Office of the Superintendent of Financial Institutions Canada
Bureau du surintendant des institutions financières Canada

Guideline

Subject: Operational Risk Management

Category: Sound Business and Financial Practices

No: E-21 **Date: June 2016**

1. Purpose and Scope of the Guideline

This Guideline sets out OSFI's expectations for the management of operational risk and is applicable to all federally regulated financial institutions (FRFIs).

OSFI recognizes that FRFIs may have different operational risk management practices depending on their: size; ownership structure; nature, scope and complexity of operations; corporate strategy and risk profile.

For the purposes of this Guideline, operational risk is defined as the risk of loss resulting from people, inadequate or failed internal processes and systems, or from external events. This includes legal risk but excludes strategic and reputational risk. The risk of loss resulting from people includes, for example, operational risk events relating specifically to internal or external fraud, non-adherence to internal procedures/values/objectives, or unethical behaviour more broadly. Risk exposure relating to external events and that stems from coverage sold by insurers to third parties is excluded, while risk on an insurer's own operations is considered within scope.

OSFI recognises that within industry practice, external fraud may be currently categorised within business risk (rather than separately within operational risk). OSFI encourages institutions to consider including external fraud events in the definition of operational risk for risk management purposes.

Table of Contents

2. Operational Risk Management Framework

Principle 1:

Operational risk management should be fully integrated within a FRFI's overall risk management program and appropriately documented.

Operational risk is inherent in all products, activities, processes and systems. As such, the effective management of operational risk should be a fundamental element of a FRFI's risk management program. OSFI expects FRFIs to have a framework for operational risk management that sets forth mechanisms for identifying and managing operational risk[1].

Understanding operational risks leads to better decision making through the observation and analysis of past operational risk events and the patterns of observed behaviour within the FRFI. In addition, a robust framework for operational risk management provides a mechanism for discussion and effective escalation of issues leading to better risk management over time and increased institutional resilience. The comprehensive data collection which the framework supports allows for analysis of complex corporate-wide issues and facilitates tailored risk mitigation actions. Additional tools such as analysis of external events and scenario analysis can provide risk management value and discourage complacency in operational risk management.

3. Operational Risk Appetite Statement

Principle 2:

Operational risk management should serve to support the overall corporate governance structure of the FRFI. As part of this, FRFIs should develop and utilise an operational risk appetite statement, or in the case of small, less complex FRFIs with lower operational risk profiles, use of reporting/escalation thresholds for material operational risk events.

Larger, more complex FRFIs with significant levels of operational risk in their activities should develop and maintain a comprehensive risk appetite statement for operational risks, as part of the FRFI's overall Risk Appetite Framework (see OSFI's *Corporate Governance* Guideline including its Annex B). The risk appetite statement for operational risk should articulate the nature and types of operational risk that the FRFI is willing or expected to assume. The operational risk appetite statement should be succinct, clear, and include a measurable component (limits/thresholds). The purpose of having a measurable component is to indicate the level of operational risk that is considered acceptable within the FRFI. The limits/thresholds may also serve to indicate the level at which operational risk events, near misses, or cumulative patterns, are considered necessary for escalation to Senior Management (in some cases, separate reporting thresholds may be established).

[1] See Annex 1 item 1 for elements of operational risk frameworks which may be considered best practice for larger, more complex FRFIs, depending on their individual risk profile. As FRFIs evolve, in terms of size or other relevant factors, supervisory expectations may increase in this area.

In formulating their risk appetite statement for operational risk, FRFIs may consider elements such as: changes in the external environment; material increases/decreases in business or activity volumes; the quality of the control environment; the effectiveness of risk management or mitigation strategies; the FRFI's operational risk event experience; and the frequency, volume or nature of risk appetite limit/threshold breaches.

The operational risk appetite statement, and/or the reporting threshold for material operational risk events should be regularly reviewed to ensure it remains appropriate. Escalation and reporting processes for breaches, or potential breaches, should be in place.

4. Three Lines of Defence

Principle 3:

FRFIs should ensure effective accountability for operational risk management. A "three lines of defence" approach, or appropriately robust structure, should serve to delineate the key practices of operational risk management and provide adequate objective overview and challenge. How this is operationalized in practice in terms of the organisational structure of a FRFI will depend on its business model and risk profile.

Appropriate accountability for the management of operational risk is essential. A "three lines of defence" structure is one way to achieve such accountability. For illustrative purposes, the roles and responsibilities of each of the three lines are described below. In determining what is considered an appropriately robust structure, both FRFIs and OSFI will consider size, ownership structure, nature, scope and complexity of operations, corporate strategy and risk profile.

First Line of Defence

The business line – the first line of defence – has ownership of risk whereby it acknowledges and manages the operational risk that it incurs in conducting its activities. The first line of defence is responsible for planning, directing and controlling the day-to-day operations of a significant activity/enterprise-wide process and for identifying and managing the inherent operational risks in products, activities, processes and systems for which it is accountable[2].

Second Line of Defence

The second line of defence are the oversight activities that objectively identify, measure, monitor and report operational risk on an enterprise basis. They represent a collection of operational risk management activities and processes, including the design and implementation of the FRFI's framework for operational risk management. The second line of defence[3] is best placed to

[2] See Annex 1 item 2 for first line of defence responsibilities which may be considered best practice for larger, more complex FRFIs, depending on their individual risk profile.

[3] See Annex 1 item 3 for second line of defence responsibilities which may be considered best practice for larger, more complex FRFIs, depending on their individual risk profile.

provide specialized reviews related to the FRFI's operational risk management. In addition, it should be noted that other staff/corporate areas of the FRFI (e.g. compliance) may also be deemed part of the second line of defence.

A key function required of the second line of defence is to provide an objective assessment[4] of the business lines' inputs to and outputs from the FRFI's risk management (including risk measurement/estimation), and to establish reporting tools to provide reasonable assurance that they are adequately complete and well-informed.

Third Line of Defence

The internal audit function is charged with the third line of defence. The third line of defence should be separate from both the first and second lines of defence, and provide an objective review and testing of the FRFI's operational risk management controls, processes, systems and of the effectiveness of the first and second line of defence functions. The third line of defence is best placed to observe and review operational risk management more generally within the context of the FRFI's overall risk management and corporate governance functions. Objective review[5] and testing coverage should be sufficient in scope to verify that the operational risk management framework has been implemented as intended and is functioning effectively.

5. Identification and Assessment of Operational Risk

Principle 4:

FRFIs should ensure comprehensive identification and assessment of operational risk through the use of appropriate management tools. Maintaining a suite of operational risk management tools provides a mechanism for collecting and communicating relevant operational risk information, both within the FRFI, and to relevant supervisory authorities.

OSFI recognises that the FRFI itself has the best perspective to determine its organizational structure, processes, and the extent of its use of tools[6] to achieve a robust level of operational risk management. FRFIs are encouraged to continue to develop and improve the tools they use to manage their operational risk and to monitor and adopt best practices in this area, as appropriate (including prioritising enterprise wide[7] coverage). The specific tools used to identify and assess/analyse operational risk will depend on a range of relevant factors, particularly the nature (including business model), size, complexity and risk profile of the FRFI.

[4] See Annex 1 item 4 for further elaboration on providing effective objective assessment.

[5] See Annex 1 item 5 for third line of defense responsibilities that may be considered best practice for larger, more complex FRFIs, depending on their individual risk profile.

[6] See Annex 1 item 6 for descriptions of operational risk management tools that may be considered best practice for larger, more complex FRFIs, depending on their individual risk profile.

[7] Enterprise-wide means throughout all business activities applicable to the FRFI and its subsidiaries world-wide.

The objective of the use of operational risk management tools is to generate risk management value proportionate to the other risks faced by the individual institution. OSFI recognises that the use of well implemented tools adds greater risk management value, and that FRFIs may have existing tools in place to collect and analyse information relevant for operational risk management. See Annex 1 item 6 for further best practices related to operational risk management tools. All tools may apply; however, the descriptions included should not be interpreted as a checklist to be used for compliance or audit purposes.

Annex 1 – Emerging Practices

The following sound practices are primarily for consideration by larger, more complex FRFIs. However, some of the practices are more widely applicable and may be helpful as concrete examples of industry practice.

The examples of emerging practices below are not exhaustive and do not represent a checklist or an end-point for supervisory or internal audit review. Discussions in these areas should focus on improvements in operational risk management, rather than focusing on compliance.

An operational risk management framework can provide a unique mechanism for specific data requests by senior management leading to more comprehensive information gathering relating to complex organisational issues. For example, if senior members of a FRFI are observing a particular type of operational risk event in one area of the organisation, it can be useful to collect information on whether similar events or patterns are occurring in other areas (i.e. there are indications of broader corporate-wide issues).

Decision making at the highest levels of an organisation benefits from more complete information. Operational risk management frameworks are designed to permit the collection of information in specific areas across business lines on an enterprise wide basis. This can be particularly useful in areas such as external fraud across product lines, legal losses across the organisation, or system breaches/inadequacies (whether indicative of isolated instances of rogue behaviour or wider systemic problems). In larger organisations with well-established second lines of defence, the information collection and aggregation capabilities of these professional groups can lead to better problem identification and thus more comprehensive and longer-term solutions to corporate-wide organisational issues.

1. Within FRFIs, the documented framework for operational risk management may consider the following elements:
   a) A description of the FRFI's approach to managing operational risk, including reference to the relevant operational risk management policies and procedures;
   b) Clear accountability and ownership for operational risk management amongst the three lines of defence;
   c) The risk assessment and reporting tools used by the FRFI and how they are used within the institution;
   d) The FRFI's approach to establishing and monitoring risk appetite and related limits for operational risk;
   e) The governance structures used to manage operational risk, including reporting lines and accountabilities. This includes ensuring that operational risk management has sufficient status within the organisation to be effective;
   f) Application to the FRFI enterprise-wide;
   g) Requirements for relevant policies to be reviewed on a regular basis, and revised as appropriate;

h) Efficient corresponding documentation, which should provide commensurate risk management value and be suitable for the intended user/audience

2. Within FRFIs, the first line of defense may be responsible for developing capabilities in the following areas:

   a) adherence to the operational risk management framework and related policies;

   b) identification and assessment of the inherent operational risk within their respective business unit and assessing the materiality of risks to the respective business units;

   c) establishment of appropriate mitigating controls and assessing the design and effectiveness of these controls;

   d) oversight of and reports on the business lines' operational risk profiles and supporting operation within established operational risk appetite statement[8];

   e) analysis and reportage of the residual operational risk that is not mitigated by controls, including operational risk events, control deficiencies, human resources, process, and system inadequacies[9];

   f) promotion of a strong operational risk management culture throughout the first line of defence;

   g) confirmation of timely and accurate escalation, within the FRFI, of material issues;

   h) staff training in their roles in operational risk management if required.

Depending on the size and complexity of the financial institutions, the first line of defense may be further divided between '1a' and '1b[10]' roles.

3. OSFI recognizes that the nature, size, complexity and risk profile of different FRFIs will mean that the responsibilities of the second line of defence groups may overlap with those of the first line of defence. Further, the size and degree of independence of the second line of defence will differ among FRFIs. For example, for small FRFIs with low operational risk exposures, objective overview may be achieved through separation of duties. In larger FRFIs, however, the second line of defence will generally consist of a separate function most often

8 The second line of defence may also contribute to this role; particularly with respect to aggregating information on an enterprise wide basis.

9 The second line of defence may also contribute to this role; particularly with respect to aggregating information on an enterprise wide basis.

10 1b – the business may choose to establish control groups that may have specific accountability for activities specific to operational risk, including:

- Identifying, measuring, managing, monitoring and reporting operational risk arising from operating activities and initiatives in line with corporate standards
- Establishing an appropriate internal control structure to manage the operational risks in their specific area
- Escalate, in a timely manner, operational risks to senior management or risk management
- Develop and implement, in a timely manner, corrective actions for operational risk issues that have been identified.

reporting into the risk management function. The second line of defence should have an appropriate level of sufficiently skilled resources and stature to effectively fulfill its responsibilities.

Within FRFI's, examples of responsibilities commonly associated with the second line of defence include:

a) providing effective objective assessment, which should be evidenced and documented where material (e.g. by providing examples of the challenges and outcomes) so as to be subsequently observable to the first line of defence;

b) confirming continued development of appropriate strategies to identify, assess, measure, monitor and control/mitigate operational risk;

c) confirming continued establishment and documentation of appropriate FRFI-wide policies and procedures relating to the FRFI's operational risk management framework;

d) confirming continued development, implementation and use of appropriate enterprise – wide operational risk management tools;

e) confirming adequate processes and procedures exist to provide appropriate oversight of the FRFI's operational risk management practices;

f) confirming that operational risk measurement processes are appropriately integrated into the overall risk management of the FRFI;

g) reviewing and contributing, to the monitoring and reporting of the FRFI's operational risk profile (this may also include aggregating and reporting);

h) promoting a strong operational risk management culture throughout the enterprise; and

i) confirming timely and accurate escalation, within the FRFI, of material issues.

Similar to the first line, the second line of defence may also be further divided between '2a' and '2b[11]' roles.

4. Objective Assessment is the process of developing an objective view regarding the quality and sufficiency of the business unit's operational risk management activities, including the identification and assessment of operational risks; identification and assessment of controls; assumptions; and risk decision (e.g., acceptance, transfer, denial, action plan). This includes providing challenge when appropriate.

Objective Assessment is:

- based on a structured and repeatable process that accommodates continuous improvement (while allowing for ad-hoc flexibility where appropriate);

[11] 2b – the second line of defence may choose to establish a quality assurance program that challenges the quality and nature of the effective challenge provided by the second line of defence (2a).

- applied through the various operational risk management tools, reporting and other governance processes;
- performed by knowledgeable and competent staff;
- shared with the business in a constructive manner;
- performed on a timely basis;
- measured by outcomes (e.g., it has influenced a management decision/action);
- evidenced/documented.

Evidence of observable challenge may include both evidence of challenge integral to a process or evidence of challenge with supporting documentation at various stages of the process, as appropriate. Consistent with other areas of operational risk management, and risk management more generally, the level of documentation required should add risk management value and not be unduly distracting from overall risk management goals.

Objective Assessment is more than facilitation, guidance, or documentation of decisions.

5. Within FRFI's third line of defense for operational risk: objective review and testing activities generally involve testing for compliance with established policies and procedures, as well as evaluating whether the framework for operational risk management is appropriate given the size, complexity and risk profile. Objective review and testing generally consider the design and use of operational risk management tools in both the first and second lines of defence, the appropriateness of objective assessment applied by the second line of defence, and the monitoring, reporting and governance processes.

6. The following are examples of operational risk management tools that have been used within FRFIs and may be useful:
   a) Operational risk taxonomy;
   b) Risk and control assessments (RCAs);
   c) Change management risk and control assessments;
   d) Internal operational risk event collection and analysis;
   e) External operational risk event collection and analysis;
   f) Risk and performance indicators;
   g) Material business process mapping;
   h) Scenario analysis;
   i) Quantification/estimation of operational risk exposure
   j) Comparative analysis

Each risk management tool is described in more detail below.

(a) Operational Risk Taxonomy

A common taxonomy of sources of operational risk types aids with consistency of risk identification and assessment activities, and articulation of the nature and type of operational risk to which the FRFI is potentially exposed. An inconsistent taxonomy of operational risk terms may increase the likelihood of not properly identifying, categorizing, and allocating responsibility for the assessment, monitoring, and mitigation of risks.

(b) Risk and Control Assessments (RCAs)

Risk and control assessments are one of the primary tools typically used to assess inherent operational risks and the design and effectiveness of mitigating controls within FRFIs. RCAs provide value through:

- including an assessment of business environment, inherent risks, controls, and residual risks, referencing the FRFI's operational risk taxonomy;
- encouraging proper alignment between the risk and its mitigating controls;
- being completed on a periodic basis (to support accurate and timely information); and
- having appropriate supporting activities and frequency of maintenance to remain current and relevant in the management of operational risk

RCAs generally are completed by the first line of defence across the enterprise, including the various control groups, and should reflect the current environment but also be forward-looking in nature. Resulting action plans emerging from completion of an RCA should be tracked and monitored to facilitate required enhancements being appropriately implemented. In addition, the second line of defence should review and provide objective challenge to the risk and control assessments, and the resulting action plans of the first line of defence.

(c) Change Management Risk and Control Assessments

Change management risk and control assessments establish a formalized process for assessing inherent operational risk and the appropriateness of mitigating controls when the FRFI undertakes significant changes. The operational risk assessments made as part of the change management process should generally be performed by the first line of defence. This risk assessment process may consider:

- inherent risks in the new product, service, or activity;
- changes to the FRFI's operational risk profile and risk appetite;
- the required set of controls, risk management processes, and risk mitigation strategies to be implemented;
- the residual risk (unmitigated risk); and
- changes to the relevant risk limit/threshold.

(d) Internal Operational Risk Event Collection and Analysis

Robust internal operational risk event collection and analysis includes having systems and processes in place that capture and analyse material internal operational risk events (e.g. those that exceed an appropriate internal threshold). An operational risk event, which is defined as an unintended outcome resulting from operational risk, includes actual and potential operational losses and gains, as well as near misses (i.e. where the FRFI did not experience an explicit loss or gain resulting from an operational risk event).

Internal operational risk event collection and analysis provides meaningful information for assessing 1) a FRFI's exposure to operational risk through aggregating and monitoring operational risk events over time, and 2) the overall effectiveness of the operational controls environment. The capture of internal operational risk data should primarily be managed by the first line of defence and appropriate controls (i.e. segregation of duties, verification) should be in place for maintaining data integrity at an acceptable level.

For operational risk events determined to be material, FRFIs are expected to identify the root cause as well as any required remedial action so similar events in the future either do not occur or are appropriately mitigated. Established reporting and analysis standards should also address minimum expectations over event analysis, including:

- whether the exposure is an actual, potential or near miss event;
- the underlying operational risk category exposure as defined within the risk taxonomy;
- deficiencies and control failures that can be mitigated;
- the corrective actions to be taken to address the deficiencies and control failures; and
- appropriate sign-offs and approvals

For material operational risk events, appropriate root cause analysis is generally conducted by the first line of defence and appropriately escalated based on the potential or observed impact of the event. The second line of defence reviews and applies objective challenge to the analysis conducted by the first line of defence.

(e) External Operational Risk Event Collection and Analysis

External operational risk events are operational risk related events occurring at organisations other than the FRFI itself. External operational risk event collection and analysis activities may include subscribing to an external loss reporting database, monitoring the FRFI's own operational risk event experience over time relative to its peers, assessing overall exposures, and the overall effectiveness of the operational controls environment.

(f) Risk and Performance Indicators

Risk and performance indicators are risk metrics used to monitor the main drivers of exposure associated with key operational risks which also can provide insight into control weaknesses and help to determine a FRFI's residual risk. Risk and performance indicators, paired with escalation and monitoring triggers, act to identify risk trends, warn when risk levels approach or exceed thresholds or limits, and prompt actions and mitigation plans to be undertaken. These risk metrics could contain internal and external or environmental indicators relevant to decision making.

(g) Material Business Process Mapping

Business process mapping is a common tool used to identify and manage operational risks for significant or enterprise-wide processes. Business process mapping involves identifying the steps within the process, and assessing the inherent operational risks, risk interdependencies, and the effectiveness of controls, as well as subsequent management actions required when control weaknesses are identified.

(h) Scenario Analysis

Scenario analysis is a process of identifying potential operational risk events and assessing their potential outcome and impact on the FRFI. Scenario analysis can be an effective tool to consider potential sources of operational risk and the need for enhanced risk management controls or mitigation solutions. In order to effectively use scenario analysis as part of a risk management program, operational risk scenarios developed should consider both expected and unexpected organisational response relative to an operational risk event or event type. If scenario analysis is used as an input into the quantification/estimation of operational risk exposure, the second line of defence review whether the scenarios chosen are appropriate and consistent with the FRFI's scenario analysis program.

(i) Quantification/Estimation of Operational Risk Exposure

Quantification/estimation of exposure to operational risk is discussed through existing Internal Capital Adequacy Assessment Process (ICAAP[12]) or Own Risk Solvency Assessment (ORSA[13]) exercises. Quantification/estimates may be compared to the required capital for operational risk under the relevant capital adequacy/minimum required capital guideline for additional value. Regardless of the operational risk quantification approach taken, key assumptions should be documented, and appropriate validation, vetting and verification activities should be performed.

(j) Comparative Analysis

Comparative analysis involves the first line of defence reviewing the risk assessments and outputs of each of the operational risk management tools, to confirm the overall assessment of operational risk. Comparative analysis can help to facilitate risk assessments being performed in a consistent manner and that lessons learned are appropriately shared within the organization. Comparative analysis can also identify areas where greater consistency within tools used, on an enterprise-wide basis, may generate risk management value through supporting more consistent

[12] See OSFI ICAAP Guideline E-19.

[13] See OSFI ORSA Guideline E-19.

information collection, aggregation, and resulting analysis. Comparative analysis can also help identify operational risk management tools that may not be effective or well implemented.

Annex 2 – List of Related Guidance

Referenced directly within the guideline:

Corporate Governance Guideline

Include or reference capital requirements for operational risk:

Guideline A Capital Adequacy Requirements

Guideline A Minimum Continuing Capital and Surplus Requirements

Guideline A Minimum Capital Test

Guideline E-19 Own Risk and Solvency Assessment (ORSA)

Guideline E-19 Internal Capital Adequacy Assessment Process (ICAAP)

Relevant for operational risk scenario analysis:

Guideline E-18 Stress Testing

Include specific guidance relating to FRFI processes:

Cyber Security Self-Assessment Guidance

Guideline B-7 Derivatives Sound Practices

Guideline B-8 Deterring & Detecting Money Laundering and Terrorist Financing

Guideline B-10 Outsourcing of Business Activities, Functions and Processes

Guideline B-20 Residential Mortgage Underwriting Practices and Procedures

Guideline B-21 Residential Mortgage Insurance Underwriting Practice and Procedures

Guideline E-4A Role of the Canadian Chief Agent & Record Keeping Requirements

Guideline E-4B Role of the Principal Officer and Record Keeping Requirements

Guideline E-5 Retention/Destruction of Records

Guideline E-13 Regulatory Compliance Management (RCM)

Guideline E-20 CDOR Benchmark-Setting Submissions