Oversight Review Report of the Investment Industry Regulatory Organization of Canada

Issued: July 4, 2017

Table of Contents

I. Introduction

The Investment Industry Regulatory Organization of Canada (IIROC) is the national self-regulatory organization (SRO) that oversees all investment dealers, as well as trading activity on debt and equity marketplaces in Canada.

IIROC is recognized as an SRO by the Alberta Securities Commission (ASC), the Autorité des marchés financiers (AMF), the British Columbia Securities Commission (BCSC), the Financial and Consumer Affairs Authority of Saskatchewan (FCAA), the Financial and Consumer Services Commission of New Brunswick, the Manitoba Securities Commission (MSC), the Nova Scotia Securities Commission (NSSC), the Office of the Superintendent of Securities, Service Newfoundland and Labrador, the Ontario Securities Commission (OSC), and the Prince Edward Island Office of the Superintendent of Securities, collectively, the Recognizing Regulators (RRs). IIROC's head office is in Toronto with regional offices in Montréal, Calgary and Vancouver.

This oversight review was conducted jointly by RR staff (Staff) of the ASC, AMF, BCSC, FCAA, MSC, NSSC and OSC.

This report details the objectives, methodology, frame of reference, report format, scope, overall assessment, and findings of the review for the period from April 1, 2015 to July 31, 2016 (the review period).

1. Objective

The objective of the oversight review was to evaluate whether the selected regulatory processes were effective, efficient, and applied consistently and fairly, and whether IIROC complied with the terms and conditions of the RRs' recognition orders.

2. Methodology

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

- assess the inherent risks of each functional area or key process based on:
  - reviews of internal IIROC documentation (including management self-assessments and risk assessments)
  - information received from IIROC in the ordinary course of oversight activities (periodic filings, discussions with Staff)
  - extent and prioritization of findings from the prior oversight review
  - 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 IIROC as a whole or on multiple departments
- assign an initial overall risk score for each area
- discuss with IIROC to 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
- use the adjusted risk scores to determine the scope of the review

3. Frame of Reference

Staff last performed an oversight review of IIROC in 2015. As a result of that review, Staff issued and published a report on March 3, 2016 (the 2015 oversight report), which noted a number of regulatory related findings, particularly in the Enforcement department with two high priority repeat findings. The 2015 oversight report included applicable action plans as described by IIROC to resolve the findings with timelines, which were reviewed, ultimately accepted and followed up by Staff within the normal course of Staff's oversight activities.

Since the last oversight review, IIROC has a new three year strategic plan in place to inform and shape their regulatory approach to fulfill their mandate to protect investors and to support healthy capital markets in Canada. As part of the risk assessment process, Staff assessed the following identified key trends and their implications on IIROC as an organization, and on the relevant functional areas and processes:

- *Rapid pace of technological change*: IIROC has made a strategic decision to enhance the use of technological tools to better perform its responsibilities (e.g. equity and debt market surveillance). This strategy implies increased funding and other resource needs, including enhanced staff competencies, as well as the continuing impact on IIROC's existing IT infrastructure and controls.

- *Changing investor demographics*: With an aging population tied to a significant portion of investable assets, seniors have been identified as vulnerable investors, resulting in higher public and regulatory expectations regarding investor protection; coupled with new millennial investors seeking more "do it yourself" options, IIROC Dealer Member business models have continued to evolve. These changes imply that IIROC may need to adapt existing regulatory approaches to changing business models to ensure that proper regulatory outcomes (e.g. an effective compliance to enforcement continuum) continue to be achievable.

- *Changing regulatory landscape*: Changes in statutory requirements (e.g. Client Relationship Model – Phase 2) and expectations of IIROC (e.g. perform debt market surveillance) have required IIROC to adapt its own rules, requirements and processes. These changes imply that IIROC will have to continue to expend resources to interpret and implement necessary changes to regulatory processes and systems to keep pace with the evolving regulatory environment.

4. Report Format

In keeping with a risk-based approach, this report focuses on those functional areas or key processes with findings that require corrective action. While each finding requires an

IIROC response and description of the corrective action to be taken, not all findings were made in each regional office where a particular IIROC function or process was sampled for testing. However, as applicable, Staff require that IIROC take corrective action that will ensure nationwide consistency in IIROC's approach.

5. Scope

In consideration of the status of the resolution of findings from the prior oversight review and the challenging issues that may impact IIROC, through the risk assessment process, Staff identified specific processes and activities[1] within the following above average risk areas as the focus for the review[2]:

Above Average

- Business Conduct Compliance
- Enforcement
- Information Technology
- Trading Review & Analysis
- Market Surveillance (Equity & Debt)

Also through the risk assessment process, Staff determined that the following moderate and low risk areas would not be examined during this review[3]:

Moderate

- Membership & Registration
- Financial & Operations Compliance
- Trading Conduct Compliance
- Policy
- Risk Management
- Financial Operations

Low

- Corporate Governance

6. Priority of Findings

Staff prioritized findings into high, medium, and low, based on the following criteria:

High Staff raise an issue that, if unresolved, will result in IIROC not meeting its mandate, or one or more of the terms and conditions of its recognition orders, or the applicable regulatory requirements. IIROC must immediately put in place an action plan (with any supporting documentation) and timelines for addressing the finding that are acceptable to Staff. If necessary,

[1] The processes and activities are described in more detail within the body of the report.
[2] No functional areas were determined to be categorized as High.
[3] The areas continue to be subject to oversight by the RRs through ongoing mandatory reporting by IIROC as required by the Recognition Orders, as well as regularly scheduled and ad hoc meetings between the RRs and IIROC staff.

compensating controls should be implemented before the finding is resolved. IIROC must report regularly to Staff on its progress.

Medium Staff raise an issue that, if unresolved has the potential to result in an inconsistency with IIROC's mandate, or with one or more of the terms and conditions of its recognition orders, or with applicable regulatory requirements. IIROC must put in place an action plan (with any supporting documentation) and timelines for addressing the finding that are acceptable to Staff. If necessary, compensating controls should be implemented before the finding is resolved. IIROC must report regularly to Staff on its progress.

Low Staff identified an issue requiring improvement in IIROC's processes or controls and are raising the issue for resolution by IIROC's management.

Repeat Finding A finding that was previously identified by Staff and not resolved by IIROC will be 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.

7. Summary of Findings and Assessment

In two separate functional areas, IIROC failed to ensure sufficient progress in resolving specific issues raised in the 2015 oversight report. Staff note a repeat finding in the Business Conduct Compliance department given IIROC did not implement necessary changes to their examination programs, even though IIROC had previously informed Staff that the changes were complete. This repeat finding has been prioritized as high. Similarly, Staff note that IIROC did not provide an information security program report to a Board committee on a quarterly basis, as represented in IIROC's response in the 2015 oversight report. This finding in the Information Technology department has been prioritized as medium. Staff acknowledge that IIROC made sufficient progress in resolving other findings cited in the 2015 oversight report. Staff also note other medium priority findings in the Business Conduct Compliance (one), Information Technology (one) and Enforcement (two) departments. Only one low priority finding was noted in the Market Surveillance (Equity & Debt) department, and no findings were noted in the Trading Review & Analysis department. Staff expect IIROC to resolve the findings, and Staff will continue to actively monitor and follow-up on IIROC's progress in taking specific and timely corrective action on the findings detailed within the report in accordance with the priority assigned.

The findings are set out in the *Fieldwork & Findings* section of the report. Other than the findings noted, Staff did not identify concerns with IIROC meeting the relevant terms and conditions of the recognition orders in the areas covered. Staff make no comments or conclusions on IIROC operations or activities that are outside the scope of the review.

II. Fieldwork & Findings

A. Business Conduct Compliance

Under Term & Condition 8(b) of the Recognition Orders, IIROC must administer and monitor compliance with securities laws and IIROC Rules by Dealer Members and others subject to its jurisdiction, including Alternative Trading Systems (ATSs).

Business Conduct Compliance (BCC) staff monitor Dealer Members' compliance with all non-financial regulatory requirements. For example, by way of on-site examinations, BCC staff assess Dealer Members' compliance with requirements pertaining to the suitability of investments, account opening documentation, supervision of (i) advisors, (ii) other staff and (iii) business locations, personal trading and outside business activities. Depending on a particular Dealer Member's business model, BCC staff may also assess the corporate finance and other firm specific activities such as managed accounts.

The 2015 oversight review identified two medium priority findings – (i) insufficient examination procedures with respect to client managed accounts, and (ii) an inadequate process to approve and update an internal authority and delegation document (i.e. Approval List). Since then, continuing changes in investor demographics and the Canadian securities regulatory landscape have required IIROC to strategically reassess the effectiveness of existing regulatory approaches and the impact on finite resources.

As a result, Staff focused their review on:

- IIROC's progress in resolving the findings from the 2015 oversight report
- following up on the implementation of examination procedures to assess compliance with the following securities legislation requirements: (i) dealer sales practice requirements under National Instrument 81-105 *Mutual Fund Sales Practices* (NI 81-105) and (ii) best execution obligations with respect to client managed accounts[4]
- assessing the adequacy of BCC process(es) for handling repeat findings (e.g. action plans, referral to Enforcement, etc.)
- assessing the adequacy of examination files completed using the new risk-based approach[5]

[4] A separate CSA project had been initiated in 2014 whereby IIROC agreed to assess Members' compliance with specific aspects of securities legislation not fully contemplated by current IIROC Rules or Regulations.

[5] The new risk-based approach provides guidance to BCC examination staff as to the scope and extent of testing for the existence of controls. This is done by way of inquiry, observation and walkthroughs, followed by an assessment as to the level that the firm control and supervisory infrastructure (i.e. culture of compliance or tone at the top) could be relied upon, which would then dictate the extent of substantive testing required to assess the effectiveness of the firm control and supervisory infrastructure.

- assessing the adequacy of BCC examination procedures and sampled files to identify conflicts of interest and inappropriate business titles, and if BCC has taken sufficient action to ensure Dealer Members have resolved these concerns
- assessing the effectiveness of the new process(es) used by Quebec BCC staff conducting business location and one head office reviews in the Atlantic region

Staff reviewed the following documents:

- BCC examination program module changes within the review period
- a sample of examination files and examination reports
- a sample of referral memos to Enforcement
- BCC policies and procedures manual

Staff are satisfied that IIROC resolved the finding relating to the Approvals List as described in the 2015 oversight report. However, Staff noted that the other finding from the previous oversight review pertaining to the adequacy of examination procedures to assess suitability in managed accounts had not been resolved. As IIROC had described steps in the response to the 2015 oversight report that represented that the issue had been resolved, Staff raise a repeat finding. As well, IIROC failed to implement procedures to assess Dealer Member compliance with NI 81-105 as previously agreed upon with Staff. IIROC's lack of follow through on the above commitments made to Staff are a concern. A new medium priority finding relating to report deficiency definitions is also described below.

Furthermore, in Staff's assessment of IIROC's new risk-based approach, Staff acknowledge that IIROC has provided better guidance and clarity to procedures for examination staff. Going forward, as more compliance reviews are completed, Staff expect IIROC to further refine those procedures and increase examiner specific training to ensure that a Dealer Member's overall commitment to compliance is appropriately measured by IIROC examination staff. And more specifically, given BCC staff have had difficulty in past examinations ensuring certain Dealer Members addressed deficiencies on a timely basis, Staff further expect IIROC to take regulatory action (i.e. referral to Enforcement, imposition of terms and conditions) to ensure deficiencies do not persist over long periods of time.

Staff also acknowledge that IIROC's new Consolidated Enforcement, Examination and Approval Rules relating to registration approvals (including the authority to impose terms and conditions on Dealer Members) became effective on September 1, 2016. Going forward, this could be an important tool to achieve proper regulatory outcomes and Staff expect IIROC to use the tool when warranted, especially with respect to Dealer Members with repeat and /or significant deficiencies to ensure the deficiencies are resolved on a timely basis.

Lastly, Staff note that during the review period, IIROC implemented ad hoc procedures pertaining to best execution for specific Dealer Members with managed funds, as well as

providing staff training on specific firm obligations. As a result of IIROC's internal review of the few examination files where the procedures were completed, and IIROC's on-going rationalization review of examination modules, IIROC recently decided that best execution related procedures will be performed by Trading Conduct Compliance (TCC) examination staff. Going forward, Staff expect IIROC to adequately train TCC staff and to implement adequate procedures to test applicable Dealer Member compliance with their best execution obligations, including the consideration of all business lines (e.g. managed accounts).

(1) Finding: Failure to Complete BCC Examination Program Changes on a Timely Basis

As noted above, IIROC did not have processes in place to ensure that the following important examination procedures were implemented, even though timelines had been previously agreed upon with Staff:

- Changes to the examination procedures relating to assessing suitability in client managed accounts - the same finding was initially raised in the 2015 oversight report[6], and in their response, IIROC stated that a number of changes had already been made to resolve the finding, and furthermore, described the changes to the procedures in detail.[7] However, at the start of the 2016 oversight review, Staff confirmed that the changes had not been incorporated into the applicable examination modules. Staff note that the revised procedures were implemented in October 2016, eight months after IIROC initially stated the changes had been made.
- New examination procedures for assessing Dealer Members' compliance with certain aspects of NI 81-105 - Staff were informed at the commencement of the review that the procedures had not been implemented as agreed upon by June 30, 2016, and furthermore, were not even designed by that date. Staff were subsequently informed that the revised procedures were implemented in February 2017, more than seven months later.

Staff were informed that IIROC's current management were unaware that the above noted procedures had not been implemented by the agreed upon timelines. Going forward, Staff expect IIROC to assess its processes for the monitoring and resolution of issues and the tracking of required work flow, and to evaluate their effectiveness.[8]

Why this is Important / Risk Implication	The failure to undertake corrective action and effectively monitor and manage the resolution of issues as represented and agreed upon, could result in IIROC not meeting one of the terms and

[6] In the 2015 oversight report, the finding was categorized as medium priority.
[7] Staff were informed that the representation that the prior oversight review finding was resolved was made by the previous BCC management.
[8] See also (1) Finding: *Untimely Reporting – Information Security Program Material to the Finance, Audit and Risk (FAR) Committee* in the Information Technology section in regards to the monitoring and resolution of issues.

	conditions of its recognition orders, or applicable regulatory requirements.
Priority	**High**
Requirement	Please describe the action plan that IIROC will take to address this finding, including a timeline for resolution.
IIROC's Response	*IIROC acknowledges the finding, which was due in large part to the timing of a change in BCC management. IIROC will institute a process whereby the supporting work (new processes or procedures) to address and respond to identified issues raised from the CSA oversight reviews and other areas within IIROC (e.g. from internal audit reports) will be provided to General Counsel's Office before the finding will be considered resolved.*
Staff Comments and Follow-up	Staff are encouraged that IIROC will institute a centralized process whereby the General Counsel's Office will manage the tracking and resolution of issues raised in CSA oversight review reports. Staff expect the new process to be in place by no later than September 30, 2017; and also expect the General Counsel's Office to monitor and track the resolution of other identified issues (e.g. from internal audit reports), and to report on the effectiveness of the new process instituted by March 31, 2018.

(2) Finding: Inability to Resolve Report Deficiencies Due In Part to a Lack of Guidance / Definitions BCC staff have had difficulty in ensuring certain Dealer Members adequately resolve repeat and / or significant deficiencies on a timely basis. The inability to resolve deficiencies is due in part to the lack of written guidance for BCC staff to categorize findings in the examination reports or define what constitutes a (i) repeat, (ii) significant, (iii) significant repeat or (iv) other finding and what constitutes an appropriate regulatory response by Dealer Members.	
Why this is Important / Risk Implication	Without guidance or definitions, it is more likely that the classification of findings across various examination reports would not be consistent, and therefore, especially with problematic Dealer Members, the desired and appropriate regulatory outcomes may not be achieved and effectively prioritized.
Priority	**Medium**

Requirement	Please describe the action plan that IIROC will take to address this finding, including a timeline for resolution.
IIROC's Response	*IIROC acknowledges the finding.* *BCC is establishing a working group to develop guidance for categorizing findings as "repeat", "significant", "significant repeat" or "other". We plan to complete this guidance by the end of September 2017.* *As one of its strategic initiatives, IIROC is also currently drafting guidance describing an analytic framework to assist staff in determining whether a compliance issue should be referred to Enforcement. The framework includes considering when a deficiency is not adequately resolved by the Dealer Member.* *Both of these internal guidance documents will help staff gain a more consistent understanding of how to categorize exam findings and when the nature of the finding or compliance issue is such that a referral to Enforcement is warranted.*
Staff Comments and Follow-up	Staff note that IIROC is developing an analytic framework and internal guidance documents. By September 30, 2017, Staff expect IIROC to provide an update on the status of the guidance describing an analytic framework and to have the internal guidance for the categorization of findings in place (including training for applicable IIROC staff). Staff also expect IIROC to monitor and report on their status and effectiveness by March 31, 2018.

B. Enforcement

Term & Condition 8 of the Recognition Orders require IIROC to enforce compliance with its rules by Dealer Members, ATSs, registrants and others subject to its jurisdiction.

To meet its regulatory requirements, IIROC Enforcement staff are organized into the following groups:

- case assessment
- investigations
- litigation

A group to handle client complaints and inquiries is separate from the Enforcement department, although the Director is also the Director of Case Assessment.

Enforcement staff are primarily responsible for:

- performing a preliminary assessment of case files
- investigating complaints or referrals about possible regulatory misconduct
- taking disciplinary action when misconduct has taken place

The 2015 oversight review identified two high priority findings – (i) enforcement case management database (ECM) access management and (ii) inconsistent application of file standards, and two medium priority findings – (i) lack of policies and procedures pertaining to Market conduct case files and (ii) lack of independent review and approval for Market conduct case files. Since then, given the change in Dealer Member business models as a result of changing investor demographics, Staff were of the view that it would be prudent to also examine IIROC's existing regulatory approaches to ensure that effective investor protection would continue to be achievable.

As a result, Staff focused their review on:

- IIROC's progress in addressing the findings from the 2015 oversight report
- assessing the adequacy of how IIROC handles Dealer Members that have consistently demonstrated a failure to resolve issues and have a history of Enforcement actions
- assessing the adequacy of the regulatory responses to Dealer Members with a history of Enforcement actions
- evaluating how IIROC assesses the adequacy of a Dealer Member's own complaint handling procedures

Staff reviewed the following documents:

- Enforcement file statistical data
- A sample of Dealer Member and market conduct cases
- the Enforcement policies and procedures manual
- ECM access related information
- Referral memos and related documentation

Staff are satisfied that IIROC made adequate progress to resolve the 2015 oversight report findings. However, Staff raise two new medium priority findings detailed below pertaining to the (i) compliance to enforcement referral process and (ii) lack of a centralized process to ensure a holistic view of Dealer Members for Enforcement purposes.

(1) Finding: Inadequate Process - Pre-referral Meetings with IIROC Compliance Staff

IIROC has many established Enforcement processes in place to carry out its regulatory responsibilities. One such process that was examined by Staff pertains to an applicable Enforcement and Compliance staff meeting to discuss key Dealer Member examination report deficiencies cited by Compliance staff. The meeting is conducted prior to the written referral being made by Compliance staff to the Enforcement department, and is therefore known as a "pre-referral" meeting[9]. However, as part of our review, Staff were informed that:

- no minutes or summaries of the pre-referral meetings were maintained, and
- while there were established Case Selection criteria in other Enforcement areas, written guidance had not yet been developed for Enforcement staff participating in the pre-referral meetings to assist in determining which key compliance deficiencies would likely be prioritized and investigated by Enforcement staff if referred.[10]

Therefore, it was not apparent to Staff why in some instances key compliance deficiencies taken to pre-referral meetings for discussion did not result in written referrals to Enforcement.

Why this is Important / Risk Implication	Without meeting minutes / summaries and written guidance / criteria for pre-referral meetings, the referral process may be ineffective and inconsistent, and could result in Enforcement failing to pursue significant compliance issues, especially for Dealer Members with multiple issues.
Priority	**Medium**
Requirement	Please describe the action plan that IIROC will take to address this finding, including a timeline for resolution.
IIROC's Response	*IIROC acknowledges this finding.*

[9] The purpose of the meeting is to provide the referring department an opportunity to discuss and better understand Enforcement staff's views and possible concerns as they relate to the key examination findings, before deciding which findings will be referred.
[10] The decision to ultimately make a referral will rest with the referring department.

	While these meetings are intended to be somewhat informal, IIROC recognizes the value in documenting a summary of the discussions held at these meetings. As these meetings are at the request of the referring compliance department, moving forward the compliance department will document the results of any scheduled pre-referral meetings. *In regards to further guidance in making referrals to Enforcement, this issue is being addressed through IIROC's Strategic Plan (FY 2017-2019). As part of this Plan, one of Enforcement's key initiatives is to strengthen the process of compliance referrals to Enforcement. This will involve a review of the current process and the development of a framework to assist the compliance groups in assessing whether to make a referral to Enforcement.*
Staff Comments and Follow-up	Staff note that going forward, IIROC staff will document the results of scheduled pre-referral meetings. Staff expect that other relevant information discussed in the meetings that was relied upon for a result will also be summarized. By September 30, 2017, Staff expect that the written requirement will be in place and that IIROC will provide a status update on the development of the noted framework. Lastly, Staff expect IIROC to monitor and report on their status and effectiveness by March 31, 2018.

(2) Finding: Inadequate Enforcement Process – Holistic View of Dealer Members In discussions with IIROC Enforcement staff, Staff were informed that there was no formal requirement or central process to ensure that a holistic view of Dealer Members (including a history of regulatory actions applicable to each Dealer Member for Enforcement specific purposes) was in place. Such a process could provide intelligence to guide IIROC Enforcement staff on how best to handle problematic Dealer Members with multiple issues so that those issues do not persist over a long period of time.	
Why this is Important / Risk Implication	Without a holistic view of a Dealer Member, issues could be assessed in isolation rather than on a collective basis, which may result in Enforcement not taking appropriate action against Dealer Members who have a history of non-compliance.
Priority	**Medium**
Requirement	Please describe the action plan that IIROC will take to address this finding, including a timeline for resolution.

IIROC's Response	*IIROC acknowledges that there is no formal or centralized process in place. Notwithstanding, Enforcement does, from various sources, have access to and considers all the relevant information for its cases including the compliance history of a firm. We recognize additional measures can be taken to better document staff's efforts to ensure they are considering the totality of all relevant circumstances and addressing firms with multiple issues in a timely manner. Staff will take steps to ensure these considerations are properly documented in their investigation memoranda. Staff will also ensure the regulatory history of a firm is appropriately considered as part of the new compliance referral process. We anticipate these additional measures will be in place by the end of July 2017.*
Staff Comments and Follow-up	Staff are encouraged that IIROC will implement by July 31, 2017 additional measures to ensure IIROC Enforcement staff have a more holistic view of a Member firm, whereby all relevant case information is considered and documented, including the regulatory history of a Dealer Member. Staff expect IIROC to monitor and report on the effectiveness of the additional measures by March 31, 2018.

C. Information Technology

Under Term & Condition 11 of the Recognition Orders, IIROC must ensure critical technology systems have appropriate (i) internal controls to ensure the integrity and security of information and (ii) capacity; as well as controls that manage the risks associated with its operations.

IIROC's Information Technology (IT) department is responsible for the overall design, maintenance, delivery and security of technology related applications and systems required to support IIROC's business operations and strategic goals.

The 2015 oversight review identified three medium priority findings – (i) inadequate processes and documentation of Board of Directors (Board) decisions related to information security, (ii) inadequate personnel proficiencies, abilities and / or expertise, and (iii) insufficient information security policies and procedures. Given IIROC's strategic decision to use technological tools to better perform its regulatory responsibilities, the risk of inadequate resources to manage required changes to the existing IT infrastructure and related controls is significant.

As a result, Staff focused their review on:

- following up on the progress IIROC has made in addressing the findings from the 2015 oversight report
- assessing the adequacy of information security policies and procedures updated or implemented subsequent to the 2015 oversight review
- reviewing IT related Enterprise Risk Management (ERM) features to assess the methodology used for evaluating IT related internal control verification procedures

Staff reviewed the following documents:

- the departmental organizational chart and qualifications of staff
- procurement related information
- annual Information Security Report and other reports
- information security policies and procedures
- ERM related information
- internal control testing methodology documentation

Staff noted that within the review period, IIROC hired additional staff with specialized competencies and initiated other IT related projects. Staff also noted that IIROC made progress to resolve the previous oversight review findings as described in the 2015 oversight report.

Staff raise two medium priority findings pertaining to (i) the lack of timely reporting of required information security program material to the Finance, Audit and Risk Committee, and (ii) an inadequate methodology used for IT related control verification procedures.

(1) Finding: Untimely Reporting – Information Security Program Material to the Finance, Audit and Risk (FAR) Committee

Staff acknowledge that IIROC has many established processes in place that are designed to communicate information within the organization on a timely basis. However, in following up on IIROC's remediation of findings from the 2015 oversight report, Staff confirmed that an IT dashboard report on the progress of the information security program was not provided to the FAR committee on a quarterly basis, even though the Board directed IIROC staff to do so as represented by IIROC management in their response to a finding in the 2015 oversight report. Furthermore, Staff confirmed that business units or departments were responsible for monitoring the progress of their related remediation plans and that IIROC[11] did not have adequate controls in place to ensure new processes, such as the quarterly reporting requirement to the Board, were implemented and operating as intended.

Why this is Important / Risk Implication	A potential lack of information at the Board committee level may lead to ineffective Board oversight and inaccurate decisions being made. As well, the absence of a monitoring process for those controls designed to remediate identified issues could result in the persistence of the underlying issues. This could in turn adversely affect IIROC's business operations, and if not resolved, have the potential to result in an inconsistency with one or more of the terms and conditions of IIROC's recognition orders or with applicable regulatory requirements.
Priority	**Medium**
Requirement	Please describe the action plan that IIROC will take to address this finding, including a timeline for resolution.
IIROC's Response	*Maintaining IIROC's internal information security posture at a high level and cyber preparedness of IIROC Members continue to be priorities of the IIROC Board of Directors and the Finance, Audit and Risk Committee. Both the Board and the FAR Committee are kept fully informed of status, developments and improvements. Comprehensive information and reports on Information Security are provided on a regular basis.* *Whilst IIROC acknowledges that the specific Information Security Program Dashboard mentioned in the finding was not provided at all quarterly meetings of the FAR Committee during*

[11] See also (1) Finding: *Failure to Complete BCC Examination Program Changes on a Timely Basis* in the Business Conduct Compliance section in regards to the monitoring and resolution of issues.

	the review period (as no significant new information arose since the previous reports), other extensive information was provided to the FAR Committee and the Board at each meeting that provided a comprehensive update on the progress of information security initiatives across IIROC. *The IT Information Security Program Dashboard will be provided to the FAR Committee on a quarterly basis even if no new significant updates are available since the previous report.*
Staff Comments and Follow-up	Staff are encouraged that IIROC's own information security and the cybersecurity preparedness of Members continue to be priorities of IIROC's Board and FAR Committee. Staff expect IIROC to record in the quarterly meeting minutes that the IT Information Security Program Dashboard was provided to the FAR Committee, and other applicable information relevant to the discussion of the Dashboard.

(2) Finding: Inadequate Process – IT Related Enterprise Risk Management Testing Methodology Staff noted that the control verification methodology was not clearly defined and documented to conclude if IT related mitigating controls were operating as designed.	
Why this is Important / Risk Implication	Inadequate documentation of the methodology used increases the risk that control verification procedures do not properly support conclusions on the design adequacy of the mitigating controls.
Priority	**Medium**
Requirement	Please describe the action plan that IIROC will take to address this finding, including a timeline for resolution.
IIROC's Response	*IIROC acknowledges that a documented methodology for control verification for Enterprise Risk Management (ERM) does not exist. We believe that a documented methodology will not reduce the level of risk that control verification insufficiently supports conclusions on the design adequacy of mitigating controls. The key mitigation is that control verification scripts are appropriately designed and effectively executed based on the nature of each control. For every control verification performed, we perform process walkthroughs to understand the process and the nature of the controls. This information is then used in creating a control verification script of the procedures our*

	independent reviewers will perform. The control verification scripts are designed to support our conclusions on the existence of mitigating controls. We consistently applied this approach for all our control verification work since FY2015. IIROC also has a documented risk-based verification criteria, which was utilized in determining which controls to test and the appropriate frequency of verification. *IIROC has aligned its entire ERM Framework (not just for IT related ERM) with ISO 31000:2009 Risk management – Principles and guidelines. This industry standard does not contemplate control verification processes as part of an organization's ERM Framework. IIROC has, of its own volition, included control verification procedures within the Monitor and Review phase of its Risk Management Methodology. The ERM control verification that is performed was never intended to provide an audit opinion or assurances around IIROC's internal control environment. The results are simply used to determine whether the business risk self-assessments need to be re-evaluated based on the independent review of internal controls.* *In response to CSA staff:* 1. *IIROC plans on clearly noting in our annual risk management report to the FAR Committee of the Board that the ERM control verification work performed is not intended to provide an attestation or assurance over the operating effectiveness of our internal control environment.* 2. *IIROC will create a formalized procedure document outlining the control verification process undertaken for ERM. The procedure will formalize elements of guidance that have already been documented and shared within IIROC. It will focus on the key steps within the control verification process e.g.:* a. *criteria utilized in determining what controls to verify;* b. *frequency of control verification;* c. *allocation of resources to control verification;* d. *documentation standards; and* e. *review workflow* *We expect that the procedure document will be completed by end of October 2017.*

Staff Comments and Follow-up	Staff note that IIROC acknowledges that a documented methodology for control verification for ERM related testing did not exist. Staff also note that IIROC will create a formalized procedure document outlining the control verification process to be undertaken for ERM, as well as communicating to the FAR Committee about the intentions of the ERM control verification work performed. Staff expect IIROC to complete the procedure document by October 31, 2017, and to monitor and report on the effectiveness by March 31, 2018.

D. Trading Review & Analysis

Under Term & Condition 8(b) and (c) of the Recognition Orders, IIROC must administer and monitor compliance with securities laws and IIROC Rules by Dealer Members and others subject to its jurisdiction, including ATSs; and if retained by an exchange or quotation and trade reporting system, IIROC must administer, monitor and / or enforce rules pursuant to a regulation services agreement.

IIROC's Trading Review & Analysis (TR&A) department is primarily responsible for conducting:

- preliminary investigations when there are reasons to believe that improper trading activity on marketplaces may have occurred
- post-trade analysis of trading data
- special projects and reviews related to trading

Staff last reviewed TR&A in the 2014 oversight review and did not identify any high or medium priority findings. Since the 2014 oversight review, the IIROC Enforcement department revised its market case referral process whereby TR&A completes all market case assessments and refers applicable cases directly to the Enforcement Investigations group. Given the reliance on data and technological tools, and to better understand TR&A's role in post-trade debt surveillance, Staff focused their review on:

- assessing and evaluating the effectiveness of the revised TR&A market case referral process
- assessing TR&A's role in performing data analysis and / or preliminary investigations for debt market related transactions

Staff reviewed the following documents:

- a sample of market case referrals
- TR&A organizational charts
- TR&A policies and procedures manual

Staff are satisfied with the revised TR&A market case referral process. As well, Staff confirmed that TR&A continues to perform data analysis or preliminary investigations of equity transactions, and that the new Debt Market Surveillance group is responsible for data analysis and post-trade investigations of debt transactions using TR&A processes tailored for their purposes.

Finding

There were no findings noted for the area.

E. Market Surveillance (Equity & Debt)

Under Terms & Conditions 8(b) and 11 of the Recognition Orders, IIROC must administer and monitor compliance with securities laws and IIROC Rules by Dealer Members, ATSs, registrants and others subject to its jurisdiction, and ensure that its critical systems have appropriate internal controls to ensure integrity and security of information, and sufficient capacity to enable IIROC to properly carry on its business.

IIROC's Market Surveillance (Equity & Debt) – MS department:

- conducts real-time monitoring of trading on all Canadian equity marketplaces
- conducts post-trade monitoring of trading on eligible debt marketplaces
- collects information from Dealer Members on over-the-counter debt trading and is building a surveillance database for reported debt transactions
- may halt trading in particular securities or all securities, and may cancel or reprice unreasonable trades as part of its regulatory responsibilities
- currently uses the Surveillance Technology Enhancement Platform (STEP). STEP provides MS with a single portal through which to monitor equity trading activity. STEP includes SMARTS, which is the system that generates equity trading alerts and has features allowing customized views of market activity

Staff last reviewed MS in the 2014 oversight review and did not identify any high or medium priority findings. With the IIROC debt transaction reporting rules that came into effect in November 2015, IIROC established a new Debt Market Surveillance department (DMS) and has invested in technology to perform debt reporting data analysis.[12] DMS also conducts preliminary post trade monitoring of debt trading activity that may potentially be in violation of applicable IIROC Rules or securities legislation. This function of DMS is similar to the function that the TR&A department conducts in relation to equity trading activity.

As a result, Staff focused their review on:

- assessing the structure of DMS to determine if DMS has adequate resources and competencies to perform its regulatory tasks
- evaluating the appropriateness and adequacy of debt market monitoring policies and procedures
- reviewing how IIROC acquires debt transaction data from Dealer Members and to assess if the processes in place are adequate
- evaluating the adequacy of the parameters used by IIROC's debt surveillance system to generate reports and alerts
- assessing the adequacy of the investigative techniques used by DMS in regards to debt surveillance monitoring

[12] DMS is independent from Equity Market Surveillance, with separate reporting lines, fee model and budget.

Staff reviewed the following documents:

- statistical data for and a sample of generated debt market surveillance alerts
- training and continuing educational program related information
- policies and procedures manuals for DMS
- organizational chart and position descriptions for DMS
- alert development related information

Staff acknowledge that IIROC has taken initial steps in the development of DMS. Staff expect IIROC to continue to develop, assess, refine and enhance the necessary DMS processes and procedures, especially pertaining to resources, benchmarks, policies and procedures, alert development and monitoring tools.

As a result of our review of a sample of alerts that were handled by IIROC DMS staff, Staff raise the following low priority finding.

(1) Finding: Incomplete Documentation Within Debt Market Surveillance Records

Staff noted that a sample of alert records were incomplete as a result of inconsistent documentation. More specifically, certain exchanges between DMS staff and Dealer Members were not properly documented; and while corrective actions such as adjustments or cancellations of trades were recorded, the fact that an alert was closed with no action was not.

Why is this Important / Risk Implication	Inconsistent or incomplete documentation may result in DMS staff not being able to effectively demonstrate why a decision regarding an alert was made, especially after a significant period of time.
Priority	**Low**
Requirement	Please describe how IIROC will resolve the finding.
IIROC's Response	*IIROC acknowledges the finding.* *All exchanges with Dealer Members' staff related to alert investigations, including telephone conversations, are now recorded in the alert audit trail (for example, the time of call, details of response, etc.). All alerts are closed with a final disposition/explanation.*
Staff Comments and Follow-up	Staff acknowledge IIROC's response and have no further comment.