OSFI RELEASES FINAL GUIDELINE ON INTEGRITY AND SECURITY

Posted on February 6, 2024

Categories: Insights, Publications

Following a consultation last year, the Office of the Superintendent of Financial Institutions ("**OSFI**") released the final Integrity and Security Guideline (the "**Guideline**") on January 31, 2024.[1] The Guideline sets out OSFI's expectations for federally regulated financial institutions ("**FRFIs**") for adequate policies and procedures to protect against threats to integrity and security, with particular emphasis on technology and foreign interference. The Guideline is designed to work in tandem with other OSFI guidelines, including guidelines for corporate governance, technology and cyber risk management, and operational risk management, among others. FRFIs are expected to regularly assess existing policies and procedures against the expectations set out in the Guideline and the related guidelines to identify gaps and maintain effectiveness.

The Guideline identifies integrity and security as two distinct but related concepts, and provides details on OSFI's expectations for both.

Integrity

OSFI defines integrity as "actions, behaviours, and decisions that are consistent with the letter and intent of regulatory expectations, laws, and codes of conduct."[2] The Guideline focuses on four ways of promoting integrity within the FRFI:

1. Ensuring that those in senior positions possess good character, and demonstrate integrity through their actions, behaviours, and decisions. Reference is made to Guideline E-17 Background Checks on Directors and Senior Management ("**E-17**").
2. Fostering norms that encourage ethical behaviour, which includes valuing compliance, honesty, and responsibility. Reference is made to OSFI's draft Culture and Behaviour Risk Guideline.
3. Ensuring sound governance to oversee important decisions of the FRFI, including business plans, strategies, risk appetite, culture, internal controls, oversight of senior management, and accountability mechanisms. The Guideline specifically notes the importance of compliance with the law, avoiding conflicts of interest, maintaining objectivity, ensuring security of assets and information, and the necessity of regular assessments. Reference is made to OSFI's Corporate Governance Guideline.
4. Establishing an effective Regulatory Compliance Management framework. Reference is made to Guideline E-13 on Regulatory Compliance Management.

Security

OSFI broadly identifies security as "protection against malicious or unintentional external or internal threats to real property, infrastructure, and personnel (physical threats), and technology assets (electronic threats)."[3] The Guideline focuses on six areas of interest:

1. Physical premises should be safe, secure, and monitored appropriately. Further details can be found in Guideline B-13 Technology and Cyber Risk Management ("**B-13**") and draft Guideline E-21 Operational Resilience and Operational Risk Management ("**E-21**").
2. Appropriate background checks should be conducted based on the risk factor of the employee or contractor, which should include education/professional credentials and references at a minimum. See also Guideline E-17.
3. Technology assets should be secured appropriately as outlined in Guideline B-13.
4. Standards of control for data and information should be established, including the creation of data classification that considers the FRFI's vulnerability to malicious activity, undue influence, and foreign interference. Reference is made to Guidelines E-21 and B-13.
5. Risks posed by third parties must be assessed and identified based on their access to the FRFI's physical premises, people, technology assets, and data and information. The assessment should be conducted both before engagement and on an ongoing basis. Further details can be found in Guideline B-10 Third-Party Risk Management.
6. When an FRFI identifies threats of suspected undue influence, foreign interference, or malicious activity, it should report to the appropriate authorities such as the RCMP and CSIS. Notification must also be provided to OSFI immediately. FRFIs should also document incidents that do not meet the reporting threshold.

Timeline

Implementation of the Guideline will occur in phases:

- Currently: Notify OSFI when reporting incidents to law enforcement or CSIS.
- By July 31, 2024: Submit a comprehensive action plan detailing how the FRFI will meet the new and expanded expectations for OSFI's review.
- By January 31, 2025: Observe all new and expanded expectations, except for background checks.
- By July 31, 2025: Observe new expectations on background checks.[4]

Takeaways

The Guideline integrates existing and draft OSFI guidelines to further enhance public confidence in the

Canadian financial system. The emphasis on technology and foreign interference recognizes the new landscape that FRFIs operate in.

Once the Guideline is implemented, FRFI's will need to have processes in place for conducting regular assessments of existing measures to ensure that the integrity and security of the FRFI is consistently maintained.

If you have any questions about the Guideline and next steps, please do not hesitate to contact us.

[1] OSFI releases final Integrity and Security Guideline
[2] Integrity and Security - Guideline
[3] Integrity and Security - Guideline
[4] Integrity and Security - Letter

By Darcy Ammerman and ZiJian Yang (Articling Student)

A Cautionary Note