Supervisory Framework

1999

and

beyond

Office of the Superintendent
of Financial Institutions

OSFI's Mission

We are the primary regulator of federal financial institutions and pension plans. Our mission is to safeguard policyholders, depositors and pension plan members from undue loss. We advance and administer a regulatory framework that contributes to public confidence in a competitive financial system. We also provide actuarial services and advice to the Government of Canada.

We are committed to providing a professional, high quality and cost-effective service.

Office of the Superintendent of Financial Institutions Canada
255 Albert Street, Ottawa, Ontario K1A 0H2 www.osfi-bsif.gc.ca

Table of Contents

1. Introduction

OSFI's activities can be divided into two broad functions: regulation and supervision. Regulation involves providing input into developing and interpreting legislation and regulations, issuing guidelines, and approving requests from federally regulated financial institutions as required under the various financial institution legislation. Supervision involves assessing the safety and soundness of federally regulated financial institutions, providing feedback to institutions, and using supervisory powers to intervene in a timely manner to achieve OSFI's mandate.

The objective of the Supervisory Framework (Framework) is to provide an effective process to assess the safety and soundness of regulated financial institutions. This is achieved by evaluating an institution's risk profile, financial condition, risk management processes, and compliance with applicable laws and regulations.

Developing supervisory practices is a dynamic process. Continuing change in the financial markets has led OSFI to review its existing supervisory practices to ensure that they remain effective. The review was carried out over a two-year period commencing in 1997. In recognition of the increased globalization of the financial industry and the need for harmonization of supervisory practices across jurisdictions, OSFI considered the practices of a number of foreign regulators. In revising its Framework, OSFI has taken into account the practices developed by these regulators.

The revised Framework also takes into account OSFI's experience in supervising various types and sizes of institutions. It accommodates the special requirements of the deposit-taking, life insurance, and property and casualty insurance sectors. OSFI was unique in this regard when it launched its review, although a number of other countries have since moved towards a single supervisory regime for both deposit-taking institutions and insurers, irrespective of their size.

The Framework applies to all federally regulated financial institutions. It is currently being implemented and will be fine-tuned based on experience and consultation with supervised institutions. OSFI will continue to challenge and refine its practices to ensure that they remain effective and efficient in a rapidly changing environment.

2. Benefits

The principal benefits of the revised Framework are:

- better evaluation of risks through separate assessment of inherent risks and risk management processes;
- greater emphasis on early identification of emerging risks and system-wide issues;

- cost effective use of resources through a sharper focus on risk; and
- reporting of risk focused assessments to institutions.

3. Key Principles

The following key principles form the basis of the Framework:

- ♦ The supervision of Canadian financial institutions is conducted on a consolidated basis, using information from other regulators as appropriate. It includes an assessment of all material entities (subsidiaries, branches, or joint ventures) both in Canada and internationally.
- ♦ The exercise of sound judgement in identifying and evaluating risks in an institution is central to the effectiveness of the Framework. Work performed will be focused on clearly identified risks or areas of concern.
- ♦ The level and frequency of supervisory scrutiny will depend on the risk assessment of the institution. Institutions that are well managed relative to their risks will require less supervision. Not all areas within an institution need to be reviewed every year.
- ♦ Supervision will include reviews of major risk management control functions such as Financial Analysis, Compliance, Internal Audit, Risk Management, Senior Management and Board Oversight. OSFI's supervisory process uses, where appropriate, the work of the institution's internal management and control functions.
- ♦ Communication of findings and recommendations to institutions will be timely. The degree of intervention will be commensurate with the risk profile of the institution and in accordance with the Guide to Intervention for Federal Financial Institutions.
- ♦ Ratings will be provided to the institution after each on-site review (once federal legislation to protect the confidentiality of such information is promulgated). The ratings will be linked to the stages of intervention in accordance with the Guide to Intervention for Federal Financial Institutions. The evaluation criteria and definitions of ratings, once developed, will be provided to industry for consultation and comment before being implemented.
- ♦ OSFI will continue to rely on external auditors for the fairness of the financial statements and will use their work to modify the scope of its reviews to minimize duplication of effort. Similarly, OSFI will continue to rely on appointed actuaries for the adequacy of policy liabilities and will use their work to modify the scope of its reviews.
- ♦ OSFI will carry out benchmarking studies on a range of subjects which compare institutions to their peer groups to identify best industry practices for dealing with various levels of risk. OSFI will share this information with institutions' senior management and Boards of Directors so that they can ensure that their risk management processes are adequate.

4. Risk Assessment

The addition of a dynamic risk assessment process represents an important change to the Framework.

Risk assessment begins with identifying significant activities of an institution. The net risk in these activities is a function of the aggregate inherent risk offset by the aggregate quality of risk management. This evaluation is illustrated by the following equation:

Inherent Risks **mitigated by** ***Quality of Risk Management = Net Risk***

The results of the risk assessment are summarized in a Risk Matrix as discussed below (subsection 4.6).

4.1 Significant Activities

Significant activities could include any significant line of business, unit or process. Significant activities are identified from various sources including the institution's organization charts, strategic business plan, capital allocations, and internal and external financial reporting.

Sound judgement is applied in determining the significance or materiality of any activity in which an institution engages. The following are examples of criteria that may be used:

a. assets generated by the activity in relation to total assets (both on- and off-balance sheet);
b. risk-weighted assets generated by the activity in relation to total risk-weighted assets;
c. revenue generated by the activity in relation to total revenue;
d. net income before tax for the activity in relation to total net income before tax;
e. risk-weighted capital for the activity in relation to total risk-weighted capital;
f. internal allocation of capital to the activity in relation to total capital;
g. insurance underwriting exposure in relation to capital; and
h. reserves held as a percentage of total reserves.

4.2 Inherent Risk

Inherent risk is intrinsic to a business activity and arises from exposure and uncertainty from potential future events. Inherent risk is evaluated by considering the degree of probability and the potential size of an adverse impact on an institution's capital or earnings.

A thorough understanding of the environment in which an institution operates and its various business activities is essential to effectively identify and assess inherent risk in those activities. OSFI has decided to group these risks in the following categories for assessment purposes:

- credit risk;
- market risk;
- insurance risk;
- operational risk;
- liquidity risk;
- legal and regulatory risk; and
- strategic risk.

These risk categories are described in Appendix A.

After significant activities have been identified, the level of each inherent risk in those activities is assessed as **low, moderate,** or **high** (see Appendix B). This assessment is made without considering the impact of risk mitigation through the institution's risk management processes and controls. The quality of these factors are considered separately and combined with the inherent risk assessment to determine the net risk of each activity.

4.3 Quality of Risk Management

The quality of risk management is evaluated for each significant activity. In addition to Operational Management, we have identified six risk management control functions that may exist in an institution. These are: Financial Analysis, Compliance, Internal Audit, Risk Management, Senior Management and Board Oversight (see Appendix C). The presence and nature of these functions vary based on the size and complexity of an institution.

Operational Management for a given activity is primarily responsible for its day-to-day management. This function ensures that policies, processes, control systems, staff levels and experience are sufficient and effective in compensating for the risks inherent in the activity. The organizational structure and controls must be effective in preventing and detecting material errors or irregularities in a timely manner.

The degree to which an institution's Operational Management and controls for a given activity need to be reviewed depends on the assessment of the effectiveness of the institution's other risk management control functions. For example, in conglomerates it may be possible to assess the effectiveness of Operational Management and controls for a given activity through an assessment of the other risk management control functions. Where institutions lack some or all of the risk management control functions, OSFI looks to other functions, within or external to the institution, that handle these responsibilities.

Where independent reviews of Operational Management and controls have not been carried out or where independent risk management control functions are lacking, OSFI will, under normal circumstances, make appropriate recommendations or direct that appropriate work be done.

The quality of risk management processes for each significant activity is an evaluation of an institution's current practices of each risk management control function for that activity. The quality of risk management processes is assessed as **strong, acceptable or weak**.

4.4 Net Risk

The net risk for each significant activity is a function of the aggregate level of inherent risk offset by the aggregate quality of risk management. The aggregate levels are based on judgements that consider all of the inherent risk ratings and the quality of risk management for the activity.

For example, the investment banking activity of an institution may be evaluated as having a high aggregate level of inherent risk arising from a combination of high credit risk, high market risk, and high liquidity risk. However, net risk for the activity may be rated as moderate due to mitigation by a strong aggregate quality of risk management resulting from strong operational management, strong internal audit, strong risk management, and strong Board oversight.

Net risk is rated as **low, moderate** or **high** as shown in the chart below.

Aggregate Quality of Risk Management for Significant Activity	**Aggregate Level of Inherent Risk for Significant Activity**		
	Low	**Moderate**	**High**
	Net Risk Assessment		
Strong	Low	Low	Moderate
Acceptable	Low	Moderate	High
Weak	Moderate	High	High

4.5 Direction of Net Risk

The above assessments include a determination of the current direction of net risk. Direction of risk is assessed as **decreasing, stable,** or **increasing** over an appropriate time horizon for the institution. For example, the time horizon for a conglomerate may need to be much longer than for a smaller institution. The time horizon considered is indicated in each case.

4.6 Risk Matrix

A Risk Matrix (see Appendix D) is used to record the assessment of inherent risks, the quality of risk management, and the resulting net risk evaluation for each significant activity.

The Risk Matrix includes a determination of an **Overall Rating of Net Risk** and the **Direction of Risk**. In arriving at the Overall Rating of Net Risk, the relative significance or materiality of each activity is considered. This is rated **low**, **moderate**, or **high**. This assessment ensures that an activity with low materiality but high net risk does not skew the Overall Rating. OSFI's supervisory efforts will be focused on material high risk activities.

An Overall Rating for each risk management control function is also included in the Risk Matrix.

The Risk Matrix includes a **Composite Rating** and a **Direction of Composite Risk** for the institution. These could be affected by factors such as capital and earnings. Accordingly, the assessment includes a review of the quality, quantity, and availability of externally and internally generated capital. In reviewing an institution's ability to generate capital internally, profitability is considered both on a consolidated and unconsolidated basis. An appropriate time frame for the **Composite Rating** and the **Direction of Composite Risk** is also included.

While the Risk Matrix is a convenient way to summarize the conclusions of risk assessment, it is supported by documentation of the analysis and the rationale for the conclusions.

4.7 Risk Assessment Summary

The Risk Assessment Summary (RAS) is an executive summary which highlights an institution's present financial condition, its prospective risk profile, key issues, and past supervisory findings. The RAS includes:

a. A Risk Matrix;
b. An overview of the main business activities and strategies;
c. An assessment of the effectiveness of the key risk management control functions;

d. An assessment of the adequacy of capital or regulatory deposit and the profitability of the institution;
e. Where an institution is part of a foreign entity (i.e. a subsidiary or a branch), a suitable assessment of the foreign entity's operations and the supervisory system in effect in the home jurisdiction;
f. A listing of significant events during the past 12 months;
g. Financial highlights; and
h. Intervention status reports.

The RAS facilitates a sharper focus on activities that pose the greatest risk to an institution.

The RAS is used to set priorities for the year. It does not include the supervisory work to be carried out nor resources required. Planned work and resources required are included in the Supervisory Plan discussed below (subsection 6.2).

While the RAS includes a Composite Rating for an institution, this rating is preliminary and is not shared with the institution until the risk rating is confirmed through appropriate on-site reviews.

Once appropriate criteria have been developed, OSFI intends to provide the institution with an Overall Rating for each of its risk management control functions after the completion of an on-site review.

Intervention staging, in accordance with the Guide to Intervention for Federal Financial Institutions, is reviewed after the RAS has been updated. Any changes to the staging requires approval of a senior director and the Deputy Superintendent, Supervision.

The Composite Risk rating of an institution should be a clear indication of the intervention stage rating of the institution. An institution with a "low" Composite Risk Rating should be Stage 0. An institution with a "high" Composite Risk Rating should be Stage 2 or worse. An institution judged to have a "moderate" risk rating could be either a Stage 0 or a Stage 1 depending on the direction of the risk profile (decreasing, stable, or increasing) and the reasons behind the rating (for example, very weak management control processes would indicate a need for higher staging).

The RAS is the primary document provided to senior OSFI officials for briefings. Additional documentation may be necessary in case of institutions at Stage 1 or worse.

OSFI currently translates its assessments of deposit-taking institutions into the CAMEL rating for CDIC and other users of this system.

5. The Relationship Manager

Each supervisory group is headed by a director who is the designated relationship manager (RM) for all institutions in his/her group. The director may delegate the role of RM to a member of his/her team.

The RM is the focal point for the supervision of assigned institutions and OSFI's primary contact with those institutions. The RM is also part of the regulatory approval process in conjunction with the Registration and Approvals Division.

The responsibilities of a RM that support the key principles of the Framework are described below under the supervisory process.

6. The Supervisory Process

The main steps of the supervisory process are: **Analysis, Planning, Action, Documentation, Reporting, and Follow-up**. These steps are listed below. Although the steps appear sequential, updating of the risk assessment is a dynamic process requiring frequent reassessments at various stages of the supervisory process.

STEPS	OUTPUT
1. Analysis (Understanding the institution and developing a risk profile)	1. Risk Matrix 2. Risk Assessment Summary (RAS)
2. Planning (Scheduling and planning activities for the supervisory period)	3. Supervisory Plans (by Institution, Division, Group, and Sector)
3. Action (Conducting on-site reviews and on-going monitoring)	4. Information requests
4. Documentation (Preparing and filing information to support findings)	5. Section Notes 6. Working papers
5. Reporting (Report of findings and recommendations to the institution)	7. Management Report 8. Updated RAS
6. Follow-up of findings and recommendations.	9. Updated RAS

6.1 Analysis (Step 1)

Analysis of the institution is a primary input into the risk assessment process. The supervisory groups are responsible for ongoing analysis and monitoring of institutions. Analysis is performed at least once every three months for institutions rated Stage 1 or better, and on a monthly basis for institutions rated Stage 2 or worse. Analysis work carried out just prior to the preparation of the Supervisory Plan is more extensive to allow for better input into the planning process.

Analysis and monitoring includes a review of company information as well as meetings with key individuals at the institution to discuss trends and emerging issues. The scope of this work will depend on the size and the risk profile of the institution.

Results of the analysis are used to update the Risk Matrix and the RAS.

6.2 Planning (Step 2)

A Supervisory Plan is prepared at the beginning of each fiscal year and outlines work planned and resources required. The scope of the work planned is based on the RAS. The focus is on the activities and risk management processes identified in the RAS as significant risk areas. Each director uses the RAS to determine priorities for the upcoming year and to allocate resources to individual institutions accordingly.

The Supervisory Plan for each institution includes a consideration of the following:

- industry risks;
- concerns or issues raised by OSFI's Specialist Support or Regulatory Sectors;
- concerns or issues raised by OSFI executives; and
- planning for benchmarking, peer reviews, or other special studies.

As appropriate and consistent with the general agreements already in place, the planning process is to take into account issues raised by CDIC for institutions of particular concern to them.

Once Supervisory Plans are approved at the group level and priorities established, the institution specific Supervisory Plans are finalized.

The Supervisory Plan is subject to revisions if unforeseen events alter the risk profile of the institution. However, any changes require a reassessment of priorities, not just an extension of the scope of the supervisory efforts.

6.3 Action (Step 3)

The RM communicates with key parties at the institution and maintains an on-going relationship with management. For larger institutions, this will likely involve quarterly visits.

Information requested from an institution is based on the specific requirements arising from the risk assessment process. The main information request is made prior to an on-site review.

On-site reviews are a critical part of the supervisory process. The scope of on-site reviews depends on the Overall Rating of Net Risk. These reviews and interaction with the institution's management also enhance OSFI's understanding of the institution and its risk profile.

6.4 Documentation (Step 4)

All supervisory groups use the same documentation standards.

The revised supervisory file structure is consistent with the new risk framework. The file includes an updated copy of the RAS, a copy of the Management Report and related correspondence, and copies of various section notes.

A section note is prepared in the standard format for each significant activity or risk management control function identified for review. The section note is used to fully document an assessment of the activity or the risk management control function. Working papers necessary to support the assessment are also on file. If a significant activity or risk management control function is not reviewed during an on-site visit, the latest section note is brought forward. This ensures that the file contains the latest information available to OSFI on all areas of an institution.

6.5 Reporting (Step 5)

The RM writes annually to the institution outlining the results of the supervisory work whether or not an on-site review has taken place. In the case of an on-site review, the final stage of the process includes three levels of verbal and written reports. These levels target the following audiences: OSFI management, the institution's management, and external stakeholders.

Written reports to OSFI management consist of the updated RAS, a summary of the findings and section notes with detailed information of significant findings.

Findings and recommendations are first discussed with appropriate senior managers in the institution. Where there is a Risk Management or Internal Audit department, the findings and recommendations are discussed with the responsible manager. This is followed by reporting to the Chief Executive

Officer (CEO) and the Audit and/or Risk Committees. This reporting is not tied to the timing of Audit and/or Risk Committee meetings, but a meeting is scheduled with these groups at the earliest possible time after the Management Report is completed.

The Management Report is the key written document sent to the institution. It addresses findings, recommendations and follow-up of previous findings. Ultimately, the Management Report will also include a brief explanation of the Composite Rating and ratings of the applicable risk management control functions.

Management Reports to Canadian companies are addressed to the CEO and copied to the Chair of the Audit Committee. Management Reports to foreign institutions operating branches in Canada are addressed to the Principal Officer or Chief Agent of the Canadian branch. Where there are significant issues with a Canadian branch, a copy of the Management Report is sent to the CEO and the Chair of the Audit Committee at the home office. In all cases, the covering letter requests that a copy of the Management Report be provided to the external auditors and to the appointed actuary where applicable.

OSFI has agency agreements with CDIC and certain provincial regulators who receive reports from OSFI. Reporting to these parties is in accordance with their respective agreements. In all cases, the confidentiality of the information is respected.

6.6 Follow-up (Step 6)

The findings and recommendations reported to the institution are followed-up on a timely basis and the results included in the RAS updates.

Appendix A Risk Categories

Following are descriptions of the risk categories identified in subsection 4.2 of the Framework. These descriptions should be read within the context of the definition of inherent risk contained in subsection 4.2.

1. Credit Risk

Credit risk arises from a counterparty's inability or unwillingness to fully meet its on- and/or off-balance sheet contractual obligations. Exposure to this risk results from financial transactions with a counterparty including issuer, debtor, borrower, broker, policyholder, reinsurer or guarantor.

2. Market Risk

Market risk arises from changes in market rates or prices. Exposure to this risk can result from market-making, dealing, and position-taking activities in markets such as interest rate, foreign exchange, equity, commodity and real estate.

Interest rate risk and foreign exchange risk are described further below:

a. Interest Rate Risk

Interest rate risk arises from movements in interest rates. Exposure to this risk primarily results from timing differences in the repricing of assets and liabilities, both on- and off-balance sheet, as they either mature (fixed rate instruments) or are contractually repriced (floating rate instruments).

b. Foreign Exchange Risk

Foreign exchange risk arises from movements in foreign exchange rates. Exposure to this risk mainly occurs during a period in which the institution has an open position, both on- and off-balance sheet, and/or in spot and forward markets.

3. Insurance Risk

a. Product Design and Pricing Risk

Product design and pricing risk arises from the exposure to financial loss from transacting insurance and/or annuity business where costs and liabilities assumed in respect of a product line exceed the expectation in pricing the product line.

b. Underwriting and Liability Risk

Underwriting and liability risk is the exposure to financial loss resulting from the selection and approval of risks to be insured, the reduction, retention and transfer of risk, the reserving and adjudication of claims, and the management of contractual and non-contractual product options.

4. Operational Risk

Operational risk arises from problems in the performance of business functions or processes. Exposure to this risk can result from deficiencies or breakdowns in internal controls or processes, technology failures, human errors or dishonesty and natural catastrophes.

5. Liquidity Risk

Liquidity risk arises from an institution's inability to purchase or otherwise obtain the necessary funds, either by increasing liabilities or converting assets, to meet its on- and off-balance sheet obligations as they come due, without incurring unacceptable losses.

6. Legal and Regulatory Risk

Legal and regulatory risk arises from an institution's non-conformance with laws, rules, regulations, prescribed practices, or ethical standards in any jurisdiction in which the institution operates.

7. Strategic Risk

Strategic risk arises from an institution's inability to implement appropriate business plans, strategies, decision-making, resource allocation and its inability to adapt to changes in its business environment.

Appendix B Definitions of Inherent Risk Ratings

Low Inherent Risk:

Low inherent risk exists when there is a lower than average probability of an adverse impact on an institution’s capital or earnings due to exposure and uncertainty from potential future events.

Moderate Inherent Risk:

Moderate inherent risk exists when there is an average probability of an adverse impact on an institution’s capital or earnings due to exposure and uncertainty from potential future events.

High Inherent Risk:

High inherent risk exists when there is a higher than average probability of an adverse impact on an institution’s capital or earnings due to exposure and uncertainty from potential future events.

Appendix C Risk Management Control Functions

1. Operational Management

Operational management is responsible for planning, directing and controlling the day-to-day operations of an institution's business activities.

2. Financial Analysis

Financial analysis is the function that performs in-depth analyses of the operational results of an institution and reports them to management. Effective reporting is key to this function as the operational results affect strategic and business decisions made by management and the Board. This function is generally only found as a separate unit in larger institutions.

3. Compliance

Compliance is an independent function within an institution that: 1) sets the policies and procedures for adherence to regulatory requirements in all jurisdictions where an institution operates; 2) monitors the institution's compliance with these policies and procedures; and, 3) reports on compliance matters to senior management and the Board.

4. Internal Audit

Internal audit is an independent function within the institution that assesses adherence to and effectiveness of operational and organizational controls. In addition, internal audit may also assess adherence to and effectiveness of compliance and risk management policies and procedures.

5. Risk Management

Risk management is an independent function responsible for planning, directing and controlling the impact on the institution of risks arising from its operations. The function is generally only found as a separate unit in the larger institutions, and may address the following:

- identification of risks;
- development of measurement systems for risks;
- establishment of policies and procedures to manage risks;
- development of risk tolerance limits;

- monitoring of positions against approved risk tolerance limits; and
- reporting of results of risk monitoring to senior management and the Board.

6. Senior Management

Senior management is responsible for planning, directing and controlling the strategic direction and general operations of the institution. Its key responsibilities include:

- ensure organizational and procedural controls are effective;
- ensure compliance with approved policies and procedures;
- develop strategies and plans to achieve approved strategic and business objectives; and
- develop sound business practices, culture and ethics.

7. Board of Directors

The Board of Directors is responsible for providing stewardship and management oversight for the institution. Its key responsibilities include:

- ensure management is qualified and competent;
- review and approve organizational and procedural controls;
- ensure principal risks are identified and appropriately managed;
- review and approve policies and procedures for the institution's major activities;
- review and approve strategic and business plans; and
- provide for an independent assessment of management controls.

Institution Name
Risk Matrix as at DATE

Significant Activities	Materiality	Inherent Risks							Quality of Risk Management							Net Risk	Direction of Risk
		Credit	Market	Liquidity	Insurance	Operational	Legal & Regulatory	Strategic	Operational Mgmt.	Financial Analysis	Compliance	Internal Audit	Risk Mgmt.	Senior Mgmt.	Board Oversight		
Activity 1																	
Activity 2																	
Activity 3																	
etc.																	
Overall Rating																	

Capital		Earnings			
Composite Rating		Direction of Risk		Time Frame	