Letter

Title	Revised Guideline E-13 – Regulatory Compliance Management (RCM) – Letter (2014)
Category	Sound Business and Financial Practices
Date	November 13, 2014
Sector	Banks Foreign Bank Branches Life Insurance and Fraternal Companies Property and Casualty Companies Trust and Loan Companies

To: All Federally Regulated Financial Institutions (FRFIs)

Guideline E-13 sets out OSFI's expectations for FRFIs with respect to the management of regulatory compliance risk inherent in FRFIs' business activities enterprise-wide. A wide variety of laws and regulations apply to FRFIs in Canada, and for some, outside Canada. OSFI believes that adequate controls over the identification and mitigation of regulatory risk are key to a robust internal control framework.

The revised Guideline replaces the 2003 Guideline E-13 - Legislative Compliance Management to better align it with more recently updated OSFI Guidelines[1] and complement OSFI's >Supervisory Framework and Assessment Criteria. The revised Guideline does not create new regulatory requirements. Rather, it communicates OSFI's key expectations in respect of the need for FRFIs to establish and maintain an enterprise-wide framework of regulatory risk management controls. In developing the revised Guideline, OSFI has taken into account the fact that FRFIs vary in size, scope and complexity. As such, the principles-based nature of the Guideline recognizes that FRFIs will have different RCM practices.

The revised Guideline incorporates several revisions resulting from comments received during the public consultation process, which began in April 2014. The attached table summarizes comments received from industry stakeholders and provides an explanation of how these comments were dealt with. We thank all those who participated in the consultation process.

Implementation of the Guideline by FRFIs is expected by May 1, 2015.

Mark Zelmer

Deputy Superintendent

Annex – Disposition of Public Consultation Comments

Industry Comments	OSFI Response and Disposition
General Comments	
• A statement to the effect that the guideline creates "no new legal requirements…" should be added.	Such a statement is included in the cover letter.
• Foreign branches – Footnote 1 – would be helpful for OSFI to provide guidance on the expectations for foreign branches in view of fact that the reporting structure of some foreign branches is not to the Chief Agent but is instead directly to the foreign Board and therefore the group/parent often retains the responsibility for the mandate, resources and budget for the compliance function.	Outside scope of E-13 therefore not addressed in E-13 – Comments received were dealt with separately.
I. Definitions (i) Regulatory Compliance Management (RCM) – P. 3	
• In second statement, add word "framework" after "RCM" so as to read "An effective RCM **framework** should provide…"	The wording was added.
Definitions (ii) Regulatory Compliance Risk – P. 3	

• In the definition of "regulatory compliance risk", the terms "prescribed practices" and "ethical standards" are very vague and should be clarified. • The term "ethical standards" should be removed from the definition of "regulatory directives" and the terms "prescribed practices" and "ethical standards" should be included as part of the definition in footnote 3. • With respect to "regulatory directives", the term "expectations" is subjective and evolving and should therefore be removed from the definition.	The definition of regulatory compliance risk was revised to indicate that, for the purposes of Guideline E-13, it does not include risk arising from non-conformance with ethical standards. The definition of "regulatory directives" was removed.
Definitions (iii) RCM Framework – P. 3	
No comments provided.	The definition of RCM Framework was moved to the Definitions section as (iii) for consistency.
III. RCM Framework – Overview – P. 3	
• Add words "be risk-based and" to first sentence in second paragraph to read "OSFI expects the RCM framework to **be risk-based and** enable a FRFI…"	To emphasize the risk-based approach, the sentence was changed to read "The RCM framework should enable a FRFI to apply a risk-based approach for identifying, risk-assessing, communicating, managing and mitigating regulatory compliance risk."
• Remove word "all" from third paragraph, first bullet and add the words "employing a risk-based approach" to the end of the first bullet.	The word "all" was removed. Refer also to the above response.
• Where RCM practices may not be fully documented, it is suggested that OSFI take a strong overall control environment and culture of compliance into consideration.	The comment was captured in the risk-based approach that was emphasized throughout the Guideline – refer to text boxes pages 1 and 4 and comment above.

• The scope of the Guideline should be limited to risks that are material to the FRFI. • Add the words “material” or “significant” in the appropriate places in the Guideline to clarify the scope of the Guideline. • The term “material” is not currently defined. Define “material” as “having a significant negative effect on a FRFI’s reputation and/or safety and soundness.”	The risk-based approach, which includes the assessment of risk and identification of material risk, was emphasized throughout the Guideline – refer to text boxes pages 1 and 4 and comment above. “Material” is to be defined by each FRFI in consultation with the Board – refer to footnote 16.	
• With respect to the word “regularly” in the 5th paragraph, the RCM framework is not expected to change much during the year so annual review of it should be adequate to confirm if any revisions are required.	The phrase “at least annually” was added after the word “regularly” for more flexibility. OSFI expects the RCM framework to assess whether new products, business lines, and other changes in business plans carry material regulatory risk; accordingly we do not necessarily agree that the RCM framework may not change much during the year.	
IV. RCM Framework – P. 4		
	This section was re-ordered to include all key controls, including oversight functions, as the basic elements of the RCM framework, and to place more prominence on the role of the CCO by moving it to the beginning of the section.	
(i) Role of the CCO – p. 5		

• In the fourth paragraph, the standard articulated is not achievable and conflicts with the concept of the risk-based approach – suggest it be reworded as follows: "The CCO should be responsible for assessing the adequacy and effectiveness of the FRFI's RCM framework, and for providing an opinion to the Board or a Board Committee whether, based on monitoring and testing performed by the Compliance oversight functions or other oversight functions, the FRFI is in compliance in all material respects with applicable regulatory requirements." • The fourth paragraph seems to require active day to day management by the CCO, rather than supervision and oversight which conflicts with the requirement for the CCO to remain independent from the day to day management of the RCM. • The term "for functional purposes" should be clarified as to whether this means administratively or whether it means direct information reporting and discussion.	The paragraph was moved to the beginning of section and wording was changed to read, "The CCO should be responsible for assessing the adequacy of, adherence to and effectiveness of the FRFI's day-to-day controls, and for providing an opinion to the Board whether, based on the independent monitoring and testing conducted, the RCM controls are sufficiently robust to achieve compliance with the applicable regulatory requirements enterprise-wide.". OSFI considers that "compliance in all material respects" may not adequately address what OSFI means in a particular situation by "compliance". This paragraph was re-ordered and clarified accordingly. Refer to page 3 (RCM Framework Overview and page 5 (Role of the CCO). Refer also to footnotes 6 and 11. The term "for functional purposes" is in the Corporate Governance Guideline in the text box on page 7.	
• Add "employing a risk-based approach" to end of fourth paragraph.	The risk-based approach was clarified by various changes on pages 3 and 5. Refer also the text boxes on pages 1 and 4.	
(ii) Procedures for Identifying, Risk Assessing, Communicating, Managing and Mitigating Regulatory Compliance Risk and Maintaining Knowledge of Applicable Regulatory Requirements – P. 5		
No comments provided.	The word "reasonable" was added to "procedures" and a definition of what is intended here was provided in footnote 9 for clarification.	
(iii) Day-to-Day Compliance Procedures – P. 6		

• FRFIs should have the flexibility to determine not only when and how often to assess their controls but also where and what method of testing and/or monitoring is done and which line of defence testing of compliance procedures should be positioned (otherwise requirements to implement structural changes will create additional costs). • Concept of risk-based approach to monitoring and testing should be explicit in the context of the first line of defence (LOD) like it is stated in the second LOD in (iii).	The risk-based approach was emphasized throughout the Guideline – Refer to text boxes on pages 1 and 4 and comments above. The phrase, "using a risk-based approach" was added.	
• Replace the word "testing" with "assurance", OR add the words "or other appropriate control" after the word "testing" as follows "…Day-to-day compliance procedures should include a monitoring, testing **or other appropriate control**…". (The word "testing" is often connected with audits, implies certain formality and carries certain expectations such as sampling, premise testing, etc. A principles-based approach is preferred because it allows for a variety of methods to determine effectiveness of controls at the first two levels.)	The original language "monitoring and testing" was left in but footnote 13 was added to clarify that independent testing in the second LOD is not intended to duplicate the work of Internal Audit or replace an Internal Audit standard. It was decided not to add the words "or other appropriate control" as this was somewhat vague and potentially confusing.	
• Refer to the three lines of defence model specifically as "the three lines of defense model" throughout the Guideline to provide more clarity and allow clear alignment with the RCM framework frequently used by FRFIs. • Ensure that OSFI has not mandated duplication of controls. • The first LOD should be able to implement compliance controls as appropriate in the circumstances, rather than a new requirement for 'testing'.	Reference to the three lines of defence was added in footnotes 10, 12 and 14. Footnote 13 was added to clarify that independent testing in the second LOD is not intended to duplicate the work of Internal Audit or replace an Internal Audit standard. Language was added to clarify that the day-to-day compliance procedures should include monitoring and testing components using a risk-based approach. Further, risk-based approach was emphasized throughout the Guideline – Refer to text boxes on pages 1 and 4 and comments above.	

(iv) Independent Monitoring and Testing Procedures – P. 6		
• Clarify that 'testing" at the second LOD is risk-based and needed only where deemed required by the Compliance oversight function. • Confirm that the three LODs model is not intended to create duplication, and that monitoring and testing are synonymous and that OSFI does not expect the CCO to perform sample-based testing. • Clarify that the sentence requires the CCO to oversee an enterprise RCM framework with standard methodologies, where appropriate, that would provide an aggregated view of regulatory compliance risk management but which contemplates that this may include inputs and activities from second LOD units not carried out under the CCO's direction. • Extending FRFI's current LCM practices to include formal testing activities will be costly and difficult to implement within the six months timeframe contemplated. • In the third paragraph, clarify that "rotational or other regular basis" does not mean a separate report from IA on the RCM framework and/or other day-to-day compliance activities, but that it means based on the annual internal audit risk-assessment approved by the Board with annual plan and quarterly updates and that resulting reports will satisfy this requirement.	The risk-based approach was emphasized throughout the Guideline – Refer to text boxes pages 1 and 4 and comments above. The issue of potential duplication was addressed in footnote 13. The phrase "monitored and tested" was changed to "overseen by the CCO, using a risk-based approach." The next sentence was revised to address this and clarify as follows: "Where appropriate in the circumstances of the FRFI, independent monitoring and testing, wherever it is conducted within the FRFI, should be sufficiently consistent enterprise-wide to enable the aggregation of information to identify any patterns, themes or trending in compliance controls that may indicate weaknesses." Acknowledged. Not OSFI's intention. Refer to footnote 13. Acknowledged. Not OSFI's intention. The phrase "rotational or other regular basis" is used in a sentence describing validation work, which is in a section titled "(iv) Independent Monitoring and Testing Procedures". Reporting is addressed in a separate section titled "Internal Reporting".	

• More guidance is required with respect to the words “where appropriate” in the context of the first sentence in second paragraph. Alternatively, delete requirement. • More guidance should be provided on how the requirements for independent monitoring and testing may be interpreted based on the size and nature of operations of a FRFI – is it acceptable for monitoring and testing to be performed partly by the same personnel who are implementing and performing RCM?	Clarifications of the risk-based approach emphasized throughout Guideline are intended to provide more guidance.	
• Monitoring and testing should be tied to material risk. • Delete the first sentence in second paragraph “Where appropriate…” FRFIs should have accountability to include monitoring methodology in their frameworks that should ensure appropriate and sufficient oversight to manage regulatory risks, be approved by senior level management, and be reviewed by the Board/Committee. • Confirm that “appropriateness” can be determined by the FRFI	The risk-based approach was emphasized throughout the Guideline – refer to the text boxes on pages 1 and 4 and comments above. “Material” is to be defined by each FRFI in consultation with the Board – refer to footnote 16. The phrase “in the circumstances of the FRFI” was added after the phrase “where appropriate”.	
• Provide more clarity regarding the term “ongoing basis”, as it is broad. • With respect to the first and third paragraphs, use consistent language throughout, i.e. “effectiveness of”, “adherence to” and “reliability of” and provide definitional guidance for how to determine “effectiveness”.	The dictionary definition of “ongoing” includes “continuing”. The risk-based approach was emphasized throughout the Guideline. As such, being more specific was considered to be overly prescriptive. For consistency purposes, the wording was changed to “adequacy of, adherence to and effectiveness of” throughout where these words appeared. The risk-based approach was emphasized throughout Guideline. As such, being more specific regarding effectiveness was considered to be overly prescriptive.	
(v) Internal Reporting – P. 7		

(a) Reporting Procedures – P. 7		
• The term "RCM responsibilities" is very broad and should be limited to reporting to a certain level of management in order to limit the scope of reporting.	The sentence was changed to add "as determined by Senior Management within the FRFI."	
(b) Compliance Reports to Senior Management and the Board – P. 7		
• With respect to the CCO opinion, the guideline should indicate that the opinion can also be based on "or other oversight functions" as referenced in the first paragraph under (iii). • In the case of pertinent information that is "verified or reasonably verifiable", is it verified or reasonably verifiable if it is an attestation from a business unit head that is supported by due diligence?	A sentence was added to say that "The opinion should be supported by sufficient pertinent information that can be reasonably verified." Refer to footnote 6, which also addresses the comment. It can be. However OSFI does not prescribe any particular approach to verification.	
• The CCO opinion should be a negative assurance as it would not be feasible to obtain full certainty over all regulatory requirements. The opinion should be asserted at a point in time and cover a specified period of controls to ensure the statement doesn't extend beyond the intended scope. • The CCO opinion should focus on material regulatory requirements and associated RCM controls (as identified on page 8 "management's identification of material regulatory compliance risk").	The wording was changed to what is intended for the CCO opinion and what it should provide. The risk-based approach was emphasized throughout the Guideline – refer to the text boxes pages 1 and 4 and comments above.	
(c) Internal Audit or Other Independent Review Function Reports to Senior Management and the Board – P. 8		

• With respect to the term "recommendations for correcting deficiencies", audit methodology does not require that reports include "recommendations" but instead that they document management's response to the finding. As such, this requirement should be removed from the Guideline.	The reference to "recommendations" was deleted.	
(vi). Role of Internal Audit or Other Independent Review Function – P. 8		
• The guideline expands the role and requirements of IA or other independent review function. It is too prescriptive as to how IA or other independent review function should fulfil its mandate.	Language was added to clarify that the scope of work should consider the reliability of the RCM framework, which includes management's identification of material regulatory compliance risks and their corresponding controls…".	
• Clarification should be provided with respect to the term "other independent review function". • It should be clarified that the focus of independent review is on whether the RCM process is followed as documented or described, rather than on whether the company is in compliance with the requirements of each piece of legislation or regulation. • The "assessment of how effectively the Compliance oversight function fulfils its responsibilities" lies more appropriately with human resources and is therefore beyond scope of OSFI's intention. The reference should be deleted. • With respect to the frequency of IA reviews of a FRFI's RCM framework, is it appropriate that the frequency is based on the risk associated with that area within the enterprise risk universe.	This function is referenced in the Corporate Governance Guideline. Language was added to indicate that the scope of work should consider the reliability of the RCM framework, which includes management's identification of material regulatory compliance risks and their corresponding controls…". The wording was clarified to read "an assessment of the effectiveness of the compliance oversight". The words were changed to provide for "periodic review by Internal Audit or other independent review function." In addition, the risk-based approach was emphasized throughout the Guideline – refer to text boxes on pages 1 and 4.	
(viii). Role of Senior Management – P. 9		

• This section should be revised to include accountability of Senior Management (SM) for ”material problems or issues”.	This was considered to be addressed by the risk-based approach as emphasized throughout the Guideline.	
• It is preferable to distinguish between role of SM and role of operational management, e.g., the role of SM seems to overlap with role of operational management mentioned earlier in guideline, i.e., “SM should ensure that key results of **day-to-day compliance controls**…”.	This was considered to be addressed in footnotes 4 and 18.	
• When using the term “Senior Management”, it is not clear whether this includes the CCO.	Reference should be made to the Corporate Governance Guideline for a definition of “Senior Management”.	
(ix) Role of the Board - P. 10		
• OSFI should take into consideration the fact that some large financial groups include several financial institutions for which control functions may be organized at a central level independent of the business and that it would not be feasible for the Board of each financial institution member of the financial group to approve the mandate, resources and budget. • The requirement for Board to approve Compliance resources, budgets and to conduct performance reviews of the CCO goes beyond oversight and requires Board to directly manage the Compliance function – this approach erodes Management’s responsibility. These approvals should be conducted by SM with oversight by a Board committee.	Removed reference to the Board’s responsibility to approve the mandate, resources and budget of the CCO as it is referenced in the Corporate Governance Guideline.	
• Similar to the Corporate Governance Guideline, the Guideline E-13 appears to require the Board to actively manage the RCM framework, rather than provide oversight.	The wording in E-13 is consistent with the Corporate Governance Guideline.	

V. OSFI's Supervisory Assessment – P. 10		
• To improve clarity, the sentence should read "Supervision is carried out within a framework that is principles-based and focused on material risk, with the primary goal of safeguarding depositors and policyholders from loss."	The sentence was shortened to read "Supervision is carried out within a framework that is principles-based and focused on material risks."	

1 For example, OSFI's Corporate Governance Guideline published January 2013.