NEW OSFI GUIDELINE ON OPERATIONAL RISK MANAGEMENT

Posted on September 9, 2015

Categories: Insights, Publications

In August 2015 the Office of the Superintendent of Financial Institutions Canada ("**OSFI**") released its draft Guideline E-21 entitled Operational Risk Management (the "**Guideline**") for federally-regulated financial institutions ("**FRFIs**"). It applies to all FRFIs, including insurance companies but, similar to OSFI's comprehensive *Corporate Governance* Guideline finalized in January, 2013, FRFIs under the Guideline do not include branch operations of foreign banks and foreign insurance companies.

The Guideline identifies the appropriate framework and processes OSFI expects FRFIs to maintain in order to mitigate operational risk. Through the Guideline, OSFI hopes to promote industry best practices consistently across all FRFI's. The Guideline is OSFI's first direct statement on operational risk management ("**ORM**"), complementing its comprehensive list of corporate governance requirements contained in the Corporate Governance Guideline. The Guideline is open for public comment until October 9th, 2015.

According to the Guideline, operational risk is the risk of loss resulting from people, inadequate or failed internal processes and systems, or external events. Operational risk includes non-adherence to internal procedures, legal risk, fraud or unethical behaviour more broadly, but excludes strategic and reputational risk.

The Guideline is organised around the recognition of four principles:

1. ORM is integrated within the FRFI's overall risk management framework and appropriately documented;
2. ORM supports the FRFI's overall corporate governance structure and includes an operational risk appetite statement;
3. a robust accountability structure, such as the "three lines of defence" approach separates the components of ORM and provides for independent review and challenge; and
4. through appropriate ORM tools, FRFIs identify and assess their operational risk and are able to collect operational risk information for communication both internally and to supervisory authorities.

ORM Framework

OSFI expects every FRFI to have a robust framework with mechanisms in place to identify and manage operational risk as a fundamental element of the FRFI's risk management program. Depending on the nature, size, complexity and risk profile of the FRFI, the ORM framework should:

- describe the FRFI's approach to ORM and reference the relevant policies and procedures;
- embody a model that includes a structured independent peer review process (see also the "three lines of defense" model described below);
- articulate clear accountability and ownership for ORM among the "three lines of defense";
- identify risk assessment and reporting tools and their effective use;
- describe the FRFI's approach to establishing and monitoring operational risk appetite and related limits of exposure;
- address the governance structures in place to manage operational risk, including reporting lines and accountabilities (including ensuring that ORM has sufficient status within the FRFI to be effective);
- ensure independence of key functions as part of an effective control environment;
- apply to the FRFI on an enterprise-wide basis;
- require that the FRFI's relevant policies be reviewed and revised regularly to take into account material changes (all to be subject to board and senior management oversight); and
- be able to produce documentation, including risk management value, suitable for the intended audience.

Operational Risk Appetite Statement and Corporate Governance

The operational risk appetite statement developed by FRFIs should be a component of the FRFI's enterprise-wide, board-approved risk appetite framework mandated by OSFI's *Corporate Governance* Guideline. It should set out the nature, types and approximate exposure levels of operational risk that the FRFI is willing or expected to assume. It should include limits/thresholds for acceptable levels of operational risk which, if exceeded, give rise to escalation to management or the board for necessary action. The FRFI's board and management should regularly review the operational risk appetite to confirm continuing appropriateness. The ORM governance structure, including in particular, the roles of the board and senior management, should be aligned with the FRFI's overall corporate governance framework. The Guideline goes on to enumerate a number of management responsibilities for ensuring proper establishment, implementation, maintenance and oversight of the ORM and coordination of operational risks with credit, market and other risks of the FRFI.

The Three Lines of Defence Model

OSFI recognizes that a FRFI's use of any particular ORM methodology will depend on its business model and risk profile. However, OSFI recommends that the ORM framework be organized in accordance with the "three lines of defence" model in an effort to achieve accountability. According to OSFI, this particular model provides a structured independent peer review process with clear accountability at each level. Each of the three lines is responsible for implementing its respective risk management procedures to monitor and report on

operational risk.

First Line

The first line of defence, referred to as the business line, encompasses responsibility for planning, directing and controlling day-to-day operations of significant activities, and identifying and managing inherent operational risks in products, activities, processes and systems. The first line is responsible for adherence to the ORM framework, identifying and assessing operational risk; establishing and assessing mitigating controls; monitoring and reporting; reporting on unmitigated residual risk; promoting a risk management culture; and ensuring appropriate escalation of material issues.

Second Line

The second line of defence is comprised of oversight activities designed to independently identify, measure, monitor and report operational risk on an enterprise basis. The second line designs and implements the FRFI's ORM framework. It may include personnel from other FRFI functions (such as compliance and legal).

The second line effectively acts as an independent challenger to the first line's adherence to operational risk policies, and ensures that the appropriate risk management tools are put into action. Second line reviews should be made by competent staff in a structured and timely process that can be communicated to the first line in a manner that encourages continuous improvement. The Guideline emphasizes that this role is not facilitation, guidance or documentation of decisions.

Third Line

The third line of defence is generally seen to be the internal audit function (independent of both the first and second lines). It reviews the effectiveness of the first and second lines' practices from the perspective of the FRFI's overall ORM and corporate governance functions. While the third line performs much the same kind of review the second line does, it also evaluates the nature and scope of the FRFI's overall ORM framework in the context of the FRFI's size, complexity and risk profile.

As an alternative to internal audit, the third line's reviews may be performed by properly qualified external experts. Regardless, these individuals should not be involved in the development or operation of the framework; rather, their role is purely audit-focused. It is the third line's responsibility to ensure recommendations for improvements are appropriately escalated to the FRFI's management, and that an adequate and timely response is returned to address the relevant operational risks.

Identification and Assessment of Operational Risk

OSFI recognizes that each individual FRFI is in the best position to determine which tools are the most

appropriate to identify and assess the FRFI's operational risk, given the FRFI's nature, size, complexity and risk profile. The Guideline provides a description of the following important ORM tools that may be used to help the FRFI achieve a robust level of ORM:

- operational risk "taxonomy";
- risk and control assessments;
- change management risk and control assessments;
- internal operational risk event collection and analysis;
- external operational risk event collection and analysis;
- risk and performance indicators;
- business process mapping;
- scenario analysis and stress testing;
- quantification/estimation of operational risk (as
- required by other OSFI guidance); and
- comparative analysis.

Conclusion

It is OSFI's objective and in the interest of every FRFI to minimize operational risk exposure as much as possible. To achieve an effective ORM environment, the Guideline promotes four principles: integration of ORM within the FRFI's enterprise wide risk management program, the maintenance of an overall risk appetite statement for operational risk, a model of independent review and adoption of appropriate risk management tools.

According to OSFI, FRFIs have made significant improvements to their ORM practices in the last several years. Although this is OSFI's first directive on the subject, the Guideline aligns with supervisory expectations already in place across most FRFIs. As a result, the Guideline's implementation costs within the financial services industry are expected to be low. Assuming the Guideline will ultimately be issued, OSFI expects all FRFIs to fully implement the Guideline within a year of its effective date.

by Carol Lyons and Jeremy Rankin

A Cautionary Note


mcmillan