

Welcome

Registrant Outreach 2026



Agenda – Edmonton June 16, 2026

12:30 – 12:40	Opening Remarks Adam Hillier, Team Lead, Registrant Oversight
12:40 – 1:10	2026 Cybersecurity Sweep Reviews: Key Findings from Registered Firms in Alberta - Aneri Mehta, Regulatory Analyst, Registrant Oversight - Zulqer Khan, Lead, Market Regulation IT Projects
1:10 – 1:20	Break
1:20 – 2:05	FAQ Roundtable - Client Focused Reforms - Mat Pendola, Manager, Registrant Regulation - Julio Arboleda Ramirez, Senior Legal Counsel, Market Regulation
2:05 – 2:25	Break
2:25 – 3:55	FINTRAC – Spotlight on Supervision - Mark Sokolnicki – Senior Manager, Supervision – Financial Entities - Emma Rankin – Manager, Supervision – Financial Entities

Agenda – Calgary June 18, 2026

09:00 – 09:10	Opening Remarks • Adam Hillier, Team Lead, Registrant Oversight
09:10 – 10:40	FINTRAC – Spotlight on Supervision • Mark Sokolnicki – Senior Manager, Supervision – Financial Entities • Emma Rankin – Manager, Supervision – Financial Entities
10:40 – 11:00	Break
11:00 – 11:30	2026 Cybersecurity Sweep Reviews: Key Findings from Registered Firms in Alberta • Aneri Mehta, Regulatory Analyst, Registrant Oversight • Zulqer Khan, Lead, Market Regulation IT Projects
11:30 – 11:40	Break
11:40 – 12:25	FAQ Roundtable - Client Focused Reforms • Mat Pendola, Manager, Registrant Regulation • Julio Arboleda Ramirez, Senior Legal Counsel, Market Regulation

2026 Cybersecurity Sweep Reviews: Key Findings from Registered Firms in Alberta

Aneri Mehta, Regulatory Analyst

Zulqer Khan, Lead, Market Regulation IT Projects



Topics

1	Cybersecurity reviews conducted
2	Summary of observations
3	Cybersecurity policies and procedures
4	Cybersecurity training
5	Cybersecurity risk assessments and controls
6	Third-party service providers
7	Cybersecurity incident response plan
8	Questions

Cybersecurity - Evolution

- Rapid and significant change in technology usage:
 - remote work,
 - mix of devices – personal and corporate,
 - cloud-based storage, and
 - increased handling of sensitive information online.
- Resulted in focused compliance reviews regarding cybersecurity controls.
- CSA Staff Notice expected to be published this summer.

Cybersecurity reviews conducted

- Compliance system requirements in section 11.1 of NI 31-103 and the Companion Policy.
- Based on firm's business model and use of technology, firms are expected to have adequate:
 - cybersecurity policies and procedures,
 - cybersecurity training,
 - cybersecurity risk identification, assessment, and control processes,
 - due diligence of third-party service providers, and
 - cybersecurity incident response plans.

Summary of observations

- Some firms had effective cybersecurity practices but did not adequately formalize or document them.
- Some firms had adequate cybersecurity controls formalized in their policies but had not implemented them in practice.
- Some firms had both inadequate cybersecurity controls and insufficient policies and procedures.

Cybersecurity policies and procedures

- A few of the firms did not have any written cybersecurity policies and procedures.
- Many firms had written policies and procedures that could be further enhanced.
- Policies and procedures were not reviewed and updated with sufficient frequency.

Effective cybersecurity practices

- | | |
|--|---|
| <ul style="list-style-type: none"> • Cybersecurity risk assessment processes • Website and application usage • Use of privately owned electronic devices by employees | <ul style="list-style-type: none"> • Data security and encryption • Employee cybersecurity training and awareness • Ownership of cybersecurity processes |
|--|---|

Cybersecurity training

- A few of the firms did not provide any cybersecurity training to their employees.
- A few of the firms could have provided more comprehensive training.
- A few of the firms had no or limited documentation to support the training that had been provided to their employees.

Effective cybersecurity practices

- Oversight and delivery of training
- Frequency and timing of training

- Social engineering and phishing simulation tests
- Documentation of training and tests conducted

Cybersecurity risk assessments and controls

- Some firms conducted cybersecurity risk assessments that could have been more robust.
- A few of the firms had not documented any risk assessments.
- Many firms could improve their risk assessment documentation.

Effective cybersecurity practices

- Assess employee access rights and related controls
- Reliance on third-party service providers and associated risks
- Include controls that are tailored to risk areas identified by the assessment

Third-party service providers

- Some firms could strengthen their cybersecurity oversight of third-party service providers.
- Many firms had no or limited documentation to support their oversight of third-party service providers.

Effective cybersecurity practices

- Conduct meaningful due diligence on third-party service providers
- Gather information on the service provider's data storage policies, controls, and incident handling
- Assess and monitor risks from third-party access to client and firm data and systems

Cybersecurity incident response plan

- A few of the firms did not have a written cybersecurity incident response plan at all.
- Some firms could strengthen how their plan is operationalized.
- Some firms should have tested their plan more regularly.

Effective cybersecurity practices

- | | |
|---|--|
| <ul style="list-style-type: none"> • Define roles and responsibilities for the plan • Conduct regular testing | <ul style="list-style-type: none"> • Implement data backup and recovery processes • Consider cybersecurity insurance |
|---|--|

Questions?

Thank you

Contact us



Aneri Mehta
Zulqer Khan



aneri.mehta@asc.ca
zulqer.khan@asc.ca



403-355-2269
403-297-6165

Q&A Roundtable Client Focused Reforms

Julio Arboleda Ramirez – Senior Legal Counsel

Matias Pendola – Manager, Registrant Regulation



Background

- The Client Focused Reforms (**CFRs**) to National Instrument 31-103 fully came into effect on December 31, 2021.
- New or expanded requirements applicable to conflicts of interest, client disclosure, know-your client (**KYC**), know-your-product (**KYP**), and suitability.
- Guidance published by the Canadian Securities Administrators (**CSA**) and the Canadian Investment Regulatory Organization (**CIRO**):
 - CFR FAQs – last updated on December 6, 2023
 - Joint CSA/CIRO Staff Notice 31-363 – Conflicts of interest – published on August 3, 2023
 - Joint CSA/CIRO Staff Notice 31-368 – KYC, KYP, and suitability – published on December 10, 2025

Purpose of Q&A Roundtable

- Assist firms in operationalizing principles-based CFRs regulations.
- Discuss efficient approaches and best practices for meeting the CFR requirements.
- Provide additional information on friction points or unclear areas of the CFRs.
- How artificial intelligence fits into this.



Common Themes of Questions Received

Conflicts of interest	KYC	KYP	Suitability
• How to determine something is a conflict of interest • Use of a conflict-of-interest matrix • Examples of conflicts of interest • Use of artificial intelligence	• Client confirmation • Determining risk capacity • Client reluctance to provide information • Use of artificial intelligence	• Documenting analysis of third-party KYP materials • KYP for model portfolios • Documenting ongoing KYP monitoring • Use of professional judgement in assessing relevant aspects of securities • Use of artificial intelligence	• Impact of costs on expected performance • Different classes of the same security • Range of alternatives for proprietary model portfolios • Centralized documentation for trades • Client concentration in exempt market securities • Use of artificial intelligence

Q&A Roundtable Client Focused Reforms

Julio Arboleda Ramirez – Senior Legal Counsel

Matias Pendola – Manager, Registrant Regulation



Contact us



Matias Pendola

Julio Arboleda Ramirez



Matias.Pendola@asc.ca

Julio.ArboledaRamirez@asc.ca