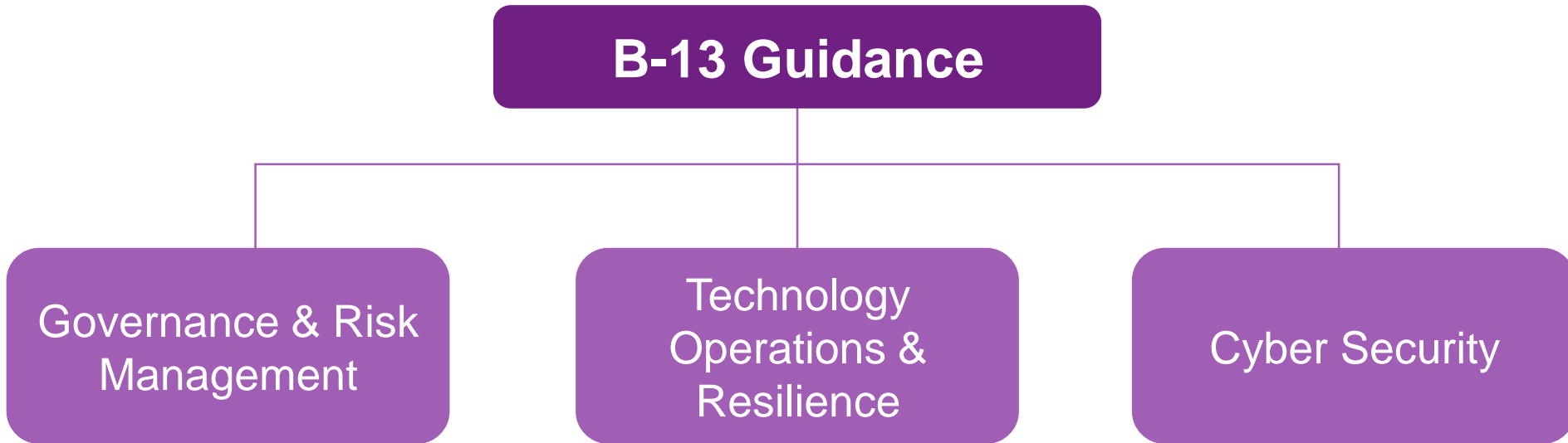
*“We are concerned with threats to institutions’ integrity and security ranging from fraud and money laundering to cyber security and foreign interference. With advances in technology, financial institutions are facing more sophisticated and frequent threats to their security and operational resilience.”*

### Planned supervision efforts:

*“In 2024 and 2025, we will selectively review institutions against our technology and cyber risk management guidelines. We will also continue our cyber resilience testing to identify control weaknesses and monitor threats from emerging technologies.”*

*“Over the plan horizon, insurance supervision will [...] intensify focus on operational resilience with activities targeted towards cyber resilience and third-party supplier risks for critical outsourced operations. [...] We will conduct thematic reviews on cyber resilience and third-party risk management of critical outsourced functions.”*

# B-13 Framework



The three domains are supported by 17 principles and nearly 60 recommended controls.

# Governance & Risk Management (“People”)

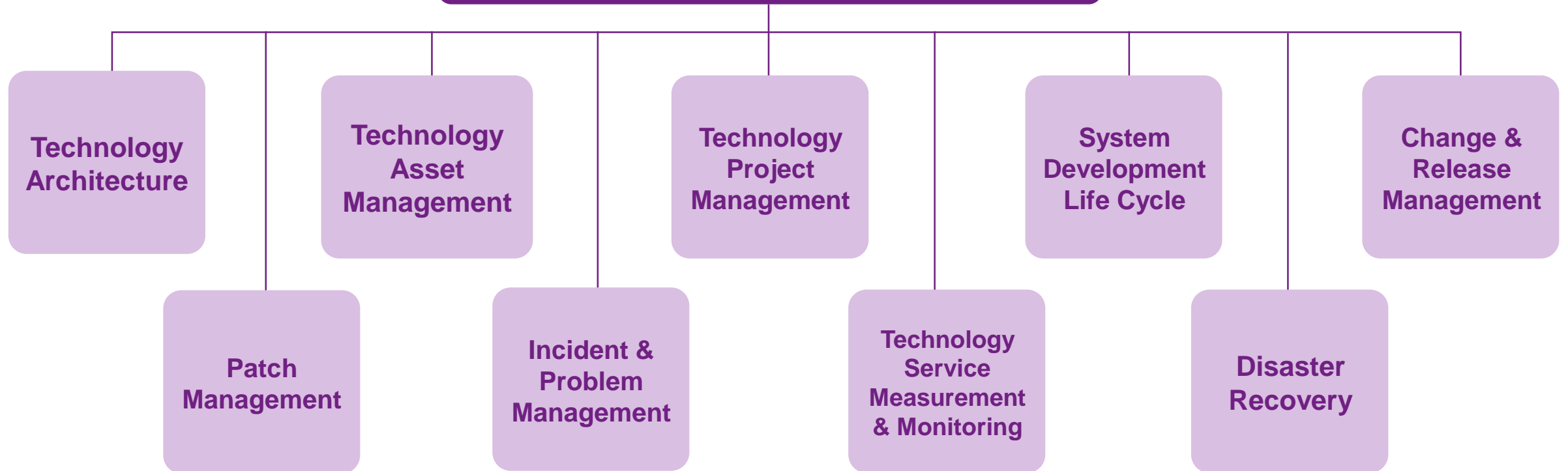


# Governance & Risk Management (cont.)

- This domain is aimed at ensuring that institutions are able to govern their technology and cyber risks through clear accountability structures and comprehensive risk management strategies and frameworks.
- Dentons recommends:
  - Including a breach coach and lawyer (ideally one and the same) as part of the team tasked with managing technology and cyber risks across your organization.
  - Continuously monitoring the threat risk environment and updating your policies and procedures as required.
  - Building up an offensive strategy by engaging a third-party cybersecurity provider to provide threat intelligence and seeking out sector-specific threat-sharing groups and government groups, such as those offered by the Canadian Centre for Cyber Security.

# Technology Operations & Resilience (“Processes”)

## Technology Operations & Resilience

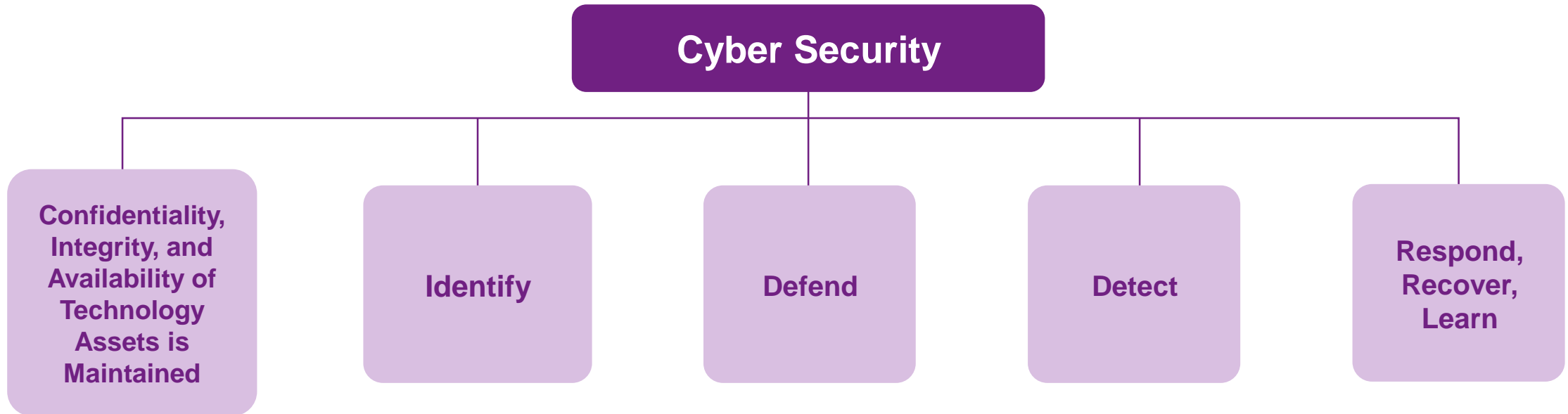




# Technology Operations & Resilience (cont.)

- This domain is aimed at ensuring that institutions are able to manage and oversee the risks related to the design, implementation, management and recovery of technology assets and services.
- Dentons recommends:
  - Paying strong attention to vendor and third-party service providers' cyber preparedness. Engage in thorough due diligence during procurement process and use strong contractual terms. If currently engaged with a third party who doesn't satisfy your expectations or are considering contracting with a third party who is weak in these areas, walk away.
  - Tabletop incident response and disaster recover plans with all relevant stakeholders – including legal, PR/Comms/GR, HR, etc. – but have only a few people aware that it is a test. Tweak plans based on lessons learned.
  - Ensure the incident response plan and disaster recovery program dovetail with the business continuity plan, and that all are applicable in a variety of circumstances.
    - See OSFI's Draft Guidance E-21 on Operational Resilience and Operation Risk Management, and its Business Continuity Planning publication.

# Cyber security (“Technology”)



# Cyber security (cont.)

- This domain is focused on ensuring that institutions have a secure technology posture that is able to maintain the confidentiality, integrity and availability of their technology assets.
- Dentons recommends:
  - Ensure alignment with international industry standards, such as NIST Cybersecurity Framework 2.0 issued in Feb 2024.
  - Engage with third party cybersecurity firms and threat-sharing groups to evaluate risks and vulnerabilities, maintain situational awareness of external threats, etc.
  - Integrate this technology piece with the governance work being done under the first domain.
  - Cyber security is not a place to become complacent; rather, a focus on continuous improvement is required to merely stay in lock step with malicious actors who are becoming increasingly sophisticated. All teams must remain agile enough to respond to the evolving threat landscape.

# Additional considerations

- **Legal privilege**
  - Solicitor-client privilege vs. Litigation privilege.
- **Compliance must be consistent with other legal obligations**
  - Ex. obligations under Canada's federal and provincial private sector privacy laws.
  - Ability to respect litigation holds.
- **Reporting obligations**
  - Example: to OSFI, privacy regulators, RCMP, CSIS, Canadian Centre for Cyber Security, etc.
  - We strongly recommend consulting with legal counsel before reporting.



# Third Party Risk Management Guideline

Taschina Ashmeade

# What is a third-party arrangement?

- A third-party arrangement refers to any type of business or strategic arrangement between the FRFI and an entity or individual, by contract or otherwise, save for arrangements with FRFI customers and employment contracts, which are excluded from this definition.
- A third-party arrangement includes:
  - Outsourced activities, functions, and services that would otherwise be undertaken by the FRFI itself;
  - Use of independent professional consultants;
  - Brokers (e.g., mortgage, insurance, deposit brokers);
  - Utilities (e.g., power sources, telecommunications);
  - Financial market infrastructures (e.g., payments systems, clearing and settlement systems, other FRFIs in cases where the FRFI does not have direct access to financial market infrastructures);
  - Services provided by parent holding companies, affiliates, and subsidiaries, or through joint ventures and partnerships; and
  - Other relationships involving the provision of goods and services or the storage, use or exchange of data (such as cloud service providers, managed service providers, technology companies that deliver financial services).

# What is third-party risk management?



# Scope of the Third-Party Risk Management Guideline

- OSFI clarified that the Third-Party Risk Management Guideline also applies to foreign insurance company branches.
- Compliance Timeline:
  - Branches have until **March 31, 2025**, to comply with the clarified provisions of Guideline B-10.
- Modification of Existing Agreements:
  - Third-party arrangements established **before March 31, 2025**, must also be reviewed.



# Differences Between Guideline B-10

## Outsourcing of Business Activities, Functions and Processes and the Third-Party Risk Management Guideline

	Guideline B-10	Third-Party Risk Management Guideline
<b>Scope</b>	Focuses on outsourcing arrangements specifically.	Encompasses all types of third-party relationships.
<b>Approach to Risk Management</b>	Emphasizes traditional outsourcing risk management practices.	Takes a holistic approach to third-party risk management, including cybersecurity, and data protection.
<b>Due diligence and Monitoring</b>	Focuses on initial due diligence and ongoing monitoring of outsourcing providers.	Requires more comprehensive and continuous due diligence and monitoring across all third-party relationships.
<b>Contingency Planning</b>	Requires contingency plans for outsourced functions.	Expands contingency planning requirements to cover a broader range of third-party disruptions.
<b>Standardized Contracts</b>	Silent regarding the management of standardized forms.	Captures the commercial reality around standardized contracts.

# OSFI's Expectations and Observations

- 1. Governance and Accountability:** The FRFI is ultimately accountable for managing the risks arising from third-party arrangements.
- 2. Third-Party Risk Management Framework:** Establish a comprehensive Third-Party Risk Management Framework that regulates the cycle of third-party arrangements from sourcing the arrangement to termination.
- 3. Regularly Assess Existing Third-Party Arrangements:** OSFI expects FRFIs to manage third-party risks in proportion to the risk level and complexity of their third-party relationships.
- 4. Identification and Assessment of Risks:** Conduct thorough risk assessments before entering into third-party arrangements and periodically through the term.
- 5. Monitoring and Assessing Performance:** Continuously monitor third-party performance and address risks and incidents proactively.
- 6. Technology and Cybersecurity:** Ensure that third-party technology and cyber operations are transparent, reliable, and secure.

# Best Practices for Third-Party Arrangements

- 1. Due Diligence:** Perform thorough due diligence before entering into third-party agreements and periodically review the third parties' performance and risk profile.
- 2. Concentration Risk:** Assess and mitigate concentration risks related to overreliance on a single third-party or geographic location.
- 3. Subcontracting Risk:** Identify, monitor, and manage risks arising from subcontractors used by third parties.
- 4. Contract Management:** Include detailed provisions in contracts covering performance standards, audit rights, security requirements, compliance obligations, and exit strategies.
- 5. Adequate Training:** Provide regular training and awareness programs for employees involved in third-party risk management to ensure they understand the policies, procedures, and their roles in managing third-party risks.

# Thank you



**Laurie LaPalme**  
Partner & Lead, National Corporate  
& Regulatory Insurance practice  
Toronto, Canada  
+1 416 863 4627  
laurie.lapalme@dentons.com



**Kirsten Thompson**  
Partner & Lead, National Privacy  
& Cybersecurity group  
Toronto, Canada  
+1 416 863 4362  
kirsten.thompson@dentons.com



**Marisa Coggin**  
Partner, Toronto, Canada  
+1 416 863 4633  
marisa.coggin@dentons.com



**Taschina Ashmeade**  
Senior Associate, Toronto, Canada  
+1 416 863 4449  
taschina.ashmeade@dentons.com



**Jaime Cardy**  
Senior Associate, Toronto, Canada  
+1 416 863 4495  
jaime.cardy@dentons.com



**Katie-May O'Donnell**  
Senior Associate, Toronto, Canada  
+1 416 863 4719  
katiemay.odonnell@dentons.com