

Oversight Review Report of the Canadian Investment Regulatory Organization

Issued: July 23, 2025

Table of Contents

I.	Executive Summary	1
II.	Introduction.....	2
A.	Background.....	2
B.	Objectives	2
III.	Risk Assessment and Oversight Review.....	3
A.	Information Technology (IT)	3
B.	Membership Intake (MI).....	4
C.	Trading Conduct Compliance (TCC).....	5
IV.	Findings.....	7
A.	Inadequate Independent Assessment of Internal Controls for the Continuing Education Reporting and Tracking System (CERTS)	7
B.	Continued Use of a Cloud Service Outside of Canada	8
C.	Partial Compliance with Term & Condition 21 (T&C 21) of AMF’s CIRO Recognition Order (RO)	9
	APPENDIX A.....	11
1.	Methodology	11
2.	Report Format	11
3.	Scope.....	11
4.	Priority of Findings	12
	APPENDIX B	14
	Applicable Regulatory Requirements and Functions	14

I. Executive Summary

In accordance with their mandates under the securities legislation of their respective jurisdictions, the Recognizing Regulators¹ of the Canadian Investment Regulatory Organization (CIRO) have jointly completed an annual risk-based oversight review (the **Review**) that targeted specific processes within the following functional areas²:

- Information Technology,
- Membership Intake, and
- Trading Conduct Compliance.

Other than the findings noted below, staff of the Recognizing Regulators (**Staff**) did not identify concerns with CIRO meeting the relevant terms and conditions of the Recognizing Regulators' recognition orders (the **Recognition Orders**) in the functional areas reviewed. Staff make no other comments or conclusions on CIRO's operations or activities that are outside the scope of the Review.³

As a result of the Review, Staff have identified three medium priority findings.⁴

The first finding is the inadequate independent assessment of internal controls for the Continuing Education Reporting and Tracking System (**CERTS**). The second finding relates to the continued use of a cloud service outside of Canada. The third finding is Québec specific and relates to CIRO's Québec Regional Office not having clearly defined responsibilities and dedicated staff for analyzing, reviewing and formulating recommendations for membership applications submitted by firms and/or members with a head office located in Québec.

Staff require CIRO to resolve the findings by taking specific and timely corrective action in accordance with the priority assigned to them. The findings are set out in [part IV Findings](#) of the report.

Staff have also identified other expectations regarding practices and procedures carried out by CIRO across the functional areas reviewed. These expectations are identified for CIRO to take note of and use as a basis for seeking improvements going forward. The expectations are set out in [part III Risk Assessment and Oversight Review](#) of the report.

Lastly, Staff acknowledge that CIRO has resolved the findings which were cited in the previous Oversight Report, which Staff followed up on prior to the Review.

¹ See [part II Introduction, section A, Background](#) of the report for the regulators that recognize CIRO.

² See [Appendix A, section 3](#) for a detailed description of the scope of the Review.

³ See CSA Staff's [2024 Annual Activities Report on the Oversight of Canadian Investment Regulatory Organization and Canadian Investor Protection Fund](#) for more details on CSA staff's oversight activities.

⁴ See [Appendix A, section 4](#) for the criteria used to prioritize findings.

II. Introduction

A. Background

CIRO is the national self-regulatory organization (**SRO**) that oversees all mutual fund dealers (**MFD**), investment dealers and trading activity on equity and debt marketplaces in Canada.

CIRO is recognized as an SRO by the Alberta Securities Commission; the Autorité des marchés financiers (AMF); the British Columbia Securities Commission; the Manitoba Securities Commission; the Financial and Consumer Services Commission of New Brunswick; the Office of the Superintendent of Securities, Digital Government and Service Newfoundland and Labrador; the Office of the Superintendent of Securities, Northwest Territories; the Nova Scotia Securities Commission; the Office of the Superintendent of Securities, Nunavut; the Ontario Securities Commission; the Prince Edward Island Office of the Superintendent of Securities; the Financial and Consumer Affairs Authority of Saskatchewan; and the Office of the Yukon Superintendent of Securities (collectively, the **Recognizing Regulators**).⁵ CIRO's head office is in Toronto with regional offices in Calgary, Montréal, and Vancouver.

This report details the objectives and the key areas that formed the basis of the Review conducted by Staff. The period covered by the Review (the **Review Period**), methodology used, report format, and scope are set out in [Appendix A](#). A description of the applicable regulatory requirements and functional areas are set out in [Appendix B](#).

B. Objectives

The objectives of the Review were to evaluate whether selected regulatory processes were effective, efficient, applied consistently and fairly, and whether CIRO complied with the terms and conditions of the Recognition Orders.

⁵ The Recognizing Regulators recognized CIRO (formerly the New Self-Regulatory Organization of Canada) effective January 1, 2023. CIRO consolidates the functions previously performed by the Investment Industry Regulatory Organization of Canada (**IIROC**) and the Mutual Fund Dealers Association of Canada (**MFDA**).

III. Risk Assessment and Oversight Review

A. Information Technology (IT)

As part of the annual risk assessment process, IT was determined to be an area with an above average adjusted risk score. IT was included in the Review due to the above-average adjusted risk score and the existence of other factors such as IT's major impact on CIRO, and the probability that an identified risk could be realized for the period under review. In so determining, Staff identified the following areas that became the focus of the Review:

- CIRO's compliance with the Recognition Orders in relation to CERTs and other critical technology systems,
- CIRO's service agreements with critical IT third-party service providers, and
- CIRO's receipt and analysis of independent system reports (**ISRs**).

CERTS is CIRO's online system MFD firms and approved persons use to comply with reporting obligations under the MFD Continuing Education (**MFD CE**) requirement.

To ensure that CIRO has the applicable controls in place, Staff reviewed:

CERTs

- CIRO's policies and procedures to comply with term and condition 19 of Appendix A of the Recognition Orders (the **T&C 19 Requirements**⁶), and
- the most recent reports by a qualified party on the review of the internal controls of CERTs.

CIRO's critical technology systems

- CIRO's policies and procedures to comply with subsection 1(2) of Schedule 2 of the Recognition Orders (the **Schedule 2 Requirements**), and
- Material changes to agreements with information technology service providers regarding critical technology systems to assess whether CIRO complied with the Schedule 2 Requirements.

CIRO's agreements with critical third-party service providers

- CIRO's policies and procedures for entering into agreements with critical third-party service providers, and
- A sample of agreements with critical third-party service providers.

ISRs

- CIRO's policies and procedures to review and assess the ISRs obtained from critical third-party systems providers, and
- CIRO's analysis of a sample of ISRs obtained from critical third-party systems providers.

⁶ See the Information Technology section of [Appendix B](#) for a description of the T&C 19 Requirements.

Based on the work performed, Staff are satisfied that CIRO has adequate processes and procedures in place in the identified areas, with the exception of two medium priority findings detailed in [*part IV Findings*](#) of the report.

In addition, while CIRO has a quarterly process in place designed to ensure that the requirements of the Recognition Orders are met (**Quarterly RO Process**), the written Quarterly RO Process does not specifically address the T&C 19 Requirements. Staff expect CIRO to enhance the Quarterly RO Process to ensure the T&C 19 Requirements are met.

Further, Staff are satisfied that CIRO staff have appropriately reviewed the ISRs provided by vendors that are critical to CIRO's operations or retain CIRO's confidential information. Staff expect CIRO to update its written policies and procedures to reflect the ISR review procedures performed, which includes updating the standard form used to document the ISR reviews to ensure the scope of an ISR pertains to the service CIRO obtains from the vendor. Staff also expect CIRO staff to adequately document the resolution of any control issues identified in the ISRs, including an assessment of the impact to CIRO and actions CIRO should take to mitigate the issues.

Staff acknowledge that after the Review, CIRO staff are updating CIRO's Quarterly RO Process to comply with the T&C 19 Requirements, and CIRO's written policies and procedures to reflect the ISR review procedures performed. Further, CIRO has developed more comprehensive documentation of the resolution of any control issues identified in the ISRs.

B. Membership Intake (MI)

As part of the annual risk assessment process, MI was determined to be an area with a moderate adjusted risk score. MI was included in the Review due to the length of time since the last Oversight Review and MI's role in reviewing membership applications, including crypto trading platform intake. In so determining, Staff identified the following areas that became the focus of the Review:

- CIRO's policies and procedures for reviewing and processing in-scope member transactions (e.g., new Dealer Member applications, dual-registration applications, crypto business changes, or other material business changes), and
- CIRO's training and onboarding program for new MI staff and assess whether MI has sufficient resources.

To ensure that CIRO has the applicable controls in place, Staff reviewed:

- A sample of in-scope member transactions, including any applicable policies and procedures, templates, and documentation of work performed, and assessed whether these processes were consistent with the applicable MI policies and procedures, and
- The roles and responsibilities of various positions within MI, including training and onboarding process, and considered whether MI has sufficient resources to handle the volume of applications.

Based on the work performed, other than the Québec only medium priority finding as set out in [part IV Findings](#) of the report, Staff identified opportunities to enhance the MI policies and procedures to accurately reflect current practices. Staff expect CIRO's MI policies and procedures to:

- i) incorporate all review programs and templates used by the department; and
- ii) provide guidance for the use of staff's discretion in determining when certain templates or standard procedures are not used during the review of in-scope member transactions, including ensuring that staff maintain the appropriate documentation for their determination on file.

Staff acknowledge that after the Review, CIRO staff have carried out the work necessary to enhance the relevant MI written policies and procedures.

C. Trading Conduct Compliance (TCC)

As part of the annual risk assessment process, TCC was determined to be an area with a moderate adjusted risk score. TCC was included in the Review in part due to the length of time since the last Oversight Review. In so determining, Staff identified the following areas that became the focus of the Review:

- TCC policies and procedures for conducting TCC examinations and the quality assurance program of TCC conducted by the Compliance Modernization Group department,
- TCC exam modules (**TCC Program**) and how they are kept up to date to incorporate new rules, changes to securities legislation, and new business models, and
- CIRO's training program for new TCC staff.

To ensure that CIRO has the applicable controls in place, Staff reviewed:

- A sample of TCC examinations and all relating documentation with a focus on higher risk areas, and assessed whether the examination processes were consistent with applicable TCC policies and procedures,
- TCC's process for making changes to the exam modules to incorporate additions or changes to rules or securities legislation, and
- TCC training materials for new staff.

Based on the work performed, Staff identified an opportunity to further enhance the existing TCC processes for monitoring changes in securities legislation and, as appropriate, communicating with the CSA jurisdictions to ensure that the TCC Program is up to date. The objective of the TCC Program is to examine Dealer Members' trading policies, procedures and supervision for compliance with applicable trading-related rules administered by CIRO (such as the Universal Market Integrity Rules and applicable CIRO dealer rules) and securities legislation. Staff expect TCC to work with the CSA to assist CIRO in determining the most appropriate processes to monitor and assess changes in applicable securities legislation to ensure that the TCC Program is up to date for monitoring Dealer Members' compliance with securities legislation.

Staff acknowledge that after the Review, CIRO and CSA staff have discussed possible approaches to monitor and assess changes in applicable securities legislations.

IV. Findings

A. Inadequate independent assessment of internal controls for CERTS

CERTS is CIRO's online system for MFD firms and approved persons to comply with reporting obligations under the MFD CE requirement. The first MFD CE cycle was from December 1, 2021 to November 30, 2023.

T&C 19(2) of Appendix A of CIRO's Recognition Orders requires a biennial report, prepared in accordance with established audit standards by a qualified party, to be provided to the Recognizing Regulators with details of a review designed to ensure that CERTS has an adequate system of internal controls, including, but not limited to, integration into CIRO's business continuity and disaster recovery plans (the **Biennial Report**).

CIRO submitted to CSA staff two penetration test reports on CERTS that detailed reviews conducted by an independent party within the first biennial MFD CE cycle. However, the reviews conducted did not fully assess the adequacy of CERTS' internal controls as required by the Recognition Orders.

Staff acknowledge that at the time the first Biennial Report was required, CIRO was undertaking a significant amount of work on integrating the information technology infrastructure and legacy back-office systems of the predecessor organizations, the MFDA and IIROC.

Further, Staff acknowledge that CERTS was upgraded in November 2023 and the CERTS platform was migrated to a unified data centre in April 2024. Conducting a comprehensive review of all required internal controls after the upgrade to the CERTS system and the migration to the unified data centre was a business determination that resulted after considering multiple factors such as resource allocation and competing priorities.

Lastly, Staff have confirmed that CIRO plans to obtain an independent review of CERTS internal controls in accordance with the requirements of the Recognition Orders in 2025.

Why this is Important

The Recognition Orders require CIRO to provide the Recognizing Regulators with a Biennial Report, prepared in accordance with established audit standards by a qualified party, with details of a review designed to ensure that CERTS has an adequate system of internal controls, including, but not limited to, integration into CIRO's business continuity and disaster recovery plans. Failure to adequately conduct an independent review may lead to internal control issues for a system identified by the CSA as critical to CIRO.

Priority

Medium

Requirement

Please describe how CIRO will resolve the finding.

CIRO's Response	We acknowledge the finding. The migration of the CERTS application, servers, storage, databases and management processes was performed as part of a larger data centre consolidation project and completed in April 2024.
	As such, the CERTS system is now subject to all the IT service management and Information Security processes and controls associated with this new environment. A successful full CERTS disaster recovery test was also performed in November 2024.
	CIRO will draft a plan for a review of these controls and, subject to the required prior discussions with the CSA regarding the plan and the third-party chosen to perform the audit, will obtain an independent review of CERTS internal controls in accordance with the requirements of the Recognition Orders in CIRO's FY26.
Staff Comments and Follow-up	Staff acknowledge CIRO's response and have no further comments.

B. Continued use of a cloud service outside of Canada

CIRO's Procurement Policy stipulates that CIRO's data hosted in the cloud must reside in Canada.

In 2021, IIROC, a predecessor organization of CIRO, engaged a service provider that hosted some of its data in the United States. At the time, IIROC's Information Security Committee approved the relationship with the service provider based on the implementation of compensating controls and that data should be moved to servers located in Canada as soon as possible.

However, while no data is currently hosted on the service provider's servers, CIRO informed Staff that approximately 15% of the subject data is still transiting on the service provider's servers located in the United States.

Staff acknowledge that CIRO confirmed that data transiting outside of Canada is non-sensitive key performance indicator related data that is not confidential in nature, is not personal information, is not saved in temporary memory within the service provider's server and that all data in transit is fully encrypted.

CIRO informed staff that it intends to develop a plan to address this issue.

Why this is Important	Data residing outside of Canada may be is subject to different data protection regimes than the ones existing in Canada.
Priority	Medium
Requirement	Please describe how CIRO will resolve the finding.
CIRO's Response	We acknowledge the finding. The service region for the relevant service provider will be switched from the United States to Canada by July 2025. Once switched, the remaining 15% of the subject data that was transiting to the service provider in the United States will transit to Canada. All associated meta-data and data for any future developed services from the relevant service provider will also reside in Canada.
Staff Comments and Follow-up	Staff acknowledge CIRO's response and have no further comments.

C. Partial compliance with T&C 21 of AMF's CIRO RO

T&C 21(1) of Appendix A of AMF's CIRO RO stipulates that CIRO maintains a regional office in Québec (the "Québec Regional Office") with clearly defined responsibilities concerning regulation, membership, sales compliance, financial compliance, market surveillance, trading desks compliance and enforcement of the Rules with respect to its Dealer Members, Marketplaces Members and Approved Persons.

During its review of the MI function, AMF staff noted that throughout the Membership Intake review process, CIRO's management from the Québec Regional Office is informed and provides its opinion when solicited by staff from the cross-organizational Membership Intake team. The final decisions regarding firms and/or existing members with their head offices in Québec are made by the Senior Vice-President, Québec and Atlantique Canada.

However, AMF staff noted that the Québec Regional Office does not have clearly defined responsibilities and dedicated staff for analyzing, reviewing and formulating recommendations regarding membership applications submitted by firms and/or members with a head office located in Québec. The applications are reviewed, and internal processes are followed by the CIRO's cross-organizational Membership Intake team which does not include any CIRO staff from the Québec Regional Office.

This issue is raised only in regards of the membership function and not towards any other functions and responsibilities that are exercised by the Québec Regional Office.

Why this is Important	Not having clearly defined responsibilities regarding membership in the Québec Regional Office, if unresolved, could result in an inconsistency with the requirements of T&C 21(1) of AMF's CIRO RO.
Priority	Medium
Requirement	Please describe how CIRO will resolve the finding.
CIRO's Response	We acknowledge the finding. We will work toward more clearly defining responsibilities for Québec as it relates to Québec-based membership applications. In the interim, we propose to update MI's procedures to specify that the impacted Québec Relationship Manager (or their Director) is responsible for reviewing the assessment and recommendation for their compliance area and will be kept informed of the various stages throughout the analysis. For better clarity, while MI staff are responsible for preparing the written assessment and recommendation, that assessment and recommendation are not considered to be complete until each impacted Relationship Manager (or their Director) from the Québec Regional Office has confirmed their acceptance of it. MI staff will retain evidence of this confirmation in the file records for the member transaction. If an impacted Relationship Manager (or their Director) does not accept the assessment and recommendation prepared by the MI Manager or Examiner, the Relationship Manager (or Director) must provide instruction to MI staff on how to resolve the matter. Once the Québec Regional Office has confirmed acceptance of the assessment and recommendation, the proposed membership transaction can proceed to decision-maker review.
Staff Comments and Follow-up	AMF staff acknowledge CIRO's response and will closely monitor the implementation of the action plan to ensure effective remediation of the finding.

APPENDIX A

1. Methodology

The Recognizing Regulators have adopted a risk-based methodology to determine the scope of the Review. On an annual basis, the Recognizing Regulators:

- Identify the key inherent risks⁷ of each functional area or key process based on:
 - reviews of internal CIRO documentation (including management self-assessments and risk assessments),
 - information received from CIRO in the ordinary course of oversight activities (e.g., periodic filings and discussions with Staff),
 - the extent and prioritization of findings from the prior oversight review, and
 - the impact of significant events in or changes to markets and participants to a particular area.
- Evaluate known controls for each functional area,
- Consider relevant situational/external factors and the impact of enterprise-wide risks on CIRO as a whole or on multiple departments,
- Assign an initial overall risk score for each functional area,
- Identify and assess the effectiveness of other mitigating controls that may be in place in specific functional areas,
- Assign an adjusted overall risk score for each area, and
- Use the adjusted risk scores to determine the scope of the Review.

Once the scope of the Review is determined, Staff conduct the Review which involves reviewing specific documents pertaining to the Review Period and interviewing appropriate CIRO staff in order to:

- Confirm that mitigating controls were in place for the key inherent risks identified, and
- Assess the adequacy and efficacy of those mitigating controls.

2. Report Format

In keeping with a risk-based approach, this report focuses on three functional areas and key processes that were deemed warranted to be part of the Review.

3. Scope

Policy and IT were functional areas identified as above average risk but considering CIRO's ongoing policy work related to the recent amalgamation of IIROC and the MFDA, staff have decided to only include IT for this Review. Staff also utilized the risk assessment process to identify MI and TCC as the other moderate risk areas of focus for the Review.

⁷ Inherent risk is the assessed level of the unrealized potential risk, taking into account the likelihood of and impact if the risk was realized prior to the application of any mitigating controls.

The Review Period for the three functional areas selected was January 1, 2023 to August 31, 2024.

Also, through the risk assessment process, Staff determined that the following moderate and low risk areas would not be examined during the Review:⁸

Moderate

- Business Conduct Compliance (BCC)⁹
- Corporate Governance
- Debt Market Surveillance
- Equity Market Surveillance
- Enforcement
- Financial and Operations Compliance (FinOps)
- Member Services & Innovation
- Office of the Investor
- Policy
- Registration

Low

- Data Analytics
- Financial & Project Management
- Risk Management
- Trading Review & Analysis

4. Priority of Findings

Staff prioritize findings into High, Medium and Low, based on the following criteria:

High	Staff identify an issue that, if unresolved, will result in CIRO not meeting its mandate, or one or more of the terms and conditions of the Recognition Orders, or other applicable regulatory requirements. CIRO must immediately put in place an action plan (with any supporting documentation) and timelines for addressing the findings that are acceptable to Staff. If necessary, compensating controls should be implemented before the finding is resolved. CIRO must report regularly to Staff on its progress.
Medium	Staff identify an issue that, if unresolved, has the potential to result in an inconsistency with CIRO's mandate, or with one or more of the terms

⁸ These areas continue to be subject to oversight by the Recognizing Regulators through ongoing mandatory reporting by CIRO as required by the Recognition Orders, as well as regularly scheduled and ad hoc meetings between the Recognizing Regulators and CIRO staff.

⁹ CIRO's BCC department monitors business conduct related activities of investment dealers and mutual fund dealers and their registered individuals.

and conditions of the Recognition Orders, or with other applicable regulatory requirements. CIRO must put in place an action plan (with any supporting documentation) and timelines for addressing the findings that are acceptable to Staff. If necessary, compensating controls should be implemented before the finding is resolved. CIRO must report regularly to Staff on its progress.

Low Staff identify an issue requiring improvement in CIRO's processes or controls and raise the issue for resolution by CIRO's management.

Repeat Finding A finding that was previously identified by Staff and not resolved by CIRO is categorized as a repeat finding in the report and may require that the level of priority be raised from the initial level noted in the previous report.

Expectation/
Observations Minor deviations, inconsistencies, or non-conformities, from CSA expectations or industry best practices, relating to the application of a process that is otherwise well-implemented. Expectations/Observations do not significantly impact the overall quality of the entity's risk management process. CSA staff will communicate their expectations/observations to the entity.

APPENDIX B

Applicable Regulatory Requirements and Functions

Information Technology

T&C 19(2) of the Recognition Orders states that CIRO must on a reasonably frequent basis, and at least biennially, cause a report to be prepared in accordance with established audit standards by a qualified party which provides details of a review designed to ensure that the CERTs has an appropriate system of internal controls, including, but not limited to, integration into CIRO's business continuity and disaster recovery plans.

T&C 19(3) of the Recognition Orders requires that before finalizing any engagement to prepare the report described in T&C 19(2), CIRO must discuss the choice of qualified party and scope of the review with the Commission.

T&C 20(2) of the Recognition Orders states CIRO must provide the Commission with other reports, documents and information and data in a format and manner acceptable to the Commission as the Commission or its staff may request.

Section 1(2)(b) of Schedule 2 of the Recognition Orders requires CIRO to provide the Commission with at least three months' written notice prior to any intended material change to its agreement with an information technology service provider regarding its critical technology systems

The main elements of IT department's work are to manage the organization's technological ecosystem including process improvement, data management, communications, and cybersecurity.

Membership Intake

T&C 14(1) of the Recognition Orders requires that CIRO must keep records of all matters subject to regulatory approvals by CIRO under the Rules and CIRO by-laws for an appropriate time period in accordance with legal and industry standards for record retention, including but not limited to:

- a) All granted membership requests, specifying the persons to whom membership was granted and the basis for its decision; and
- b) All denied membership requests or terms and conditions imposed on membership, specifying the basis for its decision.

T&C 15(4) of the Recognition Orders, states that CIRO, through its Directors, officers and employees, must be responsible for all membership matters while giving consideration to any regional issues raised by the Regional Councils on an advisory basis.

T&C 21(1) of AMF CIRO's RO requires that CIRO maintains a regional office in Québec (the "Québec Regional Office") with clearly defined responsibilities concerning regulation,

membership, sales compliance, financial compliance, market surveillance, trading desks compliance and enforcement of the Rules with respect to its Dealer Members, Marketplaces Members and Approved Persons.

Membership Intake has three main responsibilities:

1. Intake, review, and recommendation of new membership applications for Dealer Members
2. Review of current Dealer Member transactions including crypto asset trading platforms, dual-registration, and other material changes to business activities
3. Intake and administration of Dealer Member changes in ownership, changes in structure, and membership resignations¹⁰.

Trading Conduct Compliance

T&C 15(2) of the Recognition Orders states that the TCC group is to ensure that CIRO must administer and monitor compliance with both the applicable Rules and Canadian Securities Legislation by Members and others subject to its jurisdiction and enforce compliance with the Rules by Dealer Members, including ATs, and others subject to its jurisdiction.

Subsection 6.1(b) of NI 21-101 requires all ATs to be a member of a self-regulatory entity, and therefore each AT operating in Canada has contracted with CIRO to act as its self-regulatory provider and has become a Member of CIRO.

The main elements of Trading Conduct Compliance's work are:

1. Administer and monitor compliance of Dealer Members including ATs with respect to applicable CIRO rules and Canadian Securities Legislation
2. Work with Market Policy department on rulemaking
3. Collaborate with CIRO Enforcement to investigate potential cases of wrongdoing

¹⁰ As of April 1, 2025 these responsibilities have been assigned to CIRO Member Services & Innovation department.