Registrant Outreach Seminar
June 23 and 25, 2015

Elements of an Effective Compliance System

Presenters: Trevor Walz, Dena Di Bacco and Stratis Kourous
Compliance and Registrant Regulation Branch

OSC ONTARIO SECURITIES COMMISSION

Disclaimer

This presentation is provided for general information purposes only and does not constitute legal or accounting advice.

Information has been summarized and paraphrased for presentation purposes and the examples have been provided for illustration purposes only.

Information in this presentation reflects securities legislation and other relevant standards that are in effect as of the date of the presentation.

The contents of this presentation should not be modified without the express written permission of the presenters.

Agenda

1. Key elements of an effective compliance system

2. Roles and responsibilities of the UDP and CCO

3. CCO annual report to the board of directors

4. Key aspects of policies and procedures manual and its effective implementation

5. Emerging compliance issues

6. Questions

Key elements of an effective compliance system

OSC ONTARIO SECURITIES COMMISSION

Compliance system requirements

Section 11.1 of NI 31-103 – A registered firm must establish, maintain and apply P&Ps that establish a system of controls and supervision to:

(a) provide reasonable assurance that the firm and its individuals comply with securities law, and

(b) manage its business risks in accordance with prudent business practices.

Key elements of effective compliance system

Section 11.1 of 31-103CP:

- Internal controls
- Monitoring and supervision
  - Day-to-day
  - Systemic

Specific elements:

- Visible commitment
- Sufficient resources and training
- Detailed policies and procedures
- Detailed records

OSC review of firm's compliance system

- For all compliance reviews, we assess overall adequacy of compliance system and if UDP and CCO are fulfilling their responsibilities
- Examples of steps performed to assess compliance system & UDP/CCO:
  - Interview UDP and CCO and other staff (proficiency and duties)
  - Review delegation of compliance duties
  - Assess if back-up CCO in place
  - Review internal controls, supervisory structure and risk management
  - Review policies and procedures manual and code of ethics
  - Review and test complaints and how handled
  - Assess monitoring and testing for compliance (systems and reports)
  - Assess compliance training
  - Assess how identified non-compliance was handled
  - Review and test books and records
  - Review CCO report to board, internal/external audit reports

Examples of inadequate compliance systems

- Large number of deficiencies
- Small number of serious deficiencies
- Repeat deficiencies from prior review
- CCO lack of awareness/understanding of business and operations of firm, its risks, and applicable securities law
- Lack of awareness within firm about compliance processes
- CCO has limited involvement in compliance function
- Renting-out of firm's registration
- CCO can't explain what they do, can't answer our questions
- No (or very poor) internal controls or written policies and procedures
- Policies and procedures not being enforced
- No CCO annual report to board
- No/inadequate monitoring for compliance
- Poor books and records

Consequences of inadequate compliance system

Business

- Client complaints
- Lawsuits
- Loss of existing and new clients

Regulatory

- Offside securities law
- Concerted effort to address deficiencies
- Terms and conditions to:
  - engage a compliance consultant and/or monitor
  - restrict business (e.g. no new clients)
  - replace UDP and/or CCO
- Referral to Enforcement
- Suspension of registration

Observations of effective compliance systems

- Appropriate and tailored to nature, size and risk of firm's operations including products/services, types of clients, and compensating controls
- Proactive identification and timely correction of non-compliance
- Regular testing for compliance, documents results and actions taken
- Risk-based approach to monitoring and testing
- Periodic self-assessments of compliance with securities laws and acts to improve internal controls, monitoring, supervision and P&Ps when necessary
- Identifies and manages key risks, including new products or services, new locations, technology changes

More observations of effective compliance systems

- Treats non-compliance seriously
- Adopts industry best practices
- Keeps informed of industry/regulatory changes
- Involves all employees in compliance
- Training of employees and training tracking
- Good client disclosure and agreements
- Good written policies and procedures manual

Roles and responsibilities of the UDP and CCO

OSC
ONTARIO
SECURITIES
COMMISSION

Requirements of the UDP

Section 5.1 of NI 31-103 states that the responsibilities of the UDP include:

a) Supervise the activities of the firm that are directed towards ensuring compliance with securities legislation by the firm and each individual acting on the firm's behalf; and
b) Promote compliance by the firm, and individuals acting on its behalf, with securities legislation

Responsibilities of the UDP

- Supervise the activities of the firm
  - Meet with CCO on regular basis
  - Involvement in key issues

- Promote compliance
  - Visible commitment
  - Leading by example
  - Being visible/present

Requirements of CCO

Section 5.2 of NI 31-103 states that the responsibilities of the CCO include:

a) Establish and maintain policies and procedures
b) Monitor and assess compliance by the firm, and individuals acting on its behalf, with securities legislation
c) Report to the UDP of the firm as soon as possible if the CCO becomes aware of any circumstances indicating that the firm, or any individual acting on its behalf, may be in non-compliance with securities legislation
d) Submit an annual report to the firm's board of directors

Responsibilities of the CCO

- Establish and maintain policies and procedures manual
- Monitor and assess compliance by firm and individuals
  - Checklist
    - Form 31-103F1
    - Clients' portfolios in line with their IMA
    - Signed annual code of conduct
    - Check pricing source
    - Check personal trading
    - Review complaint log
  - Keeping up to date with changes in legislation
    - Distribution listings
    - OSC annual summary reports
    - Industry associations and committees

Responsibilities of the CCO

- Report to the UDP all instances of non-compliance with securities legislation that:
  - Create a reasonable risk of harm to a client or to the market, or
  - Are part of a pattern of non-compliance
- Adequate training of staff
- Ensure sufficient resources
- Submit an annual report to the board of directors

CCO annual report to the board of directors

OSC ONTARIO SECURITIES COMMISSION

Annual report to the BOD

Contents of a good report

- Status and effectiveness of the firm's internal controls
  - Any deficiencies identified in the firm's or individual's compliance with securities law
  - Internal control weaknesses
- Resources and training
- Changes to firm's P&P
- Status and outcome of any regulatory reviews, internal audits, inquiries or investigations
- Complaints or lawsuits
- Proposed changes to securities law
- Key compliance risks facing the firm and how they are being addressed
- An overall assessment of the firm's and its individuals' compliance with securities law

Annual report to the BOD

Qualities of an effective report:

1. Timely
2. Frequent (where applicable)
3. Detailed
4. Describe actions taken

Exhibit 1

Examples of an annual report to the BOD

Key aspects of policies and procedures manual and its effective implementation

OSC ONTARIO SECURITIES COMMISSION

Key aspects of policies & procedures (P&P)

- P&Ps are key means to establish systems of control and supervision
- Expected to be in writing in a P&P manual
- No prescribed form or standard
- Needs to be appropriate for firm's size, activities and risks
- Policy – the "what", or principles to be adhered to
- Procedures – the "how", or steps to follow to achieve policy principles

Detailed policies and procedures

Per section 11.1 of 31-103CP, P&Ps should:

- Identify controls to be used to comply with laws and manage risk
- Set out standards for conduct, and system for monitoring and enforcing standards
- Outline who is expected to do what, when (frequency), and how
- Be readily accessible
- Be updated when business or laws change (and after testing for effectiveness)
- Consider general duty to deal fairly, honestly and in good faith with clients

Goals of P&Ps and compliance reviews

Goals of P&Ps per CSI CCO Qualifying Exam:

- Establish consistent compliance and performance standards
- Assist in training employees
- Reference point for activities of firm

OSC compliance reviews of P&Ps:

- Pre-registration reviews of applicants
- On-site reviews of registered firms
- All firms must have - no exception for small or inactive firms

Unacceptable practices for P&Ps

- Only a few pages in total
- Names of other firms used in the P&Ps (i.e. not tailored)
- Continuously in draft form
- Refers to outdated securities law
- Use an affiliate's P&Ps that refer to U.S. securities law or IIROC rules (i.e. not tailored)
- Drafted to be compliant with ISO standards, but not tailored for securities firm's business and activities
- Cover letter attached to NI 31-103
- Employees have not read and do not use

Observations of good P&P manual

- Identifies regulatory requirements (and prohibited activities)
- Tailored and applicable to business operations
- Covers all of firm's registration categories
- Sufficient level of length/detail
- Up-to-date
- Detailed table of contents or index
- Has both policy and procedure
- Clear/easy to understand for people using the P&P
- Includes key principles to "follow" the policy
- References applicable section of securities law or other applicable laws
- Clarifies functions and responsibilities
- Includes P&P review responsibility and frequency

More observations of good P&P manual

- States who P&Ps apply to (e.g. which business unit/function), and where they apply
- Uses titles of employees rather than names
- Uses headings and numbering system
- Has process for dealing with compliance issues not specifically covered in manual
- Process for escalating compliance issues to CCO, and regular reporting to senior management and board
- States if firm doesn't permit or engage in a particular activity
- Includes glossary/definition of terms used
- Process for policy exceptions (and maintain exceptions log)
- Dated or numbered for version control
- Includes appendices with standard forms for reference

Expectations for content of P&Ps

Some examples of topics:

- Compliance function (e.g. role of UDP and CCO)
- Risk management
- Code of ethics and personal trading
- Books and records
- Safeguarding of client assets
- Protection of client information (including cyber security)
- Business continuity plan
- Oversight of service providers
- Conflicts of interest
- Marketing practices (including use of social media)
- Portfolio management/trading (including KYC and suitability)
- Complaint handling

See Exhibit 2 (hand-out) for more examples of topics and sub-topics

How to implement P&Ps effectively

- Assign ownership of specific P&P
- Get buy-in/involvement of business units, especially on procedures
- Assess impact of new/change in P&P on services and products
- Consider if outside parties are affected
- Policy on policies
- Trial run/test before roll-out
- Approval by senior management before implemented to get endorsement
- Adequate and regular (e.g. annual) training on P&Ps
- Create training program/schedule
- Do post implementation review
- Employees certify annually that have read (or re-read) and understand

How to implement P&Ps effectively (cont'd)

- Distribute to all employees
- Communicate new P&Ps and changes to existing P&Ps to employees
- Review P&Ps on a regular basis (but at least annually) to assess if current and adequately reflect business operations, industry practices and securities law, and remove non-applicable sections/references
- Along with annual update, CCO should conduct periodic review of P&Ps to ensure adequate and effectiveness of their implementation
- Form a policy review committee
- Test the P&Ps
- Create a schedule to test certain P&Ps by certain dates through-out year
- Create a test matrix

Example 1

3.0 Marketing and Advertising

Policy: All marketing materials must be pre-approved before use to ensure the content is fair, accurate and not misleading.

Marketing materials include website, brochures, social media, …

The policy applies to new marketing materials and changes to existing materials. Examples of misleading marketing include unsubstantiated claims, outdated or inaccurate information, etc.

Procedures:
1. The preparer to provide the draft marketing material to the CCO at least 5 business days before its intended use.
2. CCO to review the draft marketing material and approve for use, or provide any changes required in writing to the preparer within 2 days.
3. CCO to maintain copies of all final marketing materials and approvals on X drive under Marketing Materials folder.

References: CSA Staff Notice 31-325, sections 44 and 46 of Act

Example 2

Oversight of Service Providers

XYZ may outsource certain functions of its operations to 3rd party service providers. When done, XYZ is still responsible for the outsourced functions and must supervise/monitor the activities of the 3rd party to ensure they comply with XYZ P&Ps and applicable securities laws.

XYZ outsources fund administration to ABC Inc. To supervise and monitor ABC, XYZ will do the following:

1. CFO & CCO to meet with ABC every six months to discuss any service issues, and ABC's policies and operations.
2. CFO to obtain and review ABC's daily reports for all XYZ funds. All issues to be discussed with ABC in a timely manner
3. CFO & CCO to annually obtain & review ABC's internal controls report & BCP.
4. CFO & CCO to obtain & review monthly report from ABC self-assessing its compliance with service standards, XYZ policies, and securities law.
5. CFO & CCO to keep evidence of meetings and their reviews, and document any issues & how resolved.

Emerging compliance issues

OSC ONTARIO SECURITIES COMMISSION

Social Media

1. Background
2. Compliance focus areas
3. Questions when developing compliance systems
4. Industry guidance

Social Media

Background

- Social media – refers to interactions among people where they create, share and exchange information and ideas in virtual communities and networks
- Examples of social media platforms used by registrants:
  - Facebook
  - Twitter
  - YouTube
  - LinkedIn
  - Chat rooms
  - Blogs
- Evolving means of communicating with current and prospective clients
- Noticing increased use amongst registrants

Social Media

Compliance Focus Areas

- Treat social media like any other form of marketing
- CSA Staff Notice 31-325 *Marketing Practices of Portfolio Managers* applies to all forms of marketing material, including social media communications
- Social media presents challenges to a compliance system from a supervisory prospective:
  - Information being posted without knowledge of the firm
  - Social media often referred to as interactive communication
  - May be tough to provide complete and fair representation to investors
  - Misleading, exaggerated and unbalanced disclosure leads to misrepresentations

Social Media

Compliance Focus Areas (continued)

- Example of specific deficiencies raised regarding social media:
  - Employee personal website: "company ABC Co. will be going public in the next year or two and the shares currently trading at $0.30 should be trading at $2 to $4 when it goes public."
  - Dealing representative tweet: "if I can provide you with 12% to 18% returns, would you say no to me?"

Social Media

Compliance Focus Areas (continued)

- Compliance expectations surrounding social media include:
  - Policies and procedures that address the review, supervision, retention, and retrieval of information
  - Designate an appropriate individual to approve the use of social media and supervise the activities (CCO or other designate)
  - Reviewing adequacy of system on an ongoing basis

Social Media

Questions When Developing Your Compliance Systems

- Do we wish to allow social media use at our firm?
- Have we developed specific policies and procedures on social media use?
- Do our policies have clear and comprehensive definitions of what forms of social media constitute advertising and marketing?
- Should our policy identify explicit prohibitions on social media use?
- Do policies identify which platforms can be used, by whom and for what purpose?
- Is there an appropriate designated person for supervision and monitoring?
- Have any business risks of using social media been identified and assessed?
- How will we properly train employees on the use of social media?
- Do we have the resources to ensure proper retention and retrieval of social media communications?

Social Media

Industry Guidance

- Below is some guidance you may wish to review
  - CSA Staff Notice 31-325 *Marketing Practices of Portfolio Managers*
    http://www.osc.gov.on.ca/documents/en/Securities-Category3/csa_20110705_31-325_marketing-practices.pdf
  - IIROC Notice 11-0349: *Guidelines for the review, supervision and retention of advertisements, sales literature and correspondence*
    http://www.iiroc.ca/Documents/2011/dbed7d6a-ed1c-4a8b-b3d9-bef60412aa27_en.pdf
  - FINRA Regulatory Notice 10-06: *Social Media Web Sites – Guidance on Blogs and Social Networking Web Sites*
    http://www.finra.org/industry/notices/10-06
  - FINRA Regulatory Notice 11-39: *Guidance on Social Networking Web Sites and Business Communications*
    https://www.finra.org/industry/notices/11-39
  - SEC National Examination Risk Alert: Investment Adviser Use of Social Media
    http://www.sec.gov/about/offices/ocie/riskalert-socialmedia.pdf

Elderly Investors

1. Background - why are we concerned with elderly investors?
2. Regulator approach to elderly clients
3. Practical guidance
4. Reference material

Elderly Investors

1. Concern with elderly investors

- Elderly investors may be considered vulnerable clients
- Vulnerable can be defined in many ways
- Elderly investors may be vulnerable because:
  - May need more investment education/advice
  - How much more attention required depends on individual circumstances
  - Due to some personal attribute or life circumstance

Elderly Investors

2. Regulator approach to elderly clients

- We have detected issues with respect to elderly clients
- Concerned with issues related to seniors because:
  - Growing as a demographic
  - Seniors rely on investments to fund retirement costs
  - Have a reduced investment time horizon to recover from financial losses
  - Possible lack of investment or business knowledge or diminished mental capacity may be exacerbated by their age

Elderly Investors

3. Practical guidance for compliance systems

- Establish effective policies to address senior specific issues
- Begin by assessing whether there is a vulnerability at your firm, and if so, the nature and extent
- Develop "red flags" to help your advisors, dealing representatives and/or compliance staff identify that a client may have diminished capacity or a reduced ability to handle financial decisions
- Compliance process can be assisted by:
  - Speaking with the advisor or dealing representative that is servicing the client
  - Speaking with the client directly

Elderly Investors

3. Practical guidance for compliance systems (continued)

- Examples of potentially vulnerable elderly investors
  - 80 year old widow in good health, who reviews her account statements, talks about current events (including business issues) but frequently asks her advisor the same questions that have been asked and answered before
  - Well educated professional whose spouse recently passed away without prior illness, leaving surviving spouse in depressed state where judgement and ability to reason is clouded
  - 70 year old retired professional who is in excellent health, a life-long *growth* investor who had high employment income and who has a high cost lifestyle but with a modest amount of investment capital and a demand for a very high income from it

Elderly Investors

3. Practical guidance for compliance systems (continued)

- Consider enhanced policies and procedures for dealing with seniors:
  - Establish policies and procedures for dealing with senior specific issues - such as aversion to long-term or speculative strategies
  - Stipulate the requirement for clearer and more detailed communication and documentation of discussions
  - Provide appropriate training to staff to identify potential capacity or vulnerability issues
  - Establish enhanced monitoring and testing of advisors or dealing representatives who have a portfolio concentrated on retirees

Elderly Investors

4. Reference material

- SEC, FINRA, NAASA – *Protecting Senior Investors: Compliance, Supervisory and other Practices used by Financial Services Firms in Serving Senior Investors*
  - Provides an overview of existing practices, including communications, supervision, ensuring compliance, training, escalation procedures, determining appropriate investments, etc.

    http://www.sec.gov/spotlight/seniors/seniorspracticesreport092208.pdf
- Investment Industry Association of Canada – *Compliance, Supervisory and Other Practices When Serving Senior Investors*
  - Best practices for dealing with seniors

    http://iiac.ca/wp-content/uploads/Canadas-Investment-Industry-Protecting-Senior-Investors_March-18-2014.pdf

Elderly Investors

4. Reference material (continued)

- OSC – *Financial Life Stages of Older Canadians*
  - Identifies the top financial concerns of older Canadians and places them in the broader context of retirement concerns including health status

    http://www.osc.gov.on.ca/documents/en/Investors/inv_research_20150601_report-life-stages-older.pdf
- MFDA – *Working to Protect Seniors From Financial Harm*
  - Discussion of some activities the MFDA is undertaking in 2015 to better protect seniors

    http://www.mfda.ca/news/releases15/release-SeniorsMonth.pdf

Cyber Security

1. Background
2. Cyber Security Topics

Cyber Security

Background

- Cyber Security an increasing topic in the media, especially as cyber-attacks are becoming more frequent and widespread
- CSA Staff Notice 11-326 *Cyber Security*
- Financial services industry:
  - Data breaches and theft of personally identifiable information
  - Client funds – advisors with custody are vulnerable potentially from cyber-criminals impersonating a client through email
- High profile cases:
  - JP Morgan
  - Sony Entertainment

Cyber Security

Cyber Security Topics

- The following topics are likely applicable to most firms
  - Compliance Risk Assessments
  - Email
  - Cloud Services
  - Website
  - Anti-Virus Protection
  - Encryption
  - Third Party Vendors

Cyber Security

Compliance Risk Assessments

- Risk assessments are attempts to ensure your firm's compliance system is adequate by identifying risks to your firm and your clients
- Checklist:
  - Inclusion of cyber security
  - What is included in your assessment
  - Risks taken into account
  - Training and expectations of employees

Cyber Security

- **Use of email**
- Use of electronic mail to communicate with clients is growing
- Exercise caution
- Checklist:
  - Email transmission of personal information
  - Authentication practices on all devices (computer and mobile)
  - Authenticate client instructions

Cyber Security

Cloud Services

- Data storage
- Enhance flexibility
- Use Checklist:
  - Due diligence on cloud service providers
  - Segregation of your data
  - Sensitive data storage and encryption
  - Use of mobile devices

Cyber Security

Firm Website

- Websites used as a marketing tool, provide disclosure information to clients, or as a client portal
- Client portal – intended to be secure access points where you can access the firm database directly and can share information
- Use Checklist:
  - Third party for website maintenance - confidentiality of information
  - Encryption of information on client portal
  - Authentication procedures for portal access

Cyber Security

Anti-Virus Protection

- Attempts to detect viruses and other threats
- Regular updates important
- Use Checklist:
  - Regular use anti-virus software on all devices
  - Running of anti-virus updates regularly
  - All software covered
  - Training and education of employees

Cyber Security

Encryption

- Encryption designed to prevent unauthorized exploitation of confidential data, such as in the case of lost or stolen equipment
- Use Checklist:
  - Categorization of data
  - Utilize encryption on all data systems that contain (or access) confidential information
  - Managing identities for authorized users

Cyber Security

Third Party Vendors

- Third party vendors present several risks, including raising the risk of access to your data by serving as another point of access
- Use Checklist:
  - Due diligence on third parties including cyber security as a component
  - Resources of third parties
  - Confidentiality agreements with third party vendors

Questions?

RegistrantOutreach@osc.gov.on.ca

Contact Centre:

inquiries@osc.gov.on.ca

416-593-8314

Or toll free 1-877-785-1555

Resources

Compliance systems

- IOSCO Final Report on Compliance Function at Market Intermediaries

https://www.iosco.org/library/pubdocs/pdf/IOSCOPD214.pdf

- OSC message to UDPs and CCOs on concerns about inadequate compliance systems and CCOs not adequately performing responsibilities

http://www.osc.gov.on.ca/documents/en/Dealers/eb_20120525_recent-communications.pdf

- Section 4.1.2 in OSC Staff Notice 33-742 under the heading *Inadequate compliance systems and UDPs and CCOs not meeting their requirements*

http://www.osc.gov.on.ca/en/SecuritiesLaw_sn_20131107_33-742_annual-rpt-dealers.htm

- Sections 11.1 to 11.3 of 31-103CP

https://www.osc.gov.on.ca/documents/en/Securities-Category3/ni_20150111_31-103_unofficial-consolidated.pdf