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

Office of the Superintendent of Financial Institutions

Internal Audit Report on Enterprise Risk Management

November 2011

OSFI BSIF

Canada

Table of Contents

1. Background

Introduction

Internal Audit conducts assurance work to determine whether the Office of the Superintendent of Financial Institution (**OSFI's**) risk management, control processes, and governance, as designed and represented by management, are adequate to ensure risks are appropriately identified and managed.

The audit of Enterprise Risk Management (**ERM**) was approved by the OSFI Audit Committee and the Superintendent for inclusion in the OSFI 2010-2011 Internal Audit Plan. This report presents the results of that audit based on audit work completed at the end of April 2011. The audit recommendations will support ERM to continuously improve the control framework for managing risks.

This report was presented to the OSFI Audit Committee and approved by the Superintendent in November, 2011. The Superintendent and the Assistant Superintendents, who have provided their management response within this report, have also reviewed it.

Why risk management is important

Risk management helps OSFI in developing an over-arching framework for managing its risk. Risk management enables OSFI to develop strategies to mitigate risk and to align its resources and priorities to ensure its continued success in meeting corporate plans and priorities.

Under the TBS Policy on Internal Audit and Directive on Departmental (Agency) Audit Committees, the Committee:

> *"should exercise oversight of core areas of departmental management, control and accountability, including reporting,"* and
>
> "*will review the departmental Corporate Risk Profile and provide any related advice to the deputy head*."

Business Objectives

The objective of OSFI Enterprise-Wide Risk Management is stated simply as:

> *"The purpose of risk management is to manage risk within established risk tolerances."*[1]

Risk is defined as:

> "*Any event that could impair our ability to achieve our objectives*."

Risk tolerance is defined as:

> "*The level of residual risk you are willing to accept after considering the level of controls*."

Continued on next page

[1] OSFI's Enterprise-Wide Risk Management Framework (November 2008)

1. Background, Continued

Context

The environment in which OSFI operates presents an array of risks to the achievement of its mandate and objectives. While many of these challenges are consistently present, the extent to which they present a risk to OSFI's objectives varies, depending on economic and financial conditions and the financial industry environment. OSFI's ability to achieve its business objectives and fulfill its mandate depends on the timeliness and effectiveness, in which it identifies, evaluates, prioritizes, and develops initiatives to address areas where its exposure (risk) is the greatest.

OSFI's ERM proactively identifies and manages its risks as a continuous risk assessment process. The ERM's top-down and bottom-up communication approach ensures that those with the broadest knowledge provide timely input into the determination and assessment of key risks and mitigation strategies and their incorporation into strategic and business planning. This approach promotes buy-in and support from the Executive, management, and staff ensuring quality and consistency in application of ERM and the ability to assess the relative significance of risks across the Office.

Attachment 1: ERM Structures and Interaction sets out the five components of OSFI's ERM structures, its integration and interaction, as well as the source of risk management information.

ERM risk management

OSFI's *Enterprise-wide Risk Management* framework divides *risks* into *external* and *internal categories*. The *external risk category* consists of economic and financial conditions, the financial industry environment, OSFI's legal environment, and catastrophic events. External risks arise from events that OSFI cannot influence but they are monitored in order to mitigate potential impact of them to OSFI's operations.

The *internal risk category* consists of operational risks that are broadly categorized as people, processes (*governance* processes, *internal* processes, and *relationship management* processes), enabling *supporting systems*, and *culture* (core values and change management).

OSFI's ERM Risk Coordinator oversees OSFI's ERM process and provides a risk overview to Executive on a quarterly basis. Sector Risk Coordinators are responsible for coordinating the Sector's risk identification, assessment and reporting process in accordance with OSFI's ERM Policy and Framework within each sector.

OSFI's ERM is a systematic process for building and improving risk management capabilities across the Office by understanding, identifying, prioritizing, assessing, acting on and communicating risk issues through a dynamic risk assessment approach.

Continued on next page

1. Background, Continued

Context
(Cont'd)

Sector risk management

The Sector Risk Coordinators facilitate a broad involvement of managers and staff in risk management and ongoing communications through periodic information sessions where Sector management present their key risks and mitigation strategies. There are quarterly risk assessments providing updated risk registers including addition of new risks or removal of existing risks as appropriate and a risk summary is provided to the Executive. Annually, there are more formal risk assessments where the Sectors update their risk registers, which feeds the ERM Summary as input into OSFI's annual corporate planning.

Emerging Risks Committee

OSFI's Emerging Risks Committee (ERC) meet regularly to identify material external risks affecting the financial services industry along with work plans and related priorities associated with those risks. The Committee reports to the Executive and management on an ongoing basis and its risk assessments are incorporated into the ERM summary for corporate planning purposes.

Annual Corporate Planning

OSFI's ERM policy sets out the accountabilities and responsibilities of those involved in risk management requiring detailed, formal Sector risk assessments, for validation purposes before OSFI's annual corporate planning process begins as input into the corporate planning process. The ERM Risk Coordinators consolidate their Sector's risks into a Sector risk summary as key input into OSFI's Planning Model and Integrated Planning Cycle.

Risk management reporting

In addition to risk management reporting as part of OSFI's annual Corporate Planning there are informal and formal avenues for communicating and reporting on risk management including specific risk assessments and mitigation strategies undertaken to address them. Information about key risks and strategies undertaken are included in all-office communications such as In The Loop, Town Hall Meetings as well as providing periodic briefings on OSFI's risk management to the Audit Committee.

The Sectors and ERM brief the Executive and respective management and staff on their risk assessments (profiles). The Emerging Risk Committee also briefs the Executive and management on a periodic basis *on external risk affecting the financial services industry and their potential impact to OSFI's operations*. In addition, the ERM briefs the Audit Committee on OSFI's risk management on a quarterly basis.

Formal reporting on OSFI risk management and issues is accomplished via OSFI' Plan and Priorities, Annual Report and Departmental Performance Report. Such reporting takes into consideration risks that impact the ability of OSFI to meet its Long Term Priority.

2. Audit Objective, Scope, and Approach

Audit Objective

The objective of the audit is to provide reasonable assurance of:

- The ERM *control framework*[2] for identifying, prioritizing, assessing, acting on, and communicating external and internal risks and related control/mitigation practices (design).
- How well and the degree to which:
  - ERM policy, directives, procedures and aids/tools are understood, in place and functioning as intended (operations);
  - ERM is incorporated into corporate (strategic and business) planning and Sector operations; and
  - ERM reporting and communications is incorporated into OSFI's reporting and communications.

Audit Scope

The audit covers the ERM control framework as at *1 December 2010* as well any improvements underway / planned.

The audit is focused on the underlying ERM policy, procedures, and aids/tools used for the period *from 1 April 2010 to April 2011*.

Matters outside of the scope

- A review of the *Corporate Planning Framework* except as to the integration of ERM into strategic and Sector business planning.
- A review of OSFI *performance reporting* except as to the integration of risk management reporting, as appropriate.

Audit Approach

The audit was conducted in accordance with the Institute of Internal Auditors' International Standards for the Professional Practice of Internal Auditing, consistent with the Treasury Board Policy on Internal Audit.

The audit involved three methods of examination:

- A review of ERM *policy, procedures, and aids/tool* used to assess the ERM control framework and its integration into strategic and business planning, and Sector/division operations as well as its consistency with Government policy, directives, and guidance.
- A review of *the application of the ERM* control framework and supporting *information/documents* used for the identification, prioritization, assessment, decision making, escalation of risk matters and communication/reporting of external and internal risks and related control/mitigation practices including:

Continued on next page

[2] Refer to the Appendix 2: ERM Control Criteria, a table of governance, risk management and control elements applicable to OSFI's ERM function

2. Audit Objective, Scope, and Approach, Continued

Audit Approach (Cont'd)

- ERM, Sector and corporate planning *risk management activities, processes, and aids/tools;*
- *Risk management oversight, reporting and communications* at the corporate and Sector/Division levels; and
- Risk management *accountabilities* and related practices *of the* Audit Committee, Executive, and operations management.

- Interviews with:
  - *ERM coordinator and Sector risk coordinators as well as Managing Director, Finance and Corporate Planning;*
  - Operations Sector *management and staff involved in risk management as well as corporate planning;*
  - *Management in supporting Divisions (IM/IT, Human Resources, Finance, Security and Communications)* in terms of their risk management incorporated into operations Sector and corporate planning; and
  - *Sector Assistant Superintendents, Chair of the Audit Committee, and the Superintendent.*

The results of these reviews and interviews are consolidated to ensure a consistent and balanced assessment of OSFI's ERM within the Office.

Internal control criteria

The *ERM Control Criteria, Appendix A,* will be the basis for assessing ERM's control framework.

These criteria are based on the following Government policies, directives and guidance:

- Risk Management Policy
- Integrated Risk Management Implementation Guide
- Policy on Internal Control
- Policy on Internal Audit
- Directive on Departmental Audit Committees
- Management Accountability Framework.

As well as,

- TBS, Internal Audit Sector, *Core Management Control Framework guidance and their Horizontal Audit of Corporate Risk Profiles and related Processes* (April, 2010), and internationally recognized COSO[3] control framework, as adapted to OSFI's business and risk environment.
- Recommendations of the 2009 independent assessment of OSFI's ERM program.

Continued on next page

[3] COSO: Committee of Sponsoring Organizations of the Treadway Commission

3. Conclusion

Conclusion

While OSFI, through its *ERM Policy* and related *Framework* and its *Corporate Planning Framework* and guidance, has in place and is applying all components of a comprehensive risk management framework, improvements should be undertaken to strengthen its effectiveness as presented in this Report.

A focused management effort is required in the following[4]:

- Adopting a structured comprehensive Internal Control Framework to ensure consistency in assessing controls and in the interim document controls for key risks,
- Improving the quality and consistency of the Risk Registers, a key management tool in ERM, to allow for a common understanding and aggregation of risks OSFI wide,
- Ensuring risk exposures are more transparent by separating risk tolerance, to more easily facilitate risk decisions

The following governance and control practices were observed over OSFI's risk management:

- Through its Corporate Planning Strengths Weaknesses Opportunities Threats (SWOT)and Blue-Sky exercises as well as continuous monitoring of external, emerging, and internal risk, OSFI demonstrates a strong commitment to risk management.
- Through its Long-Term Priority and In-The-Loop communications, Staff are kept abreast of risk that matters.
- Through its Emerging Risk Committee and the Research Division external and emerging risks are identified and assessed as to their potential impact to Financial Institutions and to OSFI's regulatory and supervision work and resources.
- Through an ERM Executive (Risk) Summary document, based on *Risk Registers*, and one-to-one discussions with management, the Executive and the Audit Committee are briefed on risk issues / concerns.
- Quarterly Sector and Business Line *Risk Registers* are maintained with an annual in-depth review and update for planning and priority setting purposes.

We wish to recognize the collaborative work and the rapport and exchange of views received throughout the audit, especially the introduction of improvements in ERM during the audit. The depth of the review and focusing on what matters would not have been possible without the support received.

________________________________ ____________________

Chief Audit Executive, Internal Audit Date

Continued on next page

[4] Refer to *Attachment 2: Risk Assessment Process*

4. Management Response

Overview

We thank the audit team for their collaborative approach in conducting this audit. Representatives of the ERM and Corporate Planning functions reviewed the report, its findings, observations, and recommendations.

Management acknowledges the three main themes within the report (i.e. methodology, accountability, and reporting) and generally agrees with the observations that support these themes. Recognizing the existence of linkages between some of the recommendations, management wishes to comment as follows.

Response

Risk Management Policy and Framework *– We acknowledge and concur with the recommended revisions to the ERM Policy and/or Framework regarding the portrayal of OSFI's risk management process as an integrated management tool and including reference to the robust risk communication practices already in place across the office. Revisions to these documents will be made accordingly and a requirement that the Policy and Framework be reviewed and updated on a regular basis will be added.*

Internal Control Framework and Control Documentation – *The Executive Committee has approved an initiative to plan and scope an approach towards developing an enterprise level internal control framework. Work is currently underway on this initiative, which includes integration with ERM. ERM and Corporate Planning representatives are participating in the internal working group. The group's recommendations will be presented to Executive Committee in early 2012.*

Residual Risk and Risk Tolerance *– Initially, management will separate residual risk from risk tolerance for individual risks as part of the refined methodology for completing the risk registers. In recent months, the Executive Committee has asked the Assistant Superintendent, Corporate Services, to lead an initiative to review OSFI's Risk Tolerance Framework and to develop a Risk Appetite Statement. Identification of overall risk tolerances for Business/Sub-Business lines will be considered once risk tolerance at the enterprise level is defined.*

Continued on next page

4. Management Response, Continued

Response (Cont'd)

Quality of Risk Registers

-Quarterly Updates to Risk Registers – To address the fact that completion of risk registers on a quarterly basis are seen to be time consuming (yielding few, if any, new results) and duplication of other operational activities, management will consider reducing the frequency of reporting to an annual basis at the sector level in a timeframe consistent with the overall planning process. To ensure consistency of reporting, the register templates and the instructions for completing them will be reviewed and updated. The sector coordinators will work together to ensure the quality of the risk registers is uniform across sectors. Improved practices around completion of risk registers and linkages to the Corporate Planning Process will lead to improved quality and consistency of the ERM process.

- Impact Statements and Tolerances – We acknowledge the development of impact statements at the Sector and Business/Sub-Business Line levels to facilitate the assessment of impacts of a risk on operations and on the Sector. Risk tolerances will be considered for Business/Sub-Business Lines and at the Sector level once work on risk tolerance at the enterprise level is completed, as noted above.

- Management of Mitigation Actions - We will explore options for monitoring, tracking, and reporting on mitigation actions.

Control Process

- Management Oversight – We will explore reporting options with a view to strengthen or complement the ERM Overview summary, prepared for Executive, in order to enhance the transparency of OSFI's risk profile for Executive. We will consider amendments to the methodology to enhance reporting to management for new risks and "high" risks.

- Managing Risk Information – We do not believe that an integrated automated ERM system is needed in the short term to enhance our risk management process and therefore do not wish to proceed with work in this area at this time.

- Capacity of and Competencies in Risk Management – We agree that increased resources will be needed to implement the improvements to the ERM process initially and we believe that this can be accomplished within the existing staff complement. In the longer term, we will review the resource needs (competencies and capacities) for ongoing coordination of the risk management function at OSFI. Resource requirements will need to be considered in light of the linkages with the Enterprise-wide Internal Control Framework.

Continued on next page

5. Observations and Recommendations

5.1 Risk Management Policy and Framework

Observation: OSFI's Enterprise-Wide Risk Management Policy and Framework have not been reviewed and updated since 2005 and 2008 respectively. Current practices are not fully reflected in the Policy and Framework.

OSFI's ERM Policy and Framework have not been reviewed and updated since 2005 and 2008 respectively. Not all current practices are fully reflected in these documents, for example:

- **The ERM Framework document does not capture the strong risk communication practices across the Office.** We view this important communication as the glue in integrating risk management into OSFI's day-to-day work and corporate planning.

  OSFI's ERM governance function is accountable to the Superintendent and the Executive. There is routine informal and formal risk reporting to the Executive with quarterly briefings to the Audit Committee on risk matters affecting OSFI's operations. The *ERM Risk Coordinator* meets with Sector management to review their risk assessments (risk registers), identifying areas of concern / risk for inclusion into the quarterly briefings.

  Through the *Long-Term Priority* and *In-the-Loop* communication from the Superintendent as well as regular 'town hall' meetings, Staff are kept abreast of risk that matters in OSFI.

  Through an *Emerging Risk Committee* and OSFI's *Research Division*, external emerging risks are identified and assessed as to their potential impact to Financial Institutions and a need to revise operation work plans and resources. The information is used in briefing the Executive and Sector management on potential impacts on the Financial Institutions and OSFI's operations as well as providing briefings for operation staff.

  Attachment 2: Risk Assessment Process highlights key points of communication within the current risk assessment process. By the nature of the risk information, collected both externally and internally, and the importance of applying judgment in assessing the impact of risk in achieving business objectives, robust communication is essential.

  Based on our discussion with those involved in maintaining risk assessments and reporting and our review of *Risk Registers* and *ERM Executive Summaries*, we found that the degree of involvement of the Executive and management in communicating risks across the Office to be very high.

Continued on next page

5. Observations and Recommendations, Continued

5.1 Risk Management Policy and Framework(Cont'd)

- **The relationships and responsibilities of Corporate Planning and Sector ongoing risk assessments and activities are not incorporated into the ERM framework document.**

  The key components of a comprehensive Office wide risk management, *Attachment 1: Structures and Interactions*, are set out in the ERM Policy and ERM Framework and the Corporate Planning Framework documents.

  The ERM Framework calls for an annual, in-depth review of Sector Business Lines and, as appropriate, Sub-Business Lines risks for planning purposes with quarterly reviews and update of *Risk Registers*. For risk management to be viewed and applied as an integrated management tool, OSFI's ERM Policy and Framework should incorporate the relationships between Corporate Planning and Sector risk assessments.

  Through its Corporate Planning *SWOT* and *Blue-Sky* exercises as well as continuous monitoring of external, emerging, and internal risk, OSFI demonstrates a strong commitment to risk management across the Office.

Recommendation: All components of OSFI's Office-wide risk management practices should be incorporated into the ERM Policy and ERM Framework documents and these should be updated and regularly reviewed to ensure continued relevance.

5.2 Internal Control Framework and control documentation

Observation: A structured, comprehensive Internal Control framework is not in place. The assessment of controls is informal, inconsistent, and not always transparent.

The ERM Framework sets out the consideration of internal controls in assessing risk and determining mitigation strategies / controls that are needed. Management is expected to continually review and assess their risks and controls. This informal exercise is useful but is not sufficiently robust to ensure existing internal controls are sufficient to balance risk and risk tolerance and that the controls are applied as intended.

As there is not a foundational internal control framework it is difficult to determine if all elements of internal control - governance, risk management and process controls - have been considered in the evaluation of internal control and whether controls are identified and evaluated on a consistent basis. Are risks over or under controlled?

Through a structured, comprehensive internal control framework OSFI would be able to achieve consistency and common use and understanding of internal controls, a balancing of the effectiveness of controls against the effort required, avoiding over / under controlling activities and facilitating reporting on risk and controls. We noted many instances where the risk registers included as controls activities that were not control mechanisms and where risk registers did not indicate current controls.

Recommendation: A formal internal control framework and guidance should be developed and integrated into ERM. In the interim, controls should be documented and assessed in the risk registers.

Continued on next page

5. Observations and Recommendations, Continued

5.3 Residual Risk and Risk Tolerance

Observation: Residual Risk is not transparent as it is combined with Risk Tolerance making it difficult to understand and facilitate risk decisions.

Currently a risk assessment combines its *risk, controls and risk appetite* in determining the Business / Sub-Business Line's *risk tolerance* rating. Is the risk Potentially Under Controlled, Cautionary, Acceptable, or Potentially Over Controlled?

As a result, the process does not provide for an assessment of the *risk exposure* (risk less controls) or *residual risk*. Therefore, it is difficult to know what the *risk exposure* is and whether it is acceptable or not.

It is important to separate the *residual risk* and *risk tolerance* so that the assessment process provides for a *risk decision* point (refer to *Attachment 2: Risk Assessment Process*). A risk decision point in assessing risk is integral in integrating risk management into day-to-day operations. Should we accept the risk (the *risk exposure* is in balance with the *risk appetite*) or should mitigation action be taken? Is the Business / Sub-Business Line possibly under or over controlled? Should operation plans and resources be revised to keep the risk in balance with the risk tolerance?

We noted that nearly half of the risks reported in the sector and business line risk registers are rated cautionary, that is current controls in place may need to be enhanced given the current level of risk exposure, however without transparency over residual risk it is difficult to conclude on the overall exposure and tolerance that OSFI is accepting. It was not always clear how risks rated potentially under controlled at the divisional level were aggregated up into an OSFI wide rating.

Recommendation: The risk assessment process should separate residual risk and risk tolerance and incorporate a risk decision point in the risk assessment process.

5.4 Quality of risk registers

Observation: The quality and consistency of the risk registers, a key management tool in ERM, needs improvement to ensure a clear understanding of the adequacy of risk management and alignment with OSFI's risk tolerance. Risk registers and the quarterly update are not generally viewed as a management tool but rather a compliance exercise.

OSFI's Sectors supported with *ERM Risk Coordinators* maintain quarterly *Risk Registers* at Sector Business Lines and in some cases at Division and Sub-Business Line levels. The *Registers* are intended for managing risk and mitigation activities and providing key input into Sector and Division annual business planning and priority setting. The ERM Risk Coordinators highlight for respective Sector management key risk concerns / issues and proposed mitigation action.

Based on discussions with those involved in updating, reviewing, and reporting on the *Registers* and our review of *Registers* we found that completion of the Registers was time consuming and often viewed as a compliance exercise or seen as duplication of other day-to-day operational activities.

Continued on next page

5. Observations and Recommendations, Continued

5.4
Quality of risk registers
(Cont'd)

We found inconsistencies in the interpretation of the framework and what is required in the *Registers* making it quite difficult to aggregate and understand results OSFI-wide. It was difficult in some cases to gain an understanding of the underlining risk issues, the existing controls, and impact of the risk in achieving to the business and OSFI's objectives.

We noted inconsistency in the application of the ERM framework in completing the risk registers. In particular,

- Inherent risk assessments for the same risk varied between sectors,
- Basis for risk tolerance assessments not always the same,
- Some risk registers included items while others did not, such as
  - Controls,
  - Action timelines,
  - Mitigated risks whereas others only had risks requiring mitigation,
  - Mitigation activities for acceptable risks

Having mitigation activities for acceptable risks implies a potentially over controlled risk.

Risk Registers do not clearly demonstrate the impact of a risk on the business objectives and OSFI's mandate.

Based on our review of representative *Risk Registers* we found that the relationship of the risk's *impact* and the *risk tolerance* to the *Business / Sub-Business Line's* objective(s) is not always clearly set out in the *Registers*. Although a risk's *impact* is 'rated,' it is difficult to assess the seriousness of the risk, its impact to operations and the level of control needed and its impact in OSFI being able to deliver on its mandate and long-term priorities.

Combined with weak control assessments it is difficult to determine if the risks are adequately managed. Is risk and control in balance (residual risk is under or at the risk tolerance for the Business / Sub-Business Line), or is the risk over or under controlled?

From our IA's review of *Registers*, we found cases where the linkage between a risk to OSFI's objectives and the assigned *risk tolerance* was obvious, while in other cases the linkage was not obvious.

Mitigation actions are informally managed and not well documented in the risk registers.

There is not a formal monitoring, tracking and reporting process for implementing action to mitigate the risk. Our review of the risk registers found:

- Existing controls not always included
- Completed actions not always added as a control
- Mitigation actions not tied to the business operation action plans
- Actions listed as mitigation that are business as usual
- Status and timelines of mitigation actions not always in risk registers

Continued on next page

5. Observations and Recommendations, Continued

5.4
Quality of risk registers
(Cont'd)

Recommendation: 1) The ERM framework should be consistently applied to the completion of Risk Registers to allow for a common understanding and aggregation of risks OSFI wide. Clearer instructions should be developed for the sector risk registers and the template enhanced to promote a common approach. 2) The Risk Registers should be formally integrated into management operation reporting. 3) The ERM risk coordinator should oversee the quality of the risk registers.

5.5

Management Oversight

Observation: Risk information is not sufficient for management oversight purposes

The key risk management tool is the Sector and Business / Sub-Business Line *Risk Registers* where key risks and risk assessments are documented setting out risk information: the impact of the risk, the underlying inherent risk, existing internal controls, the risk direction, and the risk tolerance. Where appropriate mitigation action is set out for review and approval by management on a quarterly basis. These *Registers* are used in preparing an ERM Executive Summary for the Executive and the Audit Committee.

Based on discussions with the *Sector Risk Coordinators, Registers* are reviewed by sector heads and updated quarterly with an informal in-depth review for annual planning purposes. The Sector registers are used as input into the quarterly ERM narrative Executive Summary to the Executive.

However, there is not roll up of risk assessment information into aggregate corporate risk profiles by key risks and by Business / Sub-Business Lines, Sector and OSFI levels, to provide an overview of risk across the Office for management overview purposes.

There is a need to pull Business / Sub-Business Line, Sector and aggregate Corporate risk information and assessments together to provide a rolled up view or *dashboard* of risk. What are the pressing risks? What Business / Sub-Business Lines are experiencing pressing risks? Are these views of risk consistent with management's top down view? Is there a concentration of risk in a specific Sub-Business Line? Are there *common risks* that should be managed on a collaborative basis?

A *management overview* would include risk information such as the inherent risk, controls, risk exposure and risk appetite, risk direction and the risk decision made (accept the risk or mitigation action taken). A *risk dashboard* would highlight 'high' risks and any concentration of risks and where they are located. Similar to the Emerging Risk Dashboard reporting the risk dashboards would include comments of the impact of the risk to OSFI and the status of mitigation action undertaken. Such a practice would facilitate a high-level presentation of the condition of risk and mitigation action undertaken at Business / Sub-business lines and Sector levels, making the risk profile of OSFI more transparent.

Recommendation: Risk reporting should be strengthened to include progressively aggregate risk assessment reporting on 'high' risks and concentration of risks at the Business / Sub-Business Line, Sector and aggregate Corporate levels.

Continued on next page

5. Observations and Recommendations, Continued

5.6 Managing risk information

Observation: Managing risk information and reporting is difficult and time consuming

Currently, it is estimated that some individual 200 risk items and some 500 individual mitigation actions are managed and reported in the *Risk Registers*. These volumes with enhanced monitoring and reporting and with the introduction of an internal control structure suggests that an integrated automated ERM system is needed to facilitate recording of risk information, monitoring and reporting at the Business / Sub-Business Line, Sector and Corporate levels.

What is equally important is to have an integrated ERM system that can capture and have access to risk and internal control information, risk assessments, monitor and track mitigation action and the ability to report on risk management across the Office. There would be an important shift of effort from performing maintenance and administrative tasks to focusing on risk management, risk decision making, and reporting at operation and management levels.

The ERM system would have OSFI custom risk and internal control inventories to draw from, enforce OSFI's ERM methodology and process, maintain in-depth risk assessments at multi-levels (Corporate, Sector and Sub-Business Line) and provide a wide variety of risk management reporting capabilities

We encourage the Office in considering the merit of acquiring an integrated ERM system. To have a small footprint on OSFI's IM/IT Strategy an online web-based system could be acquired with the benefit of a specialized dedicated ERM system with both risk management and technical support and a migration to in-house in a future date.

Recommendation: OSFI should consider the merit of acquiring an integrated ERM system to support risk management across the Office.

5.7 Capacity of and Competencies in Risk Management

Observation: Strengthen the capacity of and competencies in risk management across the Office

Strengthening the risk assessment methodology, processes and tools will involve specific risk management training for those responsible and involved in conducting risk assessments as well as for the *Risk Coordinators*.

It is important with the introduction of risk management improvements that the Office determines the competencies and capacities needed for implementing and maintaining risk management and related timelines across the Office.

Due to the effort expected for the implementation of risk management improvements and related training, we believe dedicated risk management resources are needed to lead risk management and implement the improvements in ERM.

Recommendation: The competencies and capacities needed for implementing and maintaining an Office-wide risk management function should be developed.

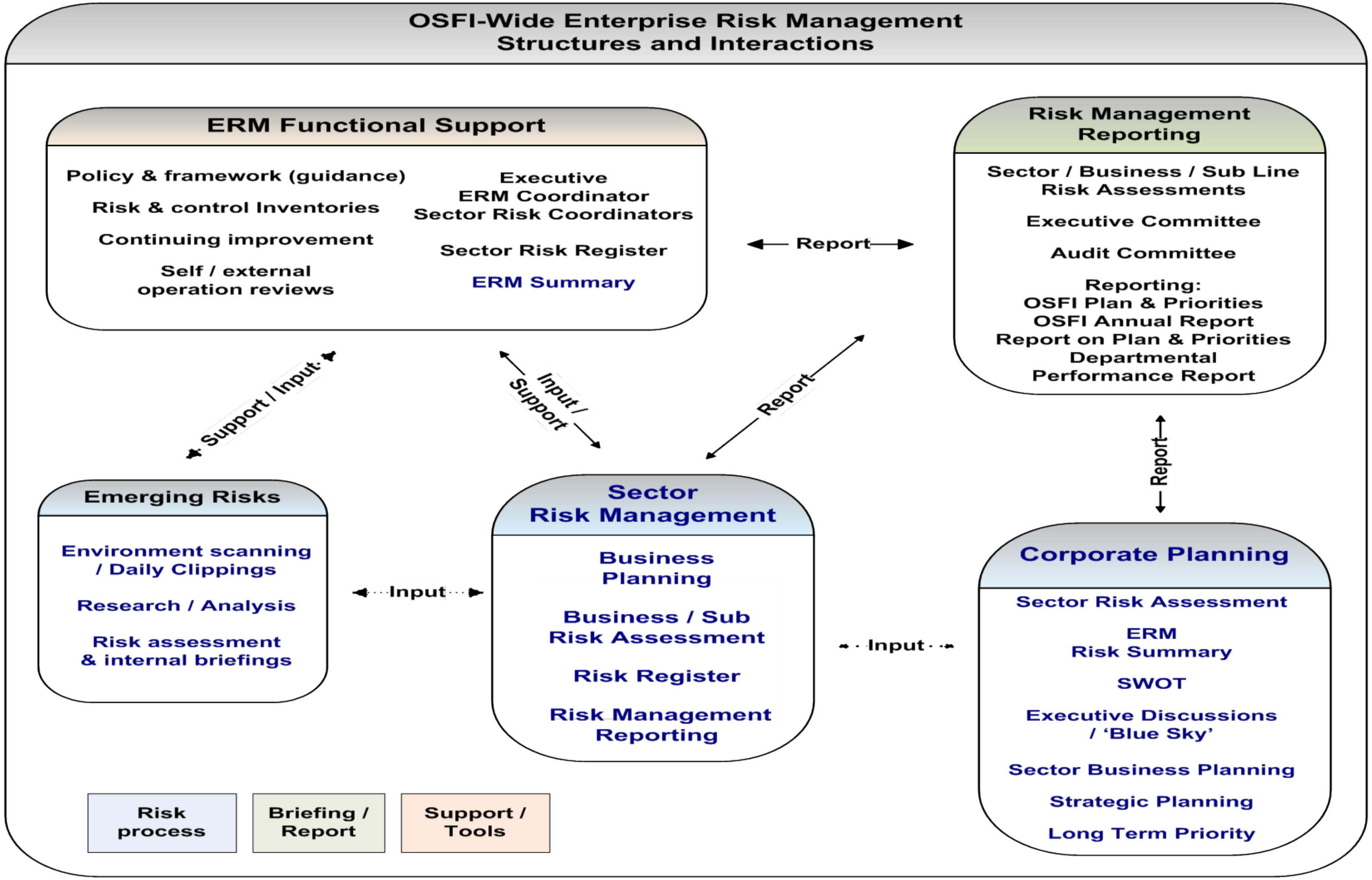
Continued on next page

Appendix A -ERM Control Criteria

Element	Components
Risk Management	▪ *External and internal risk* related to OSFI's ERM function is identified, assessed, mitigation action/controls are in place, consistent with ERM policy ▪ A *structure* exists for monitoring and managing risk /issues as to the comprehensiveness, thoroughness and currency of the ERM function ▪ Senior management has *communicated its views and decisions related to* risk, internal control and risk tolerance
Governance	
Operating Environment	▪ ERM reflects OSFI's *values and a commitment to integrate risk management* into business and corporate planning and operations ▪ *Accountabilities, responsibilities, decision-making and reporting* related to risk management at the Audit Committee, Executive, Corporate and Business levels, monitoring, escalation of risk issues, risk decisions and reporting, are defined and communicated to management and staff ▪ *Resources for* ERM and the Sectors are provided for, aligned with OSFI's corporate risk profile and its plan and priorities ▪ *Technical and competencies*, including required formal and informal training necessary to maintain knowledge levels and needed expertise, are set out
Objective Setting	▪ *ERM policy, objectives, plans, risk and control frameworks, risk methodology(top down, bottom up) are:* ▪ Defined and communicated to management and staff ▪ Align with and support OSFI's objectives (and plan and priorities) ▪ Aligned with OSFI performance reporting ▪ Align with relevant Government policies, directives, standards and guidance ▪ *Risk management and risk tolerance (qualitative/ quantitative) practices* have been established at the Business / Sub-Business Line and aggregate Sector and Corporate level
Information and Communication	▪ *Risk and internal control information requirements*, including risk and internal control structures, inherent risk (impact and likelihood), residual risk and risk tolerance, are defined and incorporated into risk management practices and reporting ▪ *Risk management reporting* is set out and communicated to management and staff as appropriate, including a SWOT analysis, Sector and Business / Sub-Business Line risk assessments (registers), emerging risk, corporate risk summary (dashboard) as well as its incorporation into key documents such as Long-Term Priority, Departmental Plan and Priorities and Annual Report ▪ *Open and timely channels of communication* exist between managers and staff: ▪ To ensure risk and control requirements are communicated ▪ To ensure currency and consistency of communications on risk management and risk decisions made ▪ A '*corporate memory*' is incorporated into ERM processes and maintained through the capture of information pertaining to risk assessments and risk decisions made

Element	Components
Monitoring and Management Reporting	▪ *An ERM continuous improvement process* exists to monitor and report on: ▪ Achieving ERM risk management objectives ▪ Adherence to risk management policy, processes and practices ▪ Adequacy of ERM resources to support risk management ▪ *Management reporting practices and tools* are in place such as risk analysis (impact, likelihood, risk distribution) and risk reporting covering areas such as business objectives at risk, considerations in risk trade-offs and risk decision-making, and mitigating/control actions with target time frames
Control Process	
Process and Control Activities	▪ A *management oversight* process exits over the ERM function ▪ *Processes e*xist that sets out: ▪ Procedures and activity requirements for: ▪ Identification of emerging issues and analysis of relevance to OSFI and risk management ▪ Facilitating Sectors conducting ongoing risk and control assessments ▪ Identifying, assessing, measuring likelihood and impact, prioritizing, risk decision-making, monitoring and reporting on risk and related control/mitigation practices ▪ Alignment of residual risk with respective risk tolerance (risk appetite) ▪ Integration of Sector, corporate planning and emerging risk identification activities and information into OSFI's overall risk management ▪ Process timelines (calendar) and deliverables ▪ *Back-up and continuity plans* of ERM information, supporting aids/tools and staff are in place

Attachment 1: ERM Structures and Interactions



OSFI-Wide Enterprise Risk Management Structures and Interactions

ERM Functional Support

Policy & framework (guidance)

Risk & control Inventories

Continuing improvement

Self / external operation reviews

Executive ERM Coordinator

Sector Risk Coordinators

Sector Risk Register

ERM Summary

Risk Management Reporting

Sector / Business / Sub Line Risk Assessments

Executive Committee

Audit Committee

Reporting:
OSFI Plan & Priorities
OSFI Annual Report
Report on Plan & Priorities
Departmental Performance Report

Emerging Risks

Environment scanning / Daily Clippings

Research / Analysis

Risk assessment & internal briefings

Sector Risk Management

Business Planning

Business / Sub Risk Assessment

Risk Register

Risk Management Reporting

Corporate Planning

Sector Risk Assessment

ERM Risk Summary

SWOT

Executive Discussions / 'Blue Sky'

Sector Business Planning

Strategic Planning

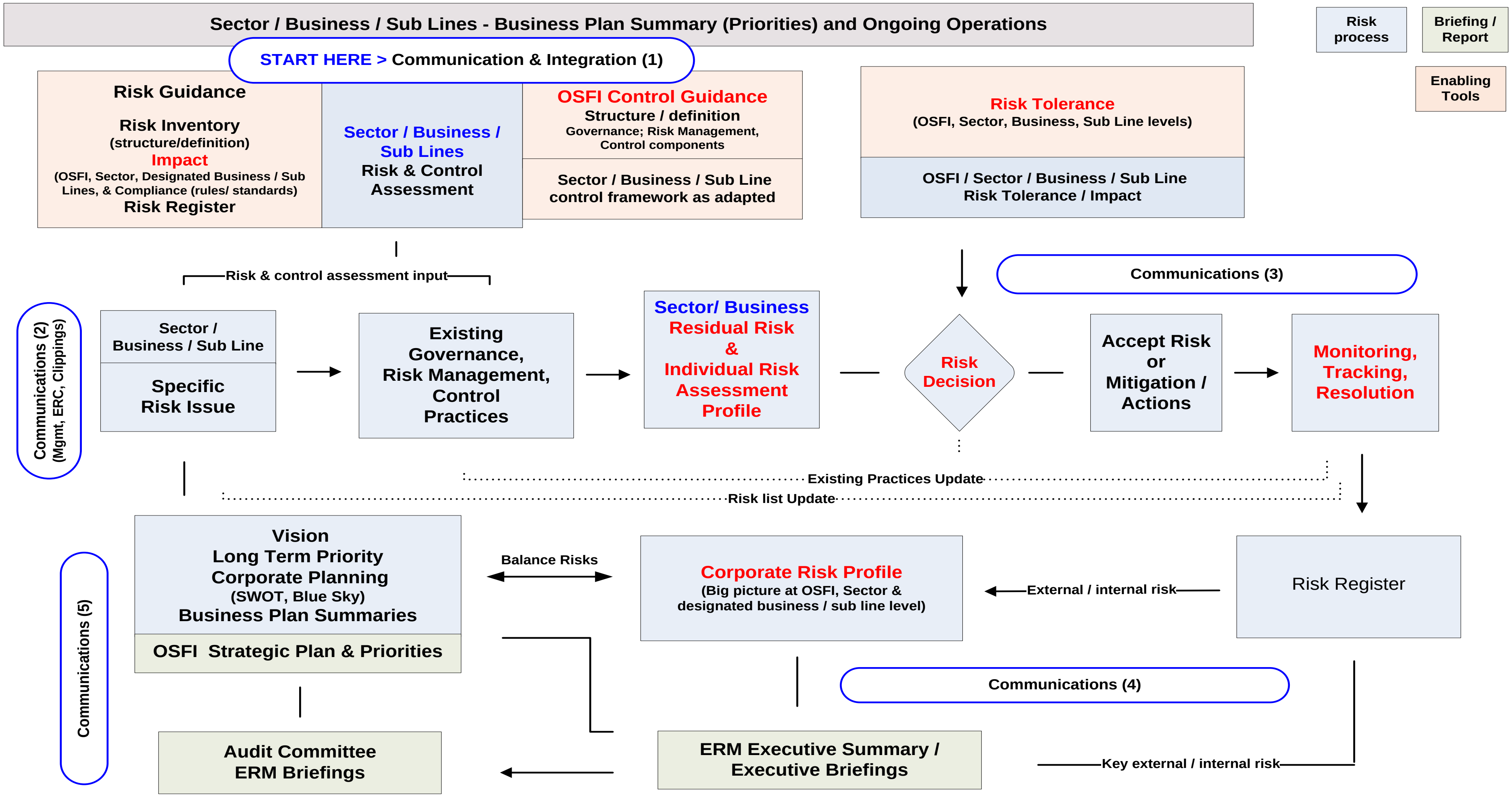
Long Term Priority

Risk process

Briefing / Report

Support / Tools

Attachment 2: Risk Assessment Process


Sector / Business / Sub Lines - Business Plan Summary (Priorities) and Ongoing Operations
Risk process
Briefing / Report
Enabling Tools
START HERE > Communication & Integration (1)
Risk Guidance
Risk Inventory
(structure/definition)
Impact
(OSFI, Sector, Designated Business / Sub Lines, & Compliance (rules/ standards)
Risk Register
Sector / Business / Sub Lines
Risk & Control Assessment
OSFI Control Guidance
Structure / definition
Governance; Risk Management, Control components
Sector / Business / Sub Line control framework as adapted
Risk Tolerance
(OSFI, Sector, Business, Sub Line levels)
OSFI / Sector / Business / Sub Line Risk Tolerance / Impact
Risk & control assessment input
Communications (3)
Communications (2)
(Mgmt, ERC, Clippings)
Sector / Business / Sub Line
Specific Risk Issue
Existing Governance, Risk Management, Control Practices
Sector/ Business Residual Risk & Individual Risk Assessment Profile
Risk Decision
Accept Risk or Mitigation / Actions
Monitoring, Tracking, Resolution
Existing Practices Update
Risk list Update
Vision
Long Term Priority
Corporate Planning
(SWOT, Blue Sky)
Business Plan Summaries
OSFI Strategic Plan & Priorities
Balance Risks
Corporate Risk Profile
(Big picture at OSFI, Sector & designated business / sub line level)
External / internal risk
Risk Register
Communications (5)
Communications (4)
Audit Committee ERM Briefings
ERM Executive Summary / Executive Briefings
Key external / internal risk