CAFII Summary Notes

2024 CLHIA Compliance and Consumer Complaints Conference, May 22-24, 2024

Vancouver, British Columbia

Contents

CLHIA Conference--Overview and Approach

The May 22-24, 2024, CLHIA Compliance and Consumer Complaints Conference included many presentations that are relevant to CAFII members. Not all presentations are summarized here, only those of CAFII member relevance.

May 22, 2024

Opening Comments

Fay Coleman, Compliance Manager, TD Life Insurance Company and Robyn Van Zant, Complaints Officer, RBC Life Insurance Company

Ms. Coleman and Ms. Van Zant welcomed participants to the Conference and spoke about the very strong presenters who would be sharing their insights over the following days.

Tone at the Top—From Barriers to Benefits: The role we play in health equity

Sarah Hoffman, President & CEO, Pacific Blue Cross

Ms. Hoffman noted that Pacific Blue Cross is a not-for-profit organization that is the number one health benefits provider in British Columbia, covering 1 in 3 British Columbians. Its values are customer experience, data-driven insights, accessibility, investing in the community, and health equity. She noted how diverse BC is, with 6% of the population identifying as 2SLGBTQ1+, 6% as Indigenous peoples, 34% as a visible minority, 13% from rural communities, and 20% living with one or more disabilities. British Columbia also has the third-highest transgender and/or non-binary population in Canada.

Ms. Hoffman noted that equity and equality are not the same and that "Health equity seeks to reduce inequalities and to increase access to opportunities and conditions conducive to health for all." She noted the various factors that are determinants of health, including:

- Income & social status;
- Employment & working conditions;
- Education & literacy;
- Childhood experiences;
- Physical environments;
- Social supports & coping skills;
- Healthy behaviours;
- Access to health services;
- Biology & genetic endowment;
- Gender;
- Culture;
- Race/racism.

Ms. Hoffman spoke about the people at Pacific Blue Cross, about the commitment to community, and some of the organization's plans. Her focus was on the initiatives Pacific Blue Cross is engaged in to promote equity and fairness, noting the many challenges that women and people from diverse communities still face in the workplace.

Chief Compliance Officers and Privacy Panel

Panelists: Keri Bush, Vice-President Global Conduct Risk and Chief Compliance Officer, Sun Life; Charles MacLean, Chief Compliance Officer, RBC Insurance; Julie Rochette, Vice President, Chief Compliance Officer and Chief Privacy Officer, iA Financial Group; Katie Wells, Chief Privacy Officer, Canada & Deputy Global Chief Privacy Officer, Manulife; Moderator: Hartley Lefton, Partner and Co-Chair, National Insurance and Reinsurance Group, McCarthy Tétrault LLP

The panelists all touched on the rapid pace of change, including what remains unchanged, and the increasing complexity of the role of Chief Compliance Officer. Compliance officers must be part of business decision-making; if marketing or sales tells compliance just before a launch of their plans and compliance says that some aspects of the plan are not acceptable, that is a bad outcome for the organization and can be avoided by engaging compliance from the beginning.

All the panelists felt that the pace of regulatory change was increasing and would not slow down. There was a concern that regulatory changes occurred regardless of the necessity or a clear demonstration of the improvement of customer protections. The key challenge for compliance departments is how to manage risk without stifling innovation.

The panelists explained that it is important for compliance to be creative and curious, with one panelist comparing compliance to water, which flows everywhere. On artificial intelligence, there was a recurring theme that humans had to be involved in critical decision making; AI might identify insights, but humans need to make the final determination on the best use of those insights.

Regulatory Perspectives From Across Canada

Erica Hiemstra, Head, Insurance Conduct, Market Conduct, Financial Services Regulatory Authority of Ontario; Harry James, Director, Regulation Advisory Services Policy & Stakeholder Engagement, BC Financial Services Authority; Julien Reid, Senior Director, Financial Institutions Policy and Resolution, Autorité des marchés financiers, Québec; Moderator: Meaghan Obee Tower, Partner, Stikeman Elliott LLP

Julien Reid from the AMF said that the authority's key priorities include climate change, with the AMF planning to publish its new *Guideline on Climate Change Risk Management* by the end of June 2024. This Guideline will be harmonised with OSFI's B-15 Guideline and will consider the most recent developments on the subject (in particular, the new IFRS S1 S2 standards). The guideline proposes a framework that incorporates best practices in terms of fair treatment of customers.

By June, the AMF will also publish a "Risk Outlook" exploring trends, issues, and opportunities on the authority's radar. This document will provide an overview of the issues that the AMF is following and that could be of interest for Québec's financial institutions.

Another AMF priority is operational resilience. In 2023, the AMF conducted a survey on operational resilience and held a webinar on the topic in February 2023. The results showed that financial institutions have different conceptions and understandings of the concept of operational resilience. The AMF intends to pursue its initiatives in this area by publishing a report presenting the results of its awareness survey in the second quarter of 2024. Building on the success of the webinar, industry also asked for more support and guidance from the regulator. In collaboration with the industry, the AMF also plans to set up a community of practice that will address various resilience-related topics. The AMF also plans to develop a new guideline in 2024 on third-party risk management, that will replace the current guideline on outsourcing risk management.

The AMF is also focused on total cost reporting. Total Cost Reporting the AMF is now at the stage of implementing CCIR expectations in the form of a regulation in Québec. The draft regulation was published for consultation from December 15, 2023, to January 31, 2024. The final regulation will be published in 2024 with a coming into force on January 1, 2026. Consumers will receive their first annual statement with full cost disclosure at the beginning of 2027.

Following the publication of its new regulation on complaint reporting, the AMF will post support materials on its website to assist businesses in understanding the new framework. The AMF will also be providing a complaint processing policy template applicable to the practice of financial intermediaries.

With respect to entry requirements, Mr. Reid said that the AMF was looking at a "review of our career entry requirements for the offer of insurance products, including the probationary period," to see if the AMF can help the industry find solutions to the existing labour shortage. He added that a public consultation on this matter should be launched before the end of summer 2024.

Mr. Reid added that the oversight of agents, including their roles and responsibilities, is one of the main compliance issues that drives AMF interventions and recommendations. The AMF is exploring options to enhance the governance and compliance of distribution firms with existing expectations. The AMF specifically seeks to clarify the regulation around the roles and responsibilities of the "responsible officer" as well as the application of the fair treatment of customers to intermediaries.

Keith Martin and Julien Reid had a 10-minute conversation prior to the conference during which Mr. Reid shared some of the points he planned to make at the conference. He was very friendly and approachable throughout the conference, with several other short conversations occurring.

Erica Hiemstra identified three key priorities currently for FSRA. The first is to strengthen the MGA regulatory framework. The second priority is to strengthen protection for consumers who invest in segregated fund contracts. This includes the Consolidated Guidance (CCIR); Total Cost Reporting, which is a FSRA rule; and the DSC cessation report. The third priority is around supervision, specifically for insurers, MGAs, and agents. Ms. Hiemstra mentioned the work that FSRA CEO Mark White, as well as Swati Agrawal, had been doing on DEI issues at the International Association of Insurance Supervisors (IAIS).

Ms. Hiemstra said that FSRA was paying attention to a Fintech Forum at IAIS. She also noted that FSRA Executive Vice President Huston Loke is the Chair of the Canadian Council of Insurance Regulators (CCIR). Ms. Hiemstra explained that she is working at the CCIR on the issue of oversight of OmbudsService of Life and Health Insurance (OLHI). Some of the current strategic priorities for the CCIR are:

- enhancing consumer protections and alignment with IAIS principles around incentive management and climate change;
- expectations from the IMF review around insurance, and regulatory efficiency, including changes to the Annual Survey on Market Conduct;
- work on complaints; and,
- insurers commitment to the fair treatment of customers.

The CCIR is looking to strengthen regulatory outcomes, including its commitment to a consolidated national guidance around segregated funds. An important CCIR committee for FSRA, and one they will continue to monitor, is the Cooperative Supervision Oversight Committee.[1]

Harry James of BCFSA identified assessing insurer adoption of the BCFSA *Insurer Code of Market Conduct* as a key priority. He explained that BCFSA wants to see how insurers are integrating the fair treatment of customers (FTC) principles into governance practices and business practices. He added that, as necessary, the BCFSA would proactively address potential issues around FTC. Another priority was around natural catastrophes and climate-related risks, with prudential issues aligned with OSFI and market conduct issues advanced principally through CCIR. He also mentioned the BCFSA Information Security Incident Reporting, which is now a guideline after industry feedback that a rule was not a requirement. This will allow for the use of the OSFI incident reporting form, although there may be cases where the OSFI form needs to

[1] The CCIR website says that "The objective of this Committee is to ensure the effective operations, maintenance and stewardship of the core elements of the cooperative supervisory framework developed by Insurance Core Principles Implementation Committee (ICPic) to increase alignment with the ICPs."

be supplemented, specifically because it lacks some data requirements around market conduct regulations.

Other issues raised by Mr. James were harmonization, cyber security and AI, and vulnerable customers. He said that there was good harmonization on prudential issues, but that, regarding market conduct issues, different regulators had to adjust their regulations to the expectations of their provincial governments. He took this to prove that there would never be complete harmonization across provinces in insurance. Later during the discussion, Mr. James returned to this theme and said that principles are often harmonized but details may differ from province to province, and that the CCIR is not a standard-setting organization.

Mr. James also mentioned the balance around the level of detail for regulation, stating that while industry asked for principles-based regulation, it often also asks for more detail on what the regulation actually entails. He added that BCFSA wants more clarity around insurer accountability for MGAs' activities. Mr. Reid added that in Quebec there is no need for dealing with MGAs as a separate license class, and that insurers bear the ultimate responsibility and risk for the behaviour of MGAs. The panelists said that insurers need to enforce FTC within MGAs.

In open discussion among the panelists, Mr. Reid said that the responsible use of AI is a priority for the AMF. Mr. James said that AI could help insurers but could also introduce biases and even barriers for consumers. Ms. Hiemstra said that FSRA is using AI to get data by scanning websites in search of possible licensing issues that are then investigated by humans. This has been a very successful project, and is saving about 250 hours of manual work per month.

Julien Reid said that the AMF is tapping into work done by the IAIS on vulnerable consumers. Erica Hiemstra spoke more about FSRA's work on MGAs, in particular organizations using a multi-tiered recruitment model. She said the life agent has a key role to play and that some of the MGAs' practices under investigation "reflect poorly on the whole industry." Some have sold universal life insurance policies to consumers that are not good fits for this coverage, which is very concerning.

On DEI, Harry James said that BCFSA is attempting to ensure that the agency's staff reflect the population it serves and expects the same commitment from industry. Julien Reid noted that the AMF gave over a year to industry to meet the new complaints requirements in Quebec.

Update from the Office of the Superintendent of Financial Institutions

Josée Turcotte Executive Director, Emerging Risk Operations Directorate

Ms. Turcotte said that the Office of the Superintendent of Financial Institution's (OSFI) Annual Risk Outlook (ARO) for 2024 to 2025 provides an overview of the current risk environment; context for the top risks the Canadian financial system faces; and OSFI's responses which supports its mandate to contribute to public confidence in the Canadian financial system and protect the rights and interests of depositors, policyholders, financial institution creditors, pension plan members, former members and entitled beneficiaries.

OSFI's ARO found four key risks to focus on in 2024-25:

1. Real estate secured lending and mortgage risks;
2. Wholesale credit risks;
3. Funding and liquidity risks;
4. Integrity, security, and foreign interference.

Other Key Risks of Focus for OSFI are:

- Housing market downturn and impacts on the mortgage insurance industry;
- Credit risks and market volatility and impacts on investment portfolios, asset liability management, and hedging strategies for all insurers;
- Earthquake, weather and flood risks and impacts on the P&C industry, as well as changes to life expectancy that impact both life insurers and pension plans;
- Cyber/Technology, climate, third party outsourcing, and transmission risk from the unregulated financial sector that impact operational resilience at institutions and pension plans;
- Outdated & emerging technologies (which increases vulnerability to threat actors and disruptions);
- Growing FRFI reliance on third parties (increases disruptions originating at third parties);
- Geopolitical & Foreign Interference Risk (increases threat activity and integrity and security vulnerabilities);
- Culture & behaviours and regulatory compliance programs (increases financial, operational, and reputational risks, and integrity and security vulnerabilities);
- Climate & growing transition risks (increases financial and operational risk).

Ms. Turcotte then spoke about OSFI's strategic plan, which has six dimensions:

- Priority 1, Expanded Mandate:
  - Develop approach to integrate I&S risk assessment into application & supervision functions;
  - Conduct analysis and risk assessments;
  - Develop report to Minister of Finance;
  - Identify potential amendments to I&S Guideline;
  - Respond to ad hoc I&S incidents.
- Priority 2, Supervisory Renewal:

    - Develop supervisory expectation tools;
    - Develop assessment criteria and tools to support integrity & security expectations;
    - Provide expertise relating to technical training and tools;
    - Timely & targeted supervisory activities.
- Priority 3: OSFI's Culture:
    - Support organizational culture initiatives and action plans;
    - Conduct Town Halls to foster team cohesion and culture;
    - Continue collaborative relationships with our partners.
- Priority 4: OSFI's Data Management and Analytics:
    - Develop, refine and launch data analytics for directorate risks, including risk metrics;
    - Develop, expand, and modernize several data calls;
    - Embed data driven intelligence.
- Priority 5: Critical Functions:
    - Conduct supervisory reviews, monitoring, and issues management;
    - FRFI risk assessment inputs;
    - Provide expertise on current and emerging risks;
    - Support legislative and approvals work through risk expertise and regulatory guidance inputs.
- Priority 6: OSFI's Operational Resilience:
    - Prepare Risk Control Self-Assessments, monitor division risks, and have effective risk mitigation strategies in place;
    - Support outreach strategy with stakeholders and partners, including security and intelligence agencies.

Ms. Turcotte then turned attention to her own department in OSFI, the Emerging Risk Operations Directorate (EROD), of which she is the Executive Director. She identified five major areas of focus for EROD:

- Culture & Compliance Risk Division (Identify FRFI-specific and industry-wide culture and compliance risks, trends and developments that may impact a FRFI's financial resilience);
- Technology Risk Division (Provide specialty technology and cyber risk expertise to ensure FRFIs are adequately managing tech & cyber risk to achieve op resilience);
- Climate Risk Division (Help FRFIs build awareness and capabilities to manage climate-related risks);
- Operational Risk Division (Provide specialty operational risk and resilience expertise to ensure FRFIs are adequately managing operational risk to achieve op resilience);
- Integrity & Security Risk Division (Ensure compliance with statutory requirements, monitor and supervise integrity & security risks).

In the execution of EROD's mandate, these risk divisions have the following roles and responsibilities:

- Policy Instruments & Tools, and New Applications (Support RAD to advance and administer a regulatory framework that promotes the adoption of policies and procedures related to nonfinancial and transverse risk management. Provide advice and support to RAD regarding new applications);
- Supervision, Reviews & Monitoring (Provide advice and support to Supervision Sector by carrying out monitoring, on-site examination, risk assessments, and early intervention activities at FRFIs, with respect to non financial and transverse risks);
- Incident Response Management (I&S, ORD, TRD) (Triage, investigate, assess, report, re: technology, cyber, integrity & security incidents);
- Data Driven Intelligence (Continuous data analytics, actionable risk insights, and reporting that support various EROD activities and initiatives).

The 2024-25 responses to the risks and trends are:

- Reviews and Monitoring (Integrity & Security (I&S) policies and procedures, third party, business continuity and disaster recovery, cyber, I-CRT, technology and culture & compliance);
- Policy and Other Developments (Operational Resilience and Operational Risk Management (E21), Culture and Behaviour Risk, Regulatory Compliance (E-13), Climate Risk Management (B-15), I&S amendments, Emerging Risk Bulletins, I&S report to the Minister);
- Supervisory Tools (Supervisory expectations (B-10, B-15, E-21, B-13 selfassessment), and risk assessment tools for culture and compliance, climate, I&S, and Culture Insights Tracker);
- Data Driven Intelligence (Climate and non-financial risk dashboards and metrics, third party data call, I&S information request, and Standardized Climate Scenario Exercise).

Ms. Turcotte then delved into each risk division, starting with the Climate Risk Division's (CRD) mandate, which is to help Canada's federally regulated financial institutions build awareness and capabilities to manage climate-related risks to enhance the safety and soundness of these institutions and strengthen public confidence in Canada's financial system. This mandate is fulfilled through policy instruments & tools and new applications; through supervision, reviews, and monitoring; and through data driven intelligence.

Ms. Turcotte noted that, in Canada, transition risk is increasing due to new policies designed to curb Canada's GHG emissions. Lenders have exposure to the carbon intensive sectors and technologies targeted by these policies, while insurers are significant investors in the Canadian economy, including the emissions intensive resource sector. FRFIs are in the early stages of quantifying the impacts of climate-related risks.

Specific initiatives for the CRD include:

- Finalize Guideline B-15 supervisory expectations and provide training;
- Develop supervisory dashboards, analytics, and/or tools for climate risk assessments;
- Monitor FRFIs' readiness to meet climate risk return filing expectations;
- Conduct Standardized Climate Scenario Exercise and publish results;
- Influence global and domestic standards and practices pertaining to climate risk.

It was noted that climate-related risks are drivers of other risks for FRFIs, with the potential to affect all asset classes across all portfolios. The unexpected timing and severity of climate change impacts create challenges around the ability to predictably price the risk over the long term. Investment portfolios are also increasingly at risk due to climate-related regulatory risks, market risks, technological changes, and reputational risks. There is the potential for increases in climate-related mortality and morbidity rates, heat-related health issues associated with extremes in weather events, especially where excessive heat may compound pre-existing health conditions or vulnerabilities (e.g., elderly populations), long-term respiratory illnesses due to wildfires and increased pollution, and increased spread of infectious diseases.

As well, climate prudential expectations are increasing, including:

- Guideline B-15 updated to reflect IFRS S2 and comes into effect year end 2024 for Internationally Active Insurance Groups;
- Mandatory climate related disclosures phased in starting in 2025;
- Standardized climate scenario analysis exercise due later this year;
- Mandatory climate risk data return effective 2025.

The Culture & Compliance Risk Division's (CCRD) mandate is to provide expertise in identifying and assessing culture and compliance risks in FRFIs. Ms. Turcotte said that FRFI's culture can be a competitive advantage or an accelerant for reputational risks in the evolving risk environment. Strong and well-developed risk measurement, management, and internal challenge functions are critical to the ongoing financial and operational resilience of all FRFIs.

On June 22, 2023, Parliament passed Bill C-47, expanding OSFI's mandate to ensure FRFIs have adequate policies and procedures against threats to their integrity or security, including foreign interference. There are intersections between integrity, security, and broader non-financial risks, such as cultural and behavioural risk.

Among the initiatives EROD has in this area:

- FSB Compensation Monitoring Contact Group (CMCG) biennial report;
- Update Guideline E-13: Regulatory Compliance Management;
- Finalize Culture & Behaviour Risk Guideline (fall 2024).

Key considerations at EROD and OSFI around culture are:

- Appropriate frameworks and structures should be in place to meet OSFI's expectations for FRFI's management of culture and behavior risks when the Culture and Behavior Risk Guideline is released;
- OSFI's focus on culture is from a prudential perspective and the extent to which it impacts sound decision-making, prudent risk-taking and effective risk management;
- Cultural risks, if not effectively managed, could negatively impact a FRFIs overall resilience.

Key considerations around compliance are:

- Heightened regulatory scrutiny due to increasing and more complex regulations; and operations in multiple jurisdictions;
- Regulatory scrutiny is also leading to increased enforcement action by regulators (i.e., fines/penalty) and public naming of FRFIs which also has reputation risk impacts;
- Across the industry there is elevated execution risk and regulatory change management risk due to the high number of competing BAU priorities and high pace of change in the regulatory environment.

The Operational Risk Division's (ORD) mandate is to provide operational risk and resilience expertise for guidance and to identify FRFI-specific, industry-wide, and/or sector-specific operational risk management trends and developments that impact a FRFIs operational resilience. These include:

- Institutions increasingly rely on third parties, including suppliers with dominant market positions.
- The number and severity of disruptive events impacting operations of financial institutions is rising, underscoring the importance of operational resilience.
- The percentage of disruptions originating at third parties is on the rise.

Among the ORD initiatives taking place:

- Finalize and publish Guideline E-21 (Summer 2024);
- Develop E-21 expectations for front line supervisors;
- Enhance and expand the third-party data call in collaboration with the industry;
- Modernize and expand to larger insurers the loss data collection (implementation 2025-26);
- Develop the non-financial risk metrics data call for larger insurance companies and banks (implementation 2025-26).

Ms. Turcotte noted some important ORD considerations:

- B-10 – Third-Party Risk Management
    - Use of third parties continues to accelerate within the life insurance sector, including dominant third parties providing cloud services, actuarial valuation software, financial data and analytics, etc.
    - Important to identify critical third parties and continually enhance third-party risk management programs.
- E-21 – operational risk management framework
    - Important to identify critical operations to focus efforts appropriately and effectively;
    - Importance of recovery plans and BCPs;
    - With rise in the frequency and severity of disruptions, life insurers need to have robust and tested disaster recovery and business continuity plans to ensure that they can recover critical systems from severe disruptions in accordance with their tolerance for disruption.

The Technology Risk Division's (TRD) mandate is to provide specialty technology and cyber risk expertise in identifying FRFI-specific risks, industry-wide risks, and/or specific trends and developments related to technology and cyber risks that may impact a FRFIs operational resilience. The TRD fulfils its mandate through some of the approaches noted for other divisions and through some additional approaches:

- Policy instruments & tools and new applications;
- Supervision, reviews, and monitoring;
- Data driven intelligence;
- Incident Response Management;
- External & internal stakeholder affairs.

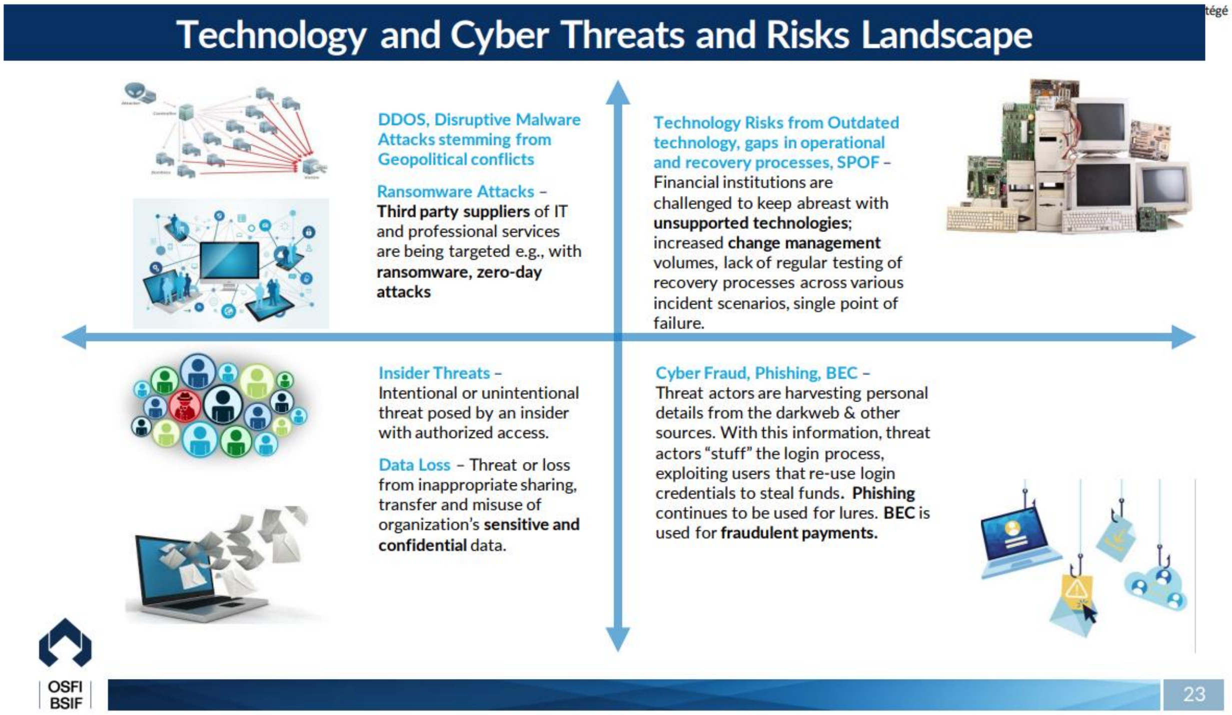
Changing and evolving technology, partnered with greater dependence on third party technology providers, have increased both the attack surface and cyber risk. The tactics used by nation states and non-nation state cyber actors have brought heightened attention to cyber risks due to geopolitical events. Outdated technology, weak disaster recovery capabilities, and failed information technology implementations continue to underscore the importance of operational resilience.

TRD initiatives are:

- Ongoing enhancement of incident response processes;
- Replace CSSA with B-13 self-assessment;
- Enhance data analytics and reporting of risks and metrics;
- Continue to develop supervisory tools;
- Issue emerging risk bulletins on: Quantum, AI, and Block Chain.

Ms. Turcotte then presented a technology and cyber threats and risks landscape (see Display 1).

Display 1: Technology and Cyber Threats and Risks Landscape

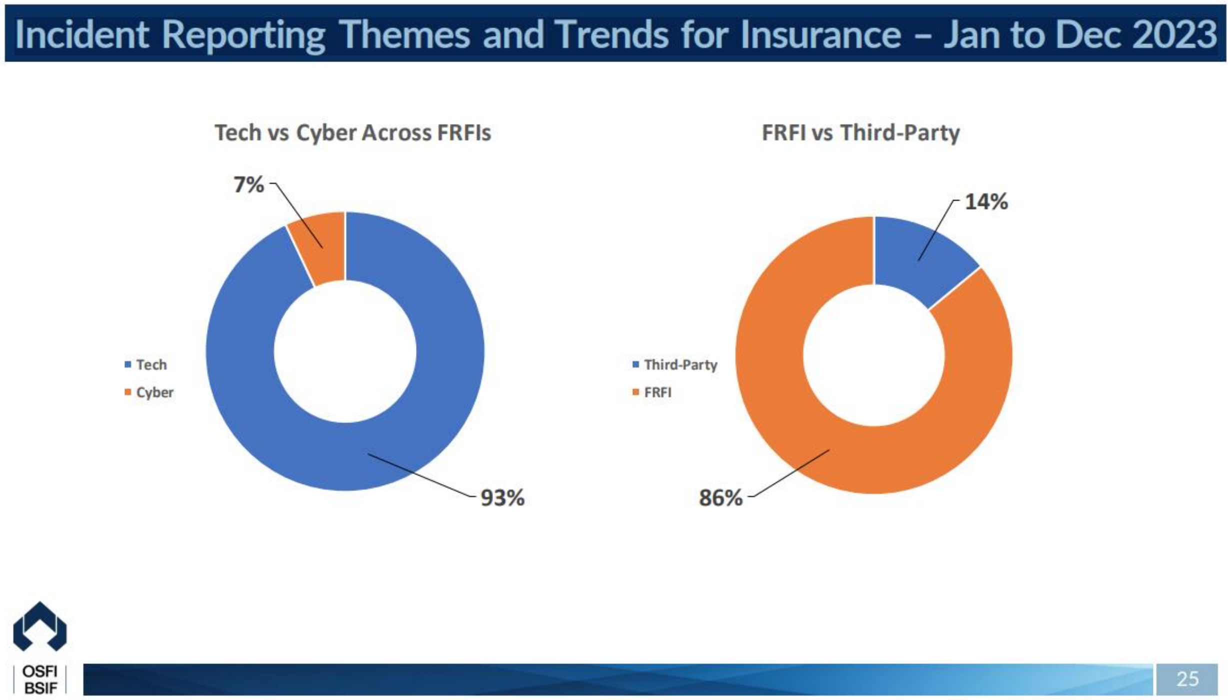


Ms. Turcotte said that there are tools and resources that can be used by industry to help them navigate these issues:

- Technology and Cyber risk management Guidance B-13
    - Published July 2022
    - Effective January 2024
- Tools and Advisory
    - Cyber Security Self-Assessment
    - Technology & Cyber Incident Advisory
    - Intelligence Led Cyber Resilience Testing (I-CRT) Framework – issued April 2023
- Cyber Intelligence and Technology Bulletins
    - Multi-Factor Authentication
    - APIs
    - Ransomware
    - Cyber and subcontracting risks

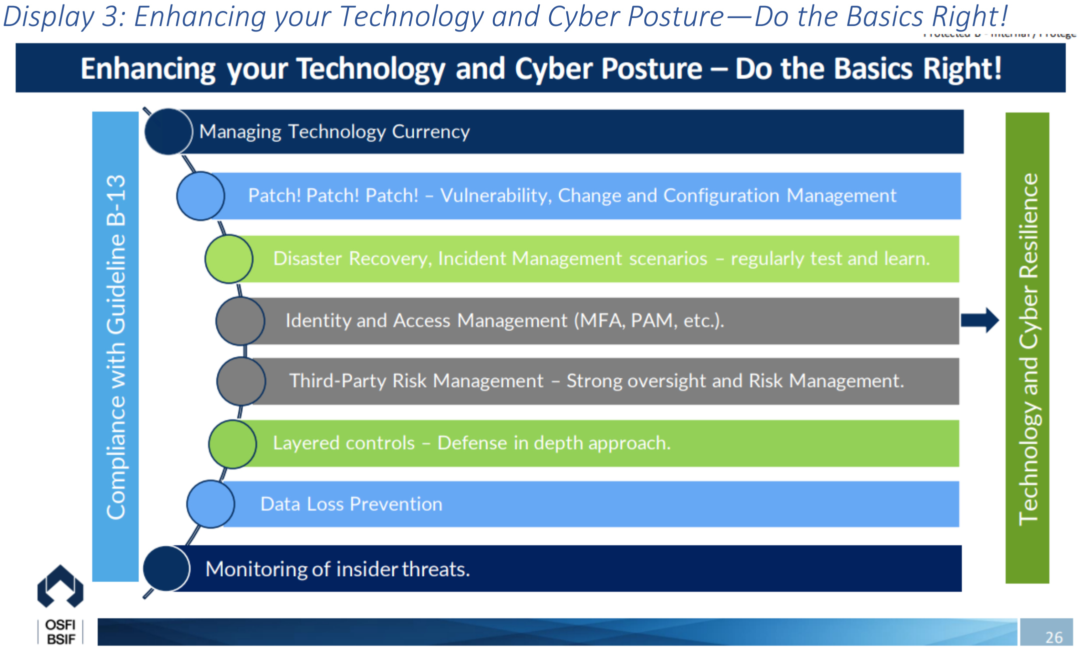
Ms. Turcotte then summarized themes and trends for insurance around these issues (see Display 2).

Display 2: Incident Reporting Themes and Trends for Insurance – Jan to Dec 2023



Ms. Turcotte also presented some suggested basics around "doing the right thing" to protect companies against some of these threats (see Display 3).

Display 3: Enhancing your Technology and Cyber Posture—Do the Basics Right!



The Integrity & Security Risk Division's (ISRD) mandate is to examine FRFIs to determine whether they have adequate policies and procedures to protect themselves against threats to their integrity or security, including foreign interference, and to report, at least annually, to the Minister of Finance.

Geopolitical events may trigger increases in foreign interference, malicious activity, and/or undue influence, potentially impacting the integrity or security of FRFIs. Outdated and emerging technology (e.g., AI and quantum computing), cyber vulnerabilities, and a greater dependence on third-party service providers have increased both the attack surface and cyber and physical threats. Evolving regulatory environment increases the likelihood of FRFI non-compliance (integrity or security).

Among these divisions initiatives are:

- Development of assessment criteria and supervisory tools to assess FRFI adherence to integrity and security expectations.
- Identify potential amendments to Integrity and Security guideline based on Supervisory assessment results.
- Revise FRFI Information Request template based on maturing supervisory approach.

The summary of expectations around integrity can be found in Display 4.

Display 4: Summary of Expectations—Integrity

Summary of Expectations – Integrity

Principle	Associated guidelines	New expectation	Expanded expectations
1. Character	E-17 Background Checks on Directors and Senior Management (E-17)	N/A	Character of responsible persons as demonstrated through their actions, behaviours, and decisions.
2. Culture	Draft Culture and Behaviour Risk Guideline	N/A	Culture reflects a commitment to norms that encourage ethical behaviour.
3. Governance	Corporate Governance Guideline E-4 Foreign Entities Operating in Canada on a Branch Basis	N/A	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. Compliance	E-13 Regulatory Compliance Management (E-13)	N/A	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.

OSFI BSIF 29

The summary of expectations around security can be found in Display 5.

Display 5: Summary of Expectations—Security

Summary of Expectations – Security

Principle	Associated guidelines	New expectation	Expanded expectations
5. Physical premises	B-13 Technology and Cyber Risk Management (B-13) Draft E-21 Operational Resilience and Operational Risk Management (E-21)	Standards and controls for physical buildings, office spaces, physical file storage, and technical security inspections.	N/A
6. People	E-17	Risk-based background checks on all employees and contractors, as appropriate to the role.	N/A
7. Technology assets	B-13	N/A	Enhanced description of what constitutes malicious actions towards IT infrastructure.
8. Data and information	B-13 and Draft E-21	Data classification considers vulnerability to malicious activity, undue influence, or foreign interference.	Personnel access requirements to prevent undue influence and foreign interference.
9. Third-party risks	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.	N/A
10. Undue influence, foreign interference, and malicious activity	E-13	Notification to OSFI when a report is made to RCMP, CSIS, or other authorities regarding undue influence, foreign interference, or malicious activity.	N/A

OSFI has adopted a phased approach to implementation:

- Immediately: FRFIs should notify OSFI of reports to law enforcement or CSIS.
- By July 31, 2024: FRFIs should submit a comprehensive action plan for OSFI's review where they do not meet expectations, including interim deliverables to achieve compliance.
- By January 31, 2025: All expectations should be met except background checks.
- By July 31, 2025: Expectations for background checks should be met.

It was noted that the integrity and security guideline apply to both banks and insurance companies. Life insurers maintain personal data on Canadians which needs to be safeguarded. As well, insurers may be targeted by bad actors looking to use products/services and data for unlawful activities. Additional risks being monitored are IFRS-17; Computing/Model Risk – Guideline E-23; and artificial intelligence.

In terms of IFRS 17:

- Insurance industry successfully transitioned to IFRS 17;
- Insurers continuing to refine their processes to achieve business at usual state;
- Increased focus on refining accounting and actuarial policies underpinning the financial statements;

- Performance metrics continue to be refined;
- IFRS 17 metrics being collected through the L4 will be reviewed including liaising with industry at the appropriate time.

In terms of computing/model risk considerations:

- The number and complexity of models has rapidly increased across the insurance industry
  - Uses span underwriting, pricing, risk segmentations, financial reporting, risk management, capital management etc.;
  - Actuaries are no longer the only model experts and users - data scientists, statisticians, software engineers are developing and using models.
- Model risk has increased and has given rise to other risks (e.g. legal, ethical, data privacy, 3rd party, etc.).
- OSFI is enhancing its Enterprise Model Risk Management guideline (E-23) to reflect the change in a modeling landscape (i.e., increasing scope and coverage, including AI/ML considerations, focus on enterprise view and proportionality).
- Model governance is a critical oversight function that should be seamlessly integrated into broader enterprise risk management framework. Key components include:
  - Policies and procedures (accountability);
  - Performance monitoring and reporting;
  - Model inventory;
  - Training and awareness;
  - Model development and validation;
  - Documentation;
  - Model risk rating;
  - Change Management.

A Fireside Chat with the CLHIA President Quebec Affairs

Lyn Duhaime, President Quebec Affairs and Senior Vice President, Marke Conduct Policy and Regulation, CLHIA; Susan Murray, Vice-President Government Relations and Policy, CLHIA; Moderated by John Burns, Vice President and Chief Compliance Officer, Securian Canada

Lyn Duhaime noted that it is a challenging time in Ottawa, with a minority government in power through a supply and confidence agreement with the NDP, leading to some policies that are not favourable to industry. In CLHIA's opinion, Bill C-64 is not a good policy initiative because it could undermine some private employee plans. National Pharmacare is not desired in Quebec and is extremely expensive. CLHIA believes that there are better ways for the federal government to achieve its objectives. CLHIA will table 18 amendments to the Bill.

Virtual health care is permitted in Quebec. While the province wishes this to continue, other provinces are less enthusiastic. This is generally only offered privately, as opposed to through group benefits. There is also legislation in Quebec to reduce the administrative burden on doctors, which could have an impact on insurers.

There is a long and growing list of OSFI requirements, leading to concerns of overregulation and slowing innovation. Many of these expectations relate to known risks which are already being monitored. Work is continuing through the CCIR on segregated funds to align that sector with mutual funds, including around "Know Your Customer."

MGAs will continue to get more regulatory attention. The CLHIA's view is that MGAs should be recognized in legislation.

Artificial intelligence will increasingly be on the radar screen of regulators; both the AMF and OSFI are already focusing on it.

MGA and Advisor Panel: How Organizations Screen and Monitor for Advisor Suitability, Market Conduct and Advisor Reviews

Aly Damji, VP Wealth Management, HUB Financial; Donna Spagnola, Partner, Borden Ladner Gervais LLP; Amanda Mulder, Director, Risk & Compliance, The Canada Life Assurance Company; Teri Ryan, AVP and Chief Compliance Officer, Equitable Lie; Kandace Hopkins, Director, Practice and Quality Assurance, Insurance Council of BC; Dylan Brown, Financial Planner, Financial Confidence

It was noted that FSRA expects all life agents, in MGAs or otherwise, to comply with all regulations, including the Fair Treatment of Customers (FTC). Agents need to be competent, capable, and knowledgeable. While MGAs will be under increasing scrutiny, and should have compliance functions, regulators will still expect that ultimate responsibility for their actions to remain with insurers. Kandace Hopkins noted the various actions that the Insurance Council of BC undertakes to ensure MGAs comply with regulations, including webinars, courses, and audits. Some agents do not understand the products that they are selling and who they are supervised by, which is a problem. Terri Ryuan said industry needs to do more to "hit the mark for success," meaning that advisors need to have the right tools in place to serve their customers and incentive programs with potential conflict of interest need to be examined more carefully. Regulators are and should continue to challenge industry to be more thoughtful about these issues.

Amanda Mulder said that her company reviews MGAs to ensure that proper controls are in place. Aly Damji said that not all MGAs should be painted with the same brush, and that carriers also have different criteria for evaluating MGAs. He said that basic tools like "reason why" letters need to be used as a standard. Another complication is the lack of harmonization across provinces around regulatory expectations for MGAs, and life insurance audits differ from province to province. There was a consensus that audits should be simplified. When books of business move, it is important to evaluate whether it is due to a new, better product in the marketplace or simply a new incentive program that provides an enticement to advisors to move business. There is an increasing trend of insurers purchasing MGAs. However, the expectations of MGAs should remain the same whether they are owned by an insurer or are independent.

Principles-Based Regulation

Christie Ford, Professor, Allard School of Law, University of British Columbia

Christie Ford, who participated previously in a CAFII webinar on principles-based regulation, said that taking such an approach does not mean industry has "carte blanche." Discretion must always be practiced, and there must always be a level of balance between principles and prescription. However, as a foundation for regulation, principles-based approaches have real, meaningful benefits.

A principles-based approach requires an effective underlying foundation, including excellent communication and credibility of all the stakeholders. Ultimately, success in this approach is based on mutual trust—that industry will be sincere and that regulators will not be looking to immediately punish errors. FSRA is the best-known Canadian provincial principles-based regulator, but Quebec and New Brunswick also emphasize their commitment to this approach.

There are some cases where a clear rule may be preferable to a principle like "be reasonable and prudent" when driving as opposed to setting specific highway speed limits. Rules are also simpler to adhere to for industry because they are clear, predictable, and consistent. However, they can also be rigid, restrictive, unfair, and lacking contextual information. Principles, on the other hand, are flexible, adaptable, nuanced, and require discretion.

While every regulatory system will be a combination of both approaches, a focus on principles leads to better regulatory outcomes if implemented effectively. It would be better to keep statutes high level to allow regulators and regulation to fill out the details. Nevertheless, rule-making authority is necessary for a principles-based regime; it gives the regulator regulatory discretion and provides a final recourse for bad players.

Because it is much more than checking boxes on a list, effective implementation of a principles-based approach requires proper resourcing and judgment. Ultimately, it is about a regulatory culture that is founded on collaboration and communication. Everyone desires clarity, but it is more effective to "figure out the best approach" collaboratively. Smaller industry players may find it hard to succeed in such an environment, and they may prefer a more rules-based approach. But, for larger players, an approach that is not based on a compliance mindset and which is focused on culture is more effective. This, however, requires an investment to make such an approach work, including better data and a better understanding of risks in the business. This also ultimately allows regulators to focus their enforcement activities on bad actors.

Much like dealing with a teenager, if industry shows that it can be trusted, the regulator will be open to a principles-based approach; if industry bends the rules and is not acting in good faith, hard and fast rules are more likely to be used.

May 23, 2024

AI and the Insurance Industry

Mary Carmichael, Director, Risk Advisory, Momentum Technology

Ms. Carmichael defined AI as the "ability for a computer to think, learn and simulate human mental processes, such as perceiving, reasoning, and learning" as well as "independently performing complex tasks that once required human input." In terms of different types of AI applications, she listed the following:

- Predictive analytics;
- Machine vision;
- Natural language processing (NLP);
- Robotics/Autonomous cars;
- Automation & AI (e.g. RPA);
- Generative AI.

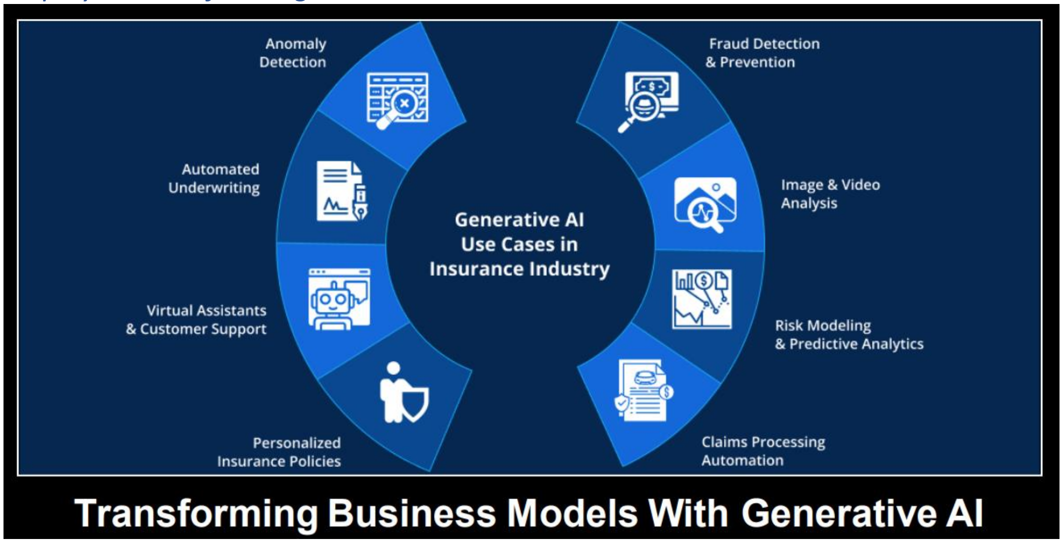
Currently, it is generative AI that is capturing the most attention. This application is a type of AI that generates prompt output in the form of text, video, audio, and/or images based on raw or training data using large language models (LLMs). A Large Language Model (LLM) is a machine learning model engineered to comprehend, generate, and manipulate human-like text through a training process involving vast datasets. LLMs use neural networks, inspired by the human brain, to learn patterns from datasets, enabling accurate text prediction to generate relevant responses.

In terms of the potential impact of AI in the insurance industry, Ms. Carmichael quoted Bill Fandrich, Executive Vice President of Technology and Operations, Blue Cross Blue Shield of Michigan:

> *Generative AI's strength is its ability to aggregate and tailor information to individual circumstances, providing insights at the right moment to support decisionmaking for our customers. This reduces administrative load and the frustration typically associated with manual research.*

Ms. Carmichael illustrated the ways in which this technology could transfer business models (see Display 6). These business models are transformed by enabling deeper customer intimacy through personalized services; by achieving operational excellence via process optimization; and by fostering product leadership with innovative, data-driven offerings.

Display 6: Transforming Business Models with Generative AI

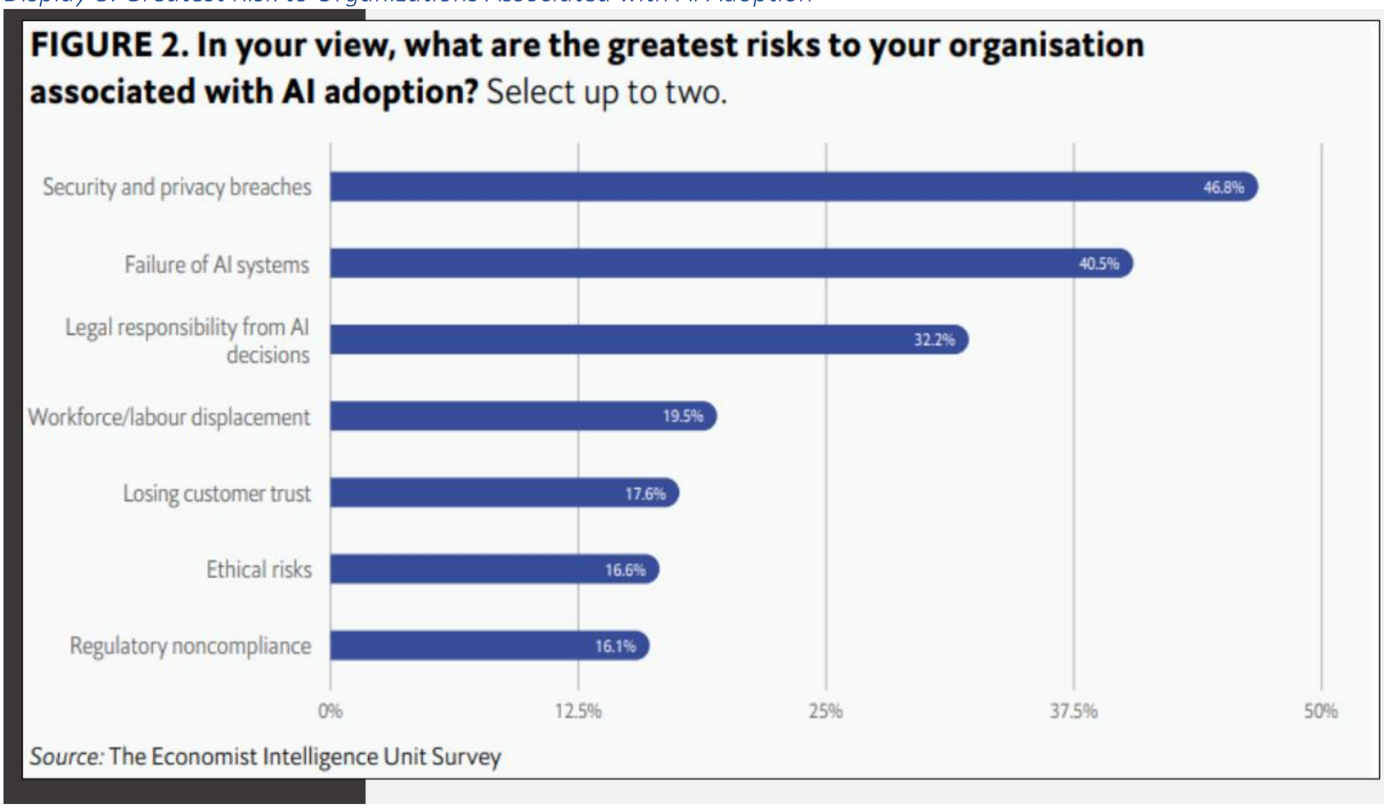


Examples of how these changes have produced benefits are demonstrated by Display 7.

Display 7: Benefits Measured

However, with these benefits come risks, including "hallucinations," that some AI models have suffered from. A list of risks from AI can be found in Display 8. Ms. Carmichael said that AI chatboxes can hallucinate 3-27% of the time, leading to incorrect or misleading responses. Air Canada experienced this when its AI chatbix promised an incorrect discount which they then had to honour. To deploy AI wisely, "companies should implement guardrails, fine-tuning, action models, and hallucination prevention to minimize risks in AI-driven customer experiences."

Display 8: Greatest Risk to Organizations Associated with AI Adoption



Ms. Carmichael also quoted the Financial Industry Forum on Artificial Intelligence (Canada):

> *The rapid advancement, proliferation, and transformative nature of artificial intelligence (AI) technology has accentuated the need to consider the ethical, legal, financial and social implications of its development and deployment. This is where well-designed risk management practices come in, comprised of robust testing and evaluation frameworks, implementation of clear and transparent decision-making processes, and creation of mechanisms for accountability and redress in the event of harm.*

The Role & Responsibilities of the Chief Compliance Officer – Legal and Regulatory Update – What you need to know

Jill McCutcheon, Partner, Torys; Melissa Prado, Partner, Torys

A key issue reviewed in this presentation is the risk of personal liability of chief compliant officers. A key case that was reviewed is the review of the Financial Services Tribunal of the findings of the AMF against World Financial Group, the same MGA that has also been investigated by FSRA and whose Chief Compliance Officer will now be April Stadnek, formerly the Executive Director of the Insurance Councils of Saskatchewan.

The Tribunal didn't agree with all the assertions made by the AMF, but it did find that WFG failed to have an adequate system of compliance and oversight for its representatives. Of particular interest to the compliance community were the Tribunal's conclusions about the personal liability of the compliance manager and the CCO/responsible officer in Quebec.

The AMF also sought a prohibition on the chief compliance officer and the compliance manager from acting as responsible officers of a firm for five (5) years and an administrative penalty of $50K and $25K, respectively.

Section 85 of the Distribution Act ("LDPSF") states that:

> *A firm and its executive officers shall oversee the conduct of the firm's representatives. They shall ensure that the representatives comply with this Act and the regulations.*

With respect to the compliance manager, the Tribunal found that:

- The manager was an employee who was always subordinate to the CCO;
- He performed his duties under the supervision of the CCO;
- The CCO retained his responsibilities;
- As such, he was a manager not an "officer" within the meaning of Section 85 of LDPSF.

With respect to the CCO, the Tribunal found that:

- He was an officer within the meaning of Section 85 of the LDPSF;
- As such he was responsible for ensuring that there is a system in place to supervise representatives to ensure that they comply with the Act and the regulations;
- Once the Tribunal found that WFG had breached the LDPSF for not having an adequate system of supervision, then the Tribunal said it had no choice but to find the CCO as an executive officer of the firm also liable.

The Tribunal did not grant the AMF its request to ban the CCO from acting as a responsible officer nor did it levy a $50K AMP on the CCO, but it did impose a $20K AMP on the CCO.

The presentation then looked at other cases against CCOs in the US and the UK and concluded that international cases demonstrated that there is an increase in enforcement actions brought against CCOs in many jurisdictions across many industries. Two main categories of cases where CCOs have been found personally liable are 1) where the CCO was found liable due to misconduct/obstructing regulators, and 2) where the CCO was found liable due to compliance function/system failures. A key legal issue is whether the CCO role is supervisory or advisory.

The presentation then focused on the roles and responsibilities of the CCO. Under the three lines of defence model, CCOs are part of the second line of defence. Under OSFI Guideline E-13, the CCO is responsible for:

> *assessing the adequacy of adherence to and effectiveness of the FRFI's day-to-day controls, and opining on whether, based on the independent monitoring and testing conducted, the RCM controls are sufficiently robust to achieve compliance with the applicable regulatory requirements enterprise-wide.*

The presentation suggested that the key elements of the CCO role are:

- Advise and inform the board of directors and senior management regularly about the financial institution's compliance with laws, regulations and guidelines, and any material deficiencies identified;
- Provide his opinion on the adequacy, observance and effectiveness of controls at all levels of the financial institution;
- Ensure that identified material compliance risks are validated with senior management and the board of directors so that these risks correspond to the level of sensitivity and priority they have established, and recommend any adjustments;
- Refine mandates and cultivate effective collaborative relationships with operational managers and oversight officers in the second line of defense, in particular with regard to developing policies for material compliance risks;
- Implement an escalation procedure for material compliance risks based on criteria predetermined by senior management and approved by the board of directors
- Report regularly to the board of directors or to the audit committee, the compliance committee or any other relevant committee;
- Meet privately at least once a year with the board of directors or with the chair, without senior management in attendance, to confirm, among other things, his independence within the financial institution and discuss certain issues and any points of disagreement with senior management.

The presentation made frequent reference to the chronic underfunding and under-resourcing of compliance departments, and the challenges this raised for the CCO. In terms of practical advice on how to avoid personal liability, the following are suggestions made:

- The obvious answer: avoid non-compliance;
- Understand the scope of your role and what are your responsibilities;
- Document and keep good records;
- Make sure your compliance programs are complete and up to date;
- Act on information immediately;
- Keep your skills up to date – look at education as iterative;
- Never attempt to conceal wrongdoing from regulators;
- Foster a strong culture of compliance within the organization;
- Monitor third parties;
- Make sure the organization's D&O insurance will respond
    - Are you an officer, are you covered?

Building an Inclusive Insurance Industry: A look into Gender Diversity and Why a Diverse, Equitable and Inclusive Culture is Fundamental to our Business

Diana Phillips, Manager, Regulatory Compliance, Pacific Blue Cross; Kai Scott, President and Gender Strategist, TransFocus Consulting Inc.; David Simmons, SVP, Global Chief Communications and Sustainability Officer, Canada Life and Great West Lifeco.

In a wide-ranging discussion on inclusion, the panelists spoke about challenges in the work environment and ways to overcome those challenges. Education and sharing information were key parts of this. Even if some of those discussions can be awkward, openness and a willingness to learn can make this process much easier. Ultimately, this is about treating people fairly and about overcoming biases. There are fundamental misunderstandings that need to be addressed, including, for example, that sex and gender are not the same.

Business resource groups (BRGs) are an important way to address these issues and lead to increased knowledge and comfort.

Data Analytics in Compliance/Complaints and Client Experiences

Nancy Carroll, Senior Counsel and Co-Chair, National Insurance and Reinsurance Group, McCarthy Tetrault; Parama Ray, AVP AI and Data Analytics, the Canada Life Insurance Company; Robert Bartman, AVP Client Service Optimization & Advocacy, Sun Life.

The panelists focused on how client problem data has been used, what they are currently working on, and how they envision the future unfolding. It was noted that as recently as 2017 collection of problem data was very limited, but this has changed and now the focus is on predictive models that allow companies to fix problems before they impact customers.

Future trends in data analytics include using natural language analysis to review case notes and lead to client problem themes; using data to understand the impact of new developments, for example, the AMF's new client problem handling protocol on our problem resolution teams; and detecting anomalies in the types of interactions we're having – what unusual but common questions or problems are we hearing from our clients.

It was noted that with increasing digitization, and despite recent efforts to beef up cybersecurity, data breaches — in which hackers steal personal data — continue to increase year-on-year: there was a 20% increase in data breaches from 2022 to 2023. Some of the trends around this uptick are disturbing. For example, globally, there were twice the number of victims in 2023 compared to 2022. The impact of cybercrime is expected to reach $10 trillion this year, surpassing the GDP of all countries in the world except the U.S. and China. Furthermore, the figure is estimated to increase to nearly $24 trillion in the next four years. Although the short-term impacts of a cyberattack on a business are quite severe, the long-term impacts can be even more important, such as the loss of competitive advantage, a reduction in credit rating, and an increase in cyber insurance premiums.

Among the ways to address these risks are compliance attestations, vulnerability aging reports, and mean-time-to-detect statistics. At the front-end, there is a need to bring greater visibility to organizations' inherent risk levels — essentially, "What are we being asked to defend?" There is also a need for much greater transparency, accuracy, and precision around how we perform against likely threats and whether we do so consistently across the attack surface. Finally, there is a need to plan for and measure performance against low probability high consequence events.

Simple measures are to collect only the data you need, to have strict protocols about who has access to what data, to anonymize and aggregate data, and to destroy data when you no longer need it.

Although sophisticated hackers and AI-fueled cyberattacks tend to dominate the headlines, one thing is clear: The biggest cybersecurity threat is human error, accounting for over 80% of incidents. This is despite the exponential increase in organizational cyber training over the past decade, and heightened awareness and risk mitigation across businesses and industries. AI could help in this area by keeping humans in check.

There is currently a great deal of interest in AI-driven cybersecurity, with estimates suggesting that the market for AI cybersecurity tools will grow from just $4 billion in 2017 to nearly $35 billion net worth by 2025. These tools typically include the use of machine learning, deep learning, and natural language processing to reduce malicious activities and detect cyber anomalies, fraud, or intrusions. Most of these tools focus on exposing pattern changes in data ecosystems, such as enterprise cloud, platform, and data warehouse assets, with a level of sensitivity and granularity that typically escapes human observers.

Supervised machine-learning algorithms can classify malignant email attacks with 98% accuracy, spotting "look-alike" features based on human classification or encoding. Deep learning recognition of network intrusion has achieved 99.9% accuracy. Natural language processing has shown high levels of reliability and accuracy in detecting phishing activity and malware through keyword extraction in email domains and messages where human intuition generally fails

Complaint Trends (Members Only) Workshop A-1

Nathalie Barbosa, Sun Life; Robert Bartman, Sun Life

The workshop, structured as an open dialogue and Q&A opportunity, asked the question: what types of complaints are insurers seeing day-to-day and what are the best ways to address them? Answers were given anonymously via electronic submission and then discussed as a group.

The first question – what type of complaints and/or trends are insurers seeing often – received the following responses:

- Service;
- Claims;
- Sales practices;
- Coverage;
- Poor understanding of policy/policies;
- Premium concerns;
- Appeals;
- Advisor services issues and complaints;
- Privacy and personal information concerns;
- Unpaid claims;
- Claims processing time;

Not all the answers were discussed but the overall conclusion was that clients are expecting a different level of attentiveness and information now. They want faster, sooner, and more in terms of options, communication, responsiveness, and clarity. The other conclusion the workshop drew was that clients are quicker to immediately escalate their concerns and complaints to the executive level if they find that their issues are not receiving the attention they believe it deserves. This is also true if their complaint(s) go unanswered. Part of this issue comes from confusion and misinformation around advisor services and client tools.

The next question asked, on average, what is the clients' knowledge base? Generally, insurers see misinterpretations and misunderstandings due to a lack of plain language and client inattentiveness. In short, clients are not reading the fine print. In the same vein, clients may not be aware of the avenues available to them for disputation; thus, they incorrectly contact doctors or executives for help. Many insurers vocalized that this has happened with paid claims.

Insurers also answered that clients are impatient with the appeals process and jump to complaints, thereby complicating everything and delaying the process. This may be due to misinformation or inattentiveness. Some expressed a growing belief that a culture of apathy is developing, in which policies are seen as no longer mattering because clients simply do not read or take the time to understand their policies. Instead, they just expect payments quickly.

The moderators then asked what trends and challenges are anticipated for 2024-25. The following answers were given:

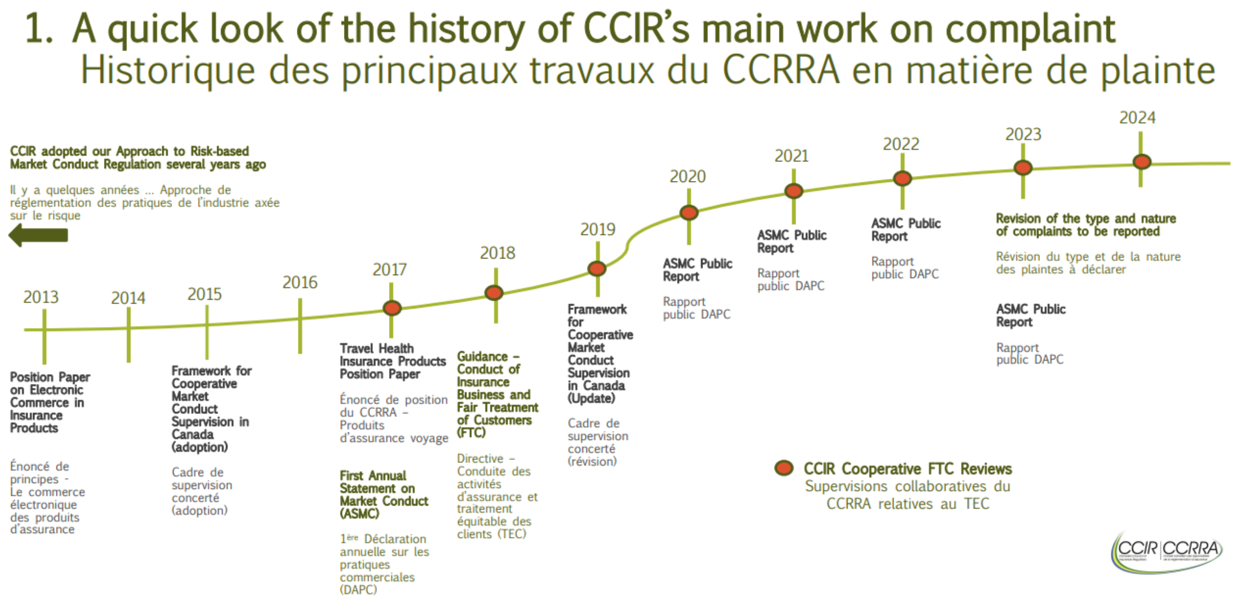
- Adequate assistance of vulnerable clients, including the development of policies and procedures to aid this. Companies then need to train their employees in whatever fair treatment of vulnerable customers framework they develop.
- Quebec and the AMF:
    - Complaints regulation and service delays from the AMF. Many are awaiting the publication of supporting material from the AMF, which agencies will then need to implement. Insurers are wondering what an acceptable extension to their service timeline is as outlined in the AMF's complaint regulation.
    - Understanding the differences between implicit and explicit communication of complaints, including the optional 20-day simplified process.
    - The file request timeline. Insurers expressed that a 60-day period makes a big difference when exchanging information with intermediaries.
    - Challenge of potentially providing Quebec clients with preferential treatment cause of the AMF's new requirements.
- Quebec disability claims. Historically, insurers have been allotted months to provide supporting documentation; however, there has been no recent guidance on this issue.

A Fireside Chat: What the CCIR is doing related to Complaints

Véronique Martel, Director, Supervision – Commercial Practices, AMF Directrice de la surveillance des pratiques commerciales, Autorité des marchés financiers and Erica Hiemstra, Head Insurance Conduct – Market Conduct, FSRA

The presentation began with an overview of the CCIR's approach to complaints. Ms. Martel then presented a historical view of the major milestones at CCIR on complaints (see Display 9).

Display 9: A Quick Look at the History of CCIR's Main Work on Complaints



Recently, the type and nature of complaints to be reported were revised, which led to a consultation with industry that began in February 2023 and ended in May 2024 with a survey of industry. Industry will have a period of transition to adopt the new approach.

Ms. Martel acknowledged that improvements were needed to the Annual Statement on Market Conduct (ASMC) and that efforts were being made to make it easier to use. The ASMC allows regulators and the CCIR to use data to identify and analyze industry trends .

Erica Hiemstra spoke about the CCIR's OmbudService Oversight Standing Committee (OOSC), with the following mandate:

> *To ensure that third party dispute resolution systems in the insurance sector, including OLHI and GIO, fulfill the public interest objectives of complaint resolution as an important component of a well-functioning consumer protection policy framework.*

The CCIR OOSC was created in 2015 when CCIR assumed oversight of the Insurance OmbudServices Cooperation and Oversight Framework (the Oversight Framework). The Oversight Framework was initially adopted in 2007 when the Joint Forum was fulfilling the oversight role and it included OBSI in addition to OLHI and GIO. In 2015, when FCAC assumed oversight of OBSI, CCIR took over the oversight of the Framework with OLHI and GIO under OOSC.

Ms. Hiemstra stated that market conduct is a provincial jurisdiction and that the CCIR needs confidence in the Independent Dispute Resolution (IDR) mechanism. The insurance consumer in Canada requires an effective IDR mechanism. CCIR, OLHI, GIO and the industry (through CLHIA and IBC) have an opportunity to build on the current IDR mechanism and update the Oversight Framework to ensure effective oversight and accountability.

Ms. Hiemstra appeared skeptical about the work of OLHI, especially around the IDR mechanism, asking if it is "delivering on its purpose?" The framework, in particular, needs some significant updates. Regulatory confidence in OLHI is essential, she stressed. OLHI needs to demonstrate that it is fulfilling its primary purpose of handling and resolving disputes between companies and consumers. FTC expectations have evolved and OLHI needs to reflect that as well.

Ms. Hiemstra then reviewed the key major steps in the current review process (see Display 10):

Display 10: OOSC's Review of the Oversight Framework

OOSC's Review of the Oversight Framework

- June 2023: - CCIR engaged a third party, Optimus SBR, to review the Oversight Framework and assess whether the Framework meets its oversight objective.
  - Optimus SBR reviewed the Framework and did not review GIO and OLHI's operations.
  - The Oversight Framework had not been reviewed since it was created over 15 years ago.
- January 2024: - Optimus SBR presented the summary of their findings and recommendations in the CCIR Winter Meeting.
- February 2024: - Optimus SBR presented the summary of their findings and recommendations to OLHI, GIO, CLHIA, and IBC.
- March 2024: - Optimus SBR concluded the project. The final draft report was shared with GIO and OLHI for comments.
  - The final report will not become public in its current form, but in a summarized CCIR publication.
  - **Optimus SBR found the Oversight Framework needs updating to ensure effectiveness.**
- April 2024: - CCIR accepted the report and approved next steps to address the recommendations from the report in cooperation with OLHI, GIO, CLHIA, and IBC.
- May 2024: - The final report was shared with GIO and OLHI. OLHI and GIO, as well as CLHIA and IBC were invited to participate in a joint CCIR-Industry Task Force and the next steps to update the Oversight Framework.
  - IBC and CLHIA immediately expressed their commitment to participate in the Task Force.

In terms of next steps, CCIR will work with OLHI, GIO, and the insurance companies represented by their industry associations – CLHIA and IBC – to update the Framework to:

1. Define Effectiveness Criteria for GIO and OLHI (i.e. effectiveness criteria for the IDR Mechanism);
2. Enhance Accountability for GIO and OLHI (the current guideline on accountability is ineffective and therefore insufficient);
3. Develop a Data Driven Information Protocol: both industry and regulators require enhanced data-driven information to ensure, among others, that the early warning mechanism to potential systemic risks is effective.

May 24, 2024

OmbudService for Life and Health Insurance (OLHI) and Industry Update

Robyn Van Zant, Complaints Officer, RBC Life Insurance Company; Nicole Caputo, Complaints Coordinator and Complaints Officer, Beneva; Laurie LaPalme, Partner, National Lead, Corporate & Regulatory Insurance Practice, Dentons; Stéphanie Robillanrd, Acting CEO & Ombudsman/Senior Deputy Ombudsman, Ombudservice for Life and Health Insurance (OLHI)

The panel discussion included that OLHI have improved their analytics which has led to improved reporting. OLHI also have consumer protection surveys on its website and an Advisor course with a lot of FTC embedded within, which ensures that customers are being treated fairly and that advisors are adequately FTC-trained.

OLHI has improved the quality of decision letters using simple language and providing more information to help enhance customer understanding. OLHI does not look at any complaints that are related to underwriting questions or product design questions.

Provincial Insurance Councils Panel

Stacey Aubrey, Executive Director, Insurance Council of Manitoba; Janet Sinclair, Chief Executive Officer, Insurance Council of British Columbia; April Stadnek, Executive Director, Insurance Councils of Saskatchewan; Zabeda Yaqoob, Director of Legal and Regulatory Affairs, Alberta Insurance Council; Moderator Dylan Friedman, SVP and CCO, Apexa Corporation

The panel covered a wide range of issues relating to licensing. It was observed that only 18% of life and health advisors are still in the business five years later. BC is seeing examples of advisors under supervision who are not able to name their supervisor. Manitoba has a single continuing education credit option on its website. Manitoba is getting closer to a single-life A&S license in the future.

With respect to the intention to introduce a Restricted Insurance Agency (RIA) regime in BC, the Insurance Council of BC is waiting for the regulation to be published so that they can see what products and persons are covered under it. This is unlikely to be published prior to the BC election in the fall of 2024. Consultations will take place with industry.

Ms. Sinclair noted that there has been a 18% increase in inquiries to the Insurance Council of BC in 2022-23 from 2021-22, and a 77% increase from 2020-21. The subject of inquiries can be found in Display 11. Specific issues relating to life insurance are inquiries around rebating, the Life Insurance Replacement Declaration (LIRD), selling travel insurance, E&O insurance, and supervision issues.

Display 11: Inquiries to the Insurance Council of BC, 2022-23