cafii acifa
The Canadian Association of Financial Institutions in Insurance | L'association canadienne des institutions financières en assurance

200-411 Richmond Street E, Toronto, ON M5A 3S5
☎ (416) 494-9224 🖷 (416) 967-6320
info@cafii.com www.cafii.com

CONFIDENTIAL TO CAFII MEMBERS and ASSOCIATES; NOT FOR WIDER DISTRIBUTION

Regulatory Update – CAFII Executive Operations Committee, November 22, 2021
Prepared By Brendan Wycks, CAFII Co-Executive Director

Table of Contents

200-411 Richmond Street E, Toronto, ON M5A 3S5
(416) 494-9224 (416) 967-6320
info@cafii.com www.cafii.com

Federal/National

Financial Consumer Agency of Canada (FCAC)

FCAC Releases Proposed Guideline On Appropriate Products And Services For Consultation
On November 22/21, the FCAC released its proposed Guideline on Appropriate Products and Services for Banks and Authorized Foreign Banks for public consultation. The submission deadline is Thursday, January 6/22.

In a transmittal message accompanying the proposed Guideline, the FCAC said that it was inviting comments on the document in support of the implementation of the new Financial Consumer Protection Framework (FCPF) in the *Bank Act*. The FCPF introduces new or enhanced consumer protection measures that will further empower and protect consumers in their dealings with banks and authorized foreign banks, the FCAC asserts.

The transmittal indicates that the Guideline sets out clear principles and expectations that Banks should use when establishing and implementing their policies and procedures to ensure they offer or sell products and services that are appropriate for their consumers, having regard to their circumstances, including their financial needs.

The FCAC believes that its consultation on the proposed Guideline will give all interested parties an opportunity to express their views and enable FCAC to benefit from a wide range of perspectives. It asserts that this new consultation is the second in a series of consultations on guidelines that FCAC has developed to help Banks comply with their obligations in the *Bank Act* and the new *Financial Consumer Protection Framework Regulations*, which will come into force on June 30, 2022. It notes that a related consultation on a proposed Guideline on Complaint Handling Procedures is in progress until December 11, 2021. And that another consultation on the obligations of Banks to implement a whistleblowing program for their employees is being planned.

Canadian Foundation For The Advancement Of Investor Rights (FAIR Canada)

FAIR Canada Lauds AMF's Draft Regulation Respecting Complaint Processing
In an e-newsletter released on November 22/21, FAIR Canada applauds the AMF's Draft Regulation Respecting Complaint Processing and Dispute Resolution in the Financial Sector.

FAIR Canada says the Regulation is designed to address numerous consumer concerns, such as access barriers, confusion, and timeliness, with respect to how complaints are managed by Quebec's provincially regulated financial institutions.

FAIR Canada asserts that, among other things the new Regulation would require financial institutions operating in Quebec to

- set up a complaint process that is simple to follow and free to use;
- assist customers who wish to file a complaint;

200-411 Richmond Street E, Toronto, ON M5A 3S5
☎ (416) 494-9224 🖷 (416) 967-6320
info@cafii.com www.cafii.com

- deliver a final response within 60 days; and
- stop using misleading terms such as "ombudsman" to refer to staff members who work on complaints

The investor rights advocacy group opines that, if enacted, the Draft Quebec Regulation would be a significant step forward and help investors who have a complaint against a financial institution in Quebec. FAIR Canada will be urging the other provinces and territories to adopt similar regulations.

"All investors in Canada deserve the same level of protections and rights when they have a complaint," the group asserts.

Canadian Life and Health Insurance Association

CLHIA Says Life Insurers Paid Out $100 Billion To Support Canadians Through Pandemic

In a September 14/21 news release, CLHIA says that Canadians received over $97 billion in benefits from life and health insurance products in 2020, a period that included the first nine months of the COVID-19 pandemic economic slowdown. Insurers helped Canadians respond to the disruption and tragedy of the pandemic by:

- paying out over $12 billion in prescription drug claims
- paying out $950 million in travel insurance claims – largely for trip cancellations;
- paying out $420 million in psychology-related claims to support mental health – up nearly a quarter from 2019; and
- paying out $154 million in life insurance claims from deaths related to COVID-19.

Insurance benefits remained remarkably resilient, CLHIA said. Because of actions taken by insurers, employers and other plan sponsors, over 26 million Canadians benefited from access to health benefits at the end of 2020 – the same as before the pandemic.
"Millions of Canadians rely on life and health insurance products during times of crisis; for all of us 2020 was one of those times," Stephen Frank, President and CEO of the Canadian Life Health and Insurance Association said. "Insurers can be proud of the proactive steps they took through premium reductions and deferrals to help employers through the pandemic, and to protect the workplace drug and health benefits their employees count on."

Additionally, insurers provided $46 billion in annuity payments, $37 billion in supplementary health benefits, and $14 billion in life insurance benefits. Life and health insurers also remained well capitalized through the crisis, with regulatory capital levels well above government targets.

"The pandemic has tested and demonstrated the resilience of life and health insurance industry and the importance of our products to the well-being of so many," Frank said.

200-411 Richmond Street E, Toronto, ON M5A 3S5
☎ (416) 494-9224 🖷 (416) 967-6320
info@cafii.com www.cafii.com

Office of the Superintendent of Financial Institutions (OBSI)

Fasken Publishes Analysis Of OSFI Draft Guideline B-13: Technology and Cyber Risk Management

By Koker Christensen, Alex Cameron, and Christopher Ferguson, Fasken, November 22, 2021
https://www.fasken.com/en/knowledge/2021/11/setting-new-standards-for-cyber-resilience

On November 9, 2021, the Office of the Superintendent of Financial Institutions Canada (OSFI) published Draft Guideline B-13: Technology and Cyber Risk Management ("Draft Guideline"), which outlines OSFI's expectations for federally regulated financial institutions (FRFIs) regarding technology and cyber risk management. The Draft Guideline would apply to all FRFIs, including banks and insurance companies, with the stated objective of helping FRFIs develop "greater resilience to technology and cyber risks". Effective November 9, 2021, OSFI is also conducting a three-month public consultation on the Draft Guideline to engage stakeholders in its development and is inviting public comments until February 9, 2022.

Meaning of Technology Risk and Cyber Risk

The Draft Guideline uses materially similar definitions for "technology risks" and "cyber risks":

- A technology risk is the "risk arising from the inadequacy, disruption, failure, loss or malicious use of information technology systems, infrastructure, people or processes that enable and support business needs and can result in financial loss".

- A cyber risk is the "risk of financial loss, operational disruption or reputational damage from the unauthorized access, malicious and non-malicious use, failure, disclosure, disruption, modification or destruction of an institution's information technology systems and/or the data contained therein".

Although these definitions both capture risks to information technology systems and the potential for financial loss, a key distinguishing feature is that cyber risks also include risks to the data hosted in information technology systems as distinct from the technology itself, whereas technology risks also include risks to other infrastructure, people, and processes. Further, cyber risks encompass a broader range of potential harms, including operational disruption and reputational damage.

Summary of OSFI's Expectations for Technology and Cyber Risk Management

The Draft Guideline is organized into five domains: Governance and Risk Management, Technology Operations, Cyber Security, Third-Party Provider Technology and Cyber Risk, and Technology Resilience. Each domain sets out OSFI's expectations, the key components of sound technology and cyber risk management, the desired risk management outcome, and guiding principles, which are summarized in the table below. FRFIs will be evaluated on these expectations commensurate with their size, the nature, scope, complexity of their operations, and their risk profiles:

200-411 Richmond Street E, Toronto, ON M5A 3S5
(416) 494-9224 (416) 967-6320
info@cafii.com www.cafii.com

Domain 1 Governance and Risk Management	***Expectations:*** Sets OSFI's expectations on formal accountability, leadership, organizational structure and framework used to support risk management and oversight of technology and cyber security. ***Desired Outcome:*** Technology and cyber risks are governed through clear accountabilities and structures, and comprehensive strategies and frameworks. ***Principles (1 to 3):*** 1. **Accountability and Organization Structure:** Senior Management should assign responsibility for managing technology and cyber risks to senior officers, and also ensure an appropriate organizational structure and adequate resourcing are in place for managing technology and cyber risks across the FRFI. 2. **Technology and Cyber Strategy:** The FRFI should define, document, approve and implement a strategic technology and cyber plan(s) that aligns to the FRFI's business strategy while setting goals and objectives that are measurable and evolve with changes in the FRFI's technology and cyber environment. 3. **Technology and Cyber Risk Management Framework:** The FRFI should establish a technology and cyber risk management framework (RMF). The framework should set out a risk appetite for technology and cyber risks, and define what processes and requirements the FRFI utilizes to identify, assess, manage, monitor and report on technology and cyber risks.
Domain 2 Technology Operations	***Expectations:*** Sets OSFI's expectations on management and oversight of risks related to the design, implementation and management of technology assets and services. ***Desired Outcome:*** A technology environment that is stable, scalable and resilient. The environment is kept current and supported by robust and sustainable technology operating processes.

200-411 Richmond Street E, Toronto, ON M5A 3S5
☎ (416) 494-9224 🖷 (416) 967-6320
info@cafii.com www.cafii.com

	Principles (4 to 11): 1. **Technology Architecture:** The FRFI should implement a technology architecture framework, with supporting processes to ensure solutions are built in line with business, technology and security requirements. 2. **Technology Asset Management:** The FRFI should maintain an updated inventory of all technology assets supporting business processes or functions. The FRFI's asset management process should address classification of assets to facilitate risk identification and assessment, record configurations to ensure asset integrity, provide for the safe disposal of assets at the end of their life cycle, and monitor and manage technology currency. 3. **Technology Project Management:** Effective processes are in place to govern and manage technology projects, from initiation to closure, to ensure that project outcomes are aligned with business objectives and are achieved within the FRFI's risk appetite. 4. **System Development Life Cycle:** The FRFI should implement a System Development Life Cycle (SDLC) framework for the secure development, acquisition and maintenance of technology systems that perform as expected in support of business objectives. 5. **Change and Release Management:** The FRFI should establish and implement a technology change and release management process and supporting documentation to ensure changes to technology assets are documented, assessed, tested, approved, implemented and verified in a controlled manner that ensures minimal disruption to the production environment. 6. **Patch Management:** The FRFI should implement patch management processes to ensure controlled and timely application of patches across its technology environment to address vulnerabilities and flaws. 7. **Incident and Problem Management:** The FRFI should effectively detect, log, manage, resolve, monitor and report on technology incidents and minimize their impacts. 8. **Technology Service Measurement and Monitoring:** The FRFI should develop service and capacity standards, and processes to monitor operational management of technology, ensuring business needs are met.
Domain 3	***Expectations:*** Sets OSFI's expectations on management and oversight of cyber risk.

200-411 Richmond Street E, Toronto, ON M5A 3S5
☎ (416) 494-9224 🖷 (416) 967-6320
info@cafii.com www.cafii.com

Cyber Security	***Desired Outcome:*** A secure technology posture that maintains the confidentiality, integrity and availability of the FRFI's technology assets. ***Principles (12 to 15):*** 1. **Identify:** The FRFI should maintain a range of practices, capabilities, processes and tools to identify and assess cyber security for weaknesses that could be exploited by external and insider threat actors. 2. **Defend:** The FRFI should design, implement and maintain multi-layer, preventive cyber security controls and measures to safeguard its technology assets. 3. **Detect:** The FRFI designs, implements and maintains continuous security detection capabilities to enable monitoring, alerting, and enable forensic cyber security incident investigations. 4. **Respond, Recover and Learn:** The FRFI should triage, respond to, contain, recover and learn from cyber security incidents impacting its technology assets, including incidents originating at third-party providers.
Domain 4 Third-Party Provider Technology and Cyber Risk	***Expectations:*** Expands on OSFI's existing guidance for outsourcing and third-party risk, and sets expectations for FRFIs that engage with third-party providers to obtain technology and cyber services that give rise to cyber and/or technology risk. ***Desired Outcome:*** Reliable and secure technology and cyber operations from third-party providers. ***Principles (16):*** 1. **General:** The FRFI should ensure that effective controls and processes are implemented to identify, assess, manage, monitor, report and mitigate technology and cyber risks throughout the TPP's life cycle, from due diligence to termination/exit.
Domain 5	***Expectations:*** Sets OSFI's expectations on the capabilities to deliver technology services through operational disruption.

200-411 Richmond Street E, Toronto, ON M5A 3S5
(416) 494-9224 (416) 967-6320
info@cafii.com www.cafii.com

Technology Resilience	***Desired Outcome:*** Technology services are delivered, as expected, through disruption. ***Principles (17):*** 1. Disaster Recovery: The FRFI should establish and maintain an Enterprise Disaster Recovery Framework (EDRF) to support its ability to deliver technology services through disruption and operate within its risk tolerance.

The Draft Guideline acknowledges that technology and cyber security best practices are fluid and dynamic, and encourages FRFIs to also consult other OSFI guidance, tools and supervisory communications, along with other applicable guidance from relevant authorities, particularly the following:

- OSFI Guideline E-21: Operational Risk Management (summarized in our previous bulletin, "OSFI Releases Final Operational Risk Management Guideline");
- OSFI Guideline B-10: Outsourcing (note that OSFI is undertaking a review of Guideline B-10);
- OSFI Cyber Security Self-Assessment Tool (summarized in our previous bulletin, "Updated OSFI Advisory: Technology and Cyber Security Incident Reporting");
- OSFI Technology and Cyber Security Incident Reporting Advisory (summarized in our previous bulletin, "Updated OSFI Advisory: Technology and Cyber Security Incident Reporting");
- Alerts, advisories and other communications issued by the Canadian Centre for Cyber Security; and,
- Recognized frameworks and standards for technology operations and information security.

Public Consultation
OSFI's three-month public consultation is intended to reflect continued stakeholder engagement and transparency on the Draft Guideline, and to assist OSFI in striking a balance between its prudential objectives and facilitating the ability of financial institutions to compete. Public comments are particularly welcomed by OSFI on:

- the clarity of OSFI's expectations as set out in the Draft Guideline;

200-411 Richmond Street E, Toronto, ON M5A 3S5
(416) 494-9224 (416) 967-6320
info@cafii.com www.cafii.com

- the application of these expectations, commensurate with the institution's size, nature, scope, and complexity of operations;
- the balance between principles and prescriptiveness in OSFI's expectations; and
- other suggestions that contribute to OSFI's mandate to protect depositors and policyholders, and maintain public confidence in the Canadian financial system, while also allowing institutions to compete and take reasonable risks.

Comments can be submitted to tech.cyber@osfi-bsif.gc.ca by February 9, 2022. OSFI is also planning an information session for financial institutions within the coming weeks to provide an overview of the Draft Guideline and an opportunity for questions.

Takeaways for FRFIs and Third-Party Providers

The publication of the Draft Guideline is pursuant to OSFI's Near-Term Plan of Prudential Policy published on May 6, 2021 ("Near-Term Plan"), which expressly committed OSFI to developing OSFI's expectations on technology and cyber risk management in Q4 of 2021. As indicated in the Near-Term Plan and Draft Guideline, OSFI's next objective is to update Guideline B-10: Outsourcing of Business Activities, Functions and Processes in Q1 of 2022, and to expand its scope of third-party risk management beyond outsourcing. Accordingly, FRFIs and their third-party providers can expect additional significant regulatory developments and should begin to strategically prepare for the potential impact on their operations.

FRFIs should review their technology and cyber risk management frameworks and third party service agreements to prepare for OSFI's new focus on these issues. Although the Draft Guideline is subject to further development after the public consultation, FRFIs should expect that its key themes will generally be maintained, and that its final expectations will go beyond making additional investments in information technology and security. While these are of course critical to any technology and cyber risk management framework, FRFIs may also need to revisit their practices with respect to governance, risk accountability, asset management, and relationships with third-party providers. For their part, third-party providers that provide information technology and other services to FRFIs may also need to revisit their Canadian financial industry templates and related practices to account for these new regulatory developments.

200-411 Richmond Street E, Toronto, ON M5A 3S5
(416) 494-9224 (416) 967-6320
info@cafii.com www.cafii.com

Manitoba
Insurance Council of Manitoba (ICM)

Barbara Palace Churchill Steps Down As Executive Director Of Insurance Council Of Manitoba
On November 18/21, Barbara Palace Churchill sent CAFII Co-Executive Directors Brendan Wycks and Keith Martin the following message to advise of some personal and ICM news:

I've been reaching out to ICM stakeholders with a bit of news – I will be leaving ICM as of December 31st. I will be relocating to southern Ontario in early January to be closer to my family who live out there and to help with my elderly mom's care. I will be working in Chatham, Ontario as the CEO of the United Way of Chatham-Kent as of January 10th, so I look forward to the new and exciting challenges there. I will miss the important work that ICM does, but I am completely confident in our team's continued strength going forward.

I've enjoyed the open and candid communications we've had over the years I've been at ICM, and I know that ICM will continue to appreciate CAFII's input as an industry stakeholder. Our Council will be announcing the changes shortly, but I wanted to reach out myself to let you know.

The Insurance Council of Manitoba's announcement of Ms. Palace Churchill's departure has been published in the Fall/Winter issue of its Update newsletter, found here: https://www.icm.mb.ca/files/Bulletin/Council%20Reports/ICM_Report_Fall_Winter_2021_for_distribution.pdf

Québec
Autorité des marchés financiers (AMF)
AMF Releases Report On Responsible Use Of Artificial Intelligence In Finance

On November 22/21, the AMF released a report on the responsible use of artificial intelligence in finance. In a news release announcing that report, the AMF states that the digital transformation, which has accelerated since the start of the pandemic, is unfolding in all sectors of our society and our economy. The AMF asserts that the more personalized offers of financial products and services that artificial intelligence systems allow are for the mutual benefit of consumers and financial institutions, but they also generate ethical, legal, and reputational risks for the latter.

The AMF therefore engaged Marc-Antoine Dilhac, associate professor of ethics and political philosophy at the University of Montreal, and central contributor to the work that led to the launch, in 2018, of the *Montreal Declaration for the Responsible Development of AI*.

200-411 Richmond Street E, Toronto, ON M5A 3S5
(416) 494-9224 (416) 967-6320
info@cafii.com www.cafii.com

As part of their preparation of the AMF's report titled "Artificial intelligence in finance: recommendations for responsible use," Professor Dilhac and his team of researchers considered not only the conclusions of work by experts in the field, but also the concerns expressed by consumers of financial products and services at workshops held earlier this year. The participation of citizens in this project adds to the depth of reflection, and clearly distinguishes this approach from other work carried out to date on the responsible use of artificial intelligence in finance.

The report contains 10 recommendations to promote the development and deployment of artificial intelligence in finance in a responsible manner: three of them are formulated for the attention of the AMF, while the other seven are directed at industry. The 10 recommendations are supported by an inventory of use cases and a detailed discussion of the risks and challenges of responsible deployment of AI in finance. The recommendations are also based on an interpretation of the principles of the *Montreal Declaration for the Responsible Development of AI* in the specific context of financial sector activities.

"I encourage participants in the financial industry to immediately consider the recommendations presented in this report in the context of the development of their artificial intelligence systems," said Louis Morisset, the AMF's Chairman and CEO. "We are committed to doing the same with regard to the recommendations made therein and with regard to the digital transformation that is also taking place within the Authority. Let us make sure we develop artificial intelligence responsibly, so that everyone can benefit from it."

The AMF's Report on the Responsible Use of Artificial Intelligence in Finance, available only in French, can be found here:
https://lautorite.qc.ca/fileadmin/lautorite/grand_public/publications/professionnels/rapport-intelligence-artificielle-finance-fr.pdf.

International

Basel Committee on Banking Supervision

Basel Committee Proposes Guidance On Climate Risks

On November 17/21, Investment Executive reported that global banking regulators are proposing new guidance for supervising climate-related risks.

The Basel Committee on Banking Supervision launched a consultation that proposed a set of principles for applying the existing global rules to risks that arise due to the effects of global warming.

"Climate change may result in physical and transition risks that could affect the safety and soundness of individual banking institutions and have broader financial stability implications for the banking system," the group said in its consultation paper.

200-411 Richmond Street E, Toronto, ON M5A 3S5
☎ (416) 494-9224 🖷 (416) 967-6320
info@cafii.com www.cafii.com

The Basel Committee's work to date has concluded that, while the existing supervisory principles are broad enough and flexible enough to allow regulators to address climate-related risks, both supervisors and banks could use additional guidance on supervisory expectations for dealing with these risks.

The proposed guidance aims to "promote a principles-based approach to improving risk management and supervisory practices related to climate-related financial risks."

It also seeks to establish a common set of expectations for larger global banks.

"Specifically, with regard to scenario analysis, including stress testing, the principles are formulated with a view towards application to large, internationally active banks," it said.

According to the paper, all banks are potentially exposed to climate-related risks, which could have wide-ranging impacts on a variety of sectors and countries.

"Banks should take into account the unique characteristics of such risks, including but not limited to potential transmission channels, the complexity of the impact on the economy and financial sector, uncertainty related to climate change and potential interactions between physical and transition risks," it said.

Additionally, while some of the risks stemming from climate change are already evident, others may emerge over time and are likely to worsen.

"The high degree of uncertainty around the timing of these risks suggests that banks should take a prudent and dynamic approach to developing their risk management capacities. Different time horizons should be considered in the process of risk identification and assessment as well as in scenario analysis," it said.

It suggested that banks should continually develop their expertise on climate-related financial risks.

The deadline for providing feedback on the proposed guidance is Feb. 16, 2022.

UK Financial Conduct Authority (FCA) and Prudential Regulatory Authority (PRA)

UK Regulators Step Up Climate Fight

On October 28/21, Investment Executive reported that alongside the UK's other major financial sector regulators, the Financial Conduct Authority (FCA) published a report that sets out its efforts to address the risks posed by climate change.

Among a range of other actions, the FCA plans in December to publish final rules setting disclosure requirements for issuers, asset managers, insurers and pension managers that follow the recommendations of the Task Force on Climate-Related Financial Disclosures (TCFD).

In addition to its forthcoming disclosure rules, the FCA said that it also plans to consult on product labeling, firms' plans for a transition to "net zero", and to issue its own TCFD-compliant report in 2022.

200-411 Richmond Street E, Toronto, ON M5A 3S5
☎ (416) 494-9224 🖷 (416) 967-6320
info@cafii.com www.cafii.com

"To successfully transition to a net-zero economy requires not only that firms adapt and innovate, but that we regulators do too. That is why we are leading the effort to ensure there are consistent, trusted standards for disclosure investors can rely on," said Nikhil Rathi, CEO of the FCA, in a release.

At the same time, a report from the U.K.'s Prudential Regulation Authority (PRA) finds that firms have made "tangible progress" at adopting climate-related risk management practices (which were mandated in July 2020), but that "there is still much further to go."

"As we move into 2022, the PRA will actively supervise to ensure firms meet expectations, with firms needing to demonstrate a good understanding and management of climate-related financial risks on an ongoing basis," the PRA said.

The prudential regulator will also be considering whether to revise banks' capital requirements to ensure that they are adequately reserved against material climate-related financial risks. "We will provide an update on our approach in 2022 following a call for further research and a conference on climate change and capital requirements," the PRA said.

Earlier this month, the Canadian Securities Administrators (CSA) published its own proposals for mandating TCFD disclosures by issuers. Those proposals are out for public comment.