

May 31, 2022

Sent via email to: Culture@osfi-bsif.gc.ca

RE: Letter Dated March 15, 2022 – The Office of the Superintendent of Financial Institutions, Canada (OSFI) on Culture Risk Management

Dear Sir or Madam:

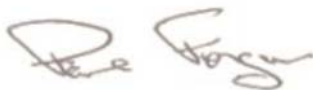
The Institute of Internal Auditors Canada (IIA–Canada) appreciates the opportunity to comment on OSFI's March 2022 letter on **Culture Risk Management**, which seeks comments on the proposed outcomes of an effective culture for inclusion in a culture risk management guideline. As an introduction, The Institute of Internal Auditors (IIA) is an international professional association that serves more than 210,000 members and has awarded 180,000 Certified Internal Auditor (CIA) designations worldwide. The IIA-Canada is affiliated with this global body, serving the needs of more than 7,400 members in Canada. The IIA is recognized as the internal audit profession's leader in standards, certification, education, research, and technical guidance throughout the world.

On behalf of The IIA and IIA-Canada, we are writing to express our support for more formalized OSFI guidelines to be used in managing expectations of culture risk management in federally regulated financial institutions (FRFIs). These guidelines should align with and leverage existing regulatory requirements and oversight bodies to achieve consistent outcomes and avoid duplicative requirements.

OSFI should also consider incorporating culture into an organization's risk management framework, which enhances the depth and breadth of qualitative and quantitative coverage through the Three Lines Model. Clearly defining roles in culture risk management for management's first and second lines, internal audit as third line, and oversight by the governing body assists in confirming the suitability of the established culture within an organization. Internal audit groups are well-positioned to provide independent assessments of contributing factors in determining FRFIs' risk culture health. The proposed guideline and defined outcomes will assist internal audit by providing transparency around the criteria used to assess culture from an objective and unbiased perspective.

Please see the attached Annex A for our comments on specific questions within OSFI's March 2022 letter on **Culture Risk Management**. Should you have any questions regarding the comments provided, please contact me at paul.forgues@theiia.org.

Sincerely,



Paul Forgues
Executive Director
The IIA Canada

Annex A

QUESTION 1

What are your views on OSFI's proposed culture risk management outcomes? Are there other outcomes OSFI should consider?

While we agree on the proposed culture risk management outcomes, we feel further definition of “organizational culture” and “risk culture” would assist in differentiating levels of focus in the application of the outcomes. For example, consider the aim of the compensation assessment. Evaluation of compensation could be assessed according to its promotion and reinforcement of a desired organizational culture, or it could be assessed according to its effectiveness in risk management – or some combination of each.

In addition, corporate strategy should be considered in the assessment of culture risk management outcomes. Corporate strategy achievement should be evaluated due to the effect a questionable culture can have on the tactics employed in accomplishing strategic initiatives.

In determining the appropriateness of risk mindsets and behaviours, OSFI should consider principles that leverage lessons learned in identifying training opportunities. An organization's approach to transparency and openness in communications, inclusive of the application of requirements like training, should also be considered in any assessment.

In addition, the outcomes focus more on criteria fostering a sound organizational culture rather than a healthy risk culture. For example, communicating risk information quickly or deploying a risk appetite to the entire organization does not necessarily guarantee a healthy risk culture. However, support provided by the FRFI of the velocity in addressing risks that exceed an organization's risk appetite expectations would be good outcomes to indicate how well an organization's risk appetite is understood from top to bottom within the organization.

Finally, a greater focus on drivers that foster a healthy risk culture, instead of mindsets and behaviours may be a better approach to assessment. Drivers more appropriately address the root cause of behaviours, are more easily measured and monitored, and can be more effective in determining corrective actions, if required. Key drivers such as organizational structure, three lines, risk supervision, and risk appetite are defined in OSFI corporate governance guidelines as well as the Financial Stability Board's Principles of Sound Compensation Practices. Again, integration with the risk management framework, along with alignment and interaction between these existing structures, would benefit all FRFIs.

As mentioned, assurance functions such as internal audit should contribute as a key component of these oversight activities.

QUESTION 3

Is your organization proactively disclosing culture risk management information as part of its published annual reports? Why or why not? Do you foresee any challenges if OSFI were to expect FRFIs to enhance existing annual reporting requirements to include this information?

Further clarity and guidance concerning OSFI expectations of culture risk management disclosure activities would be beneficial in improving understanding and enhancing planning for future needs. Clarity and guidance will also enable second and third line functions to assess the quality and completeness of culture risk management disclosures.



QUESTION 4

Does a FRFI's size, nature, complexity, risk profile or various sub-cultures (e.g., differences between geographies, business units or functions) give rise to specific culture risk management issues that OSFI should consider?

Yes, we believe this is a critical consideration in culture risk management. Each organization has a unique culture, which can be influenced by its varying degrees of sub-cultures separated internally by business unit or seniority, or geographically by level of globalization or remote employees. As discussed in the OSFI letter, support from middle management is the primary factor in ensuring alignment between the "tone from the top" and the "echo from the bottom" within these sub-cultures. Flexibility in oversight structure of these unique dynamics is important to ensure an organization's cultural health. These activities must be tailored to each organization and assessed according to a risk-based approach, focusing on the higher risk areas of each organization. This approach would also allow for an improved analysis of the alignment between culture and corporate strategy.