Organizational Risk Management for Deposit Insurers

Research Paper

Prepared by the Research and Guidance Committee of the International Association of Deposit Insurers

C/O BANK FOR INTERNATIONAL SETTLEMENTS
CENTRALBAHNPLATZ 2, CH-4002 BASEL, SWITZERLAND
TEL: +41 61 280 9933 FAX: + 41 61 280 9554
WWW.IADI.ORG

TABLE OF CONTENTS

I. Executive Summary

The International Association of Deposit Insurers (IADI) was established in 2002 with a mission to "contribute to the enhancement of deposit insurance effectiveness by promoting guidance and international cooperation." As part of its work, IADI undertakes research and, where appropriate, suggests guidance on deposit insurance issues. The objective of this paper is to review the organizational risk management frameworks and processes currently used by deposit insurers.

All organizations that operate in the public or private sector are confronted with the need to identify, assess, manage, monitor, and report in some manner on the risks to which they are exposed. Likewise, a deposit insurer, irrespective of its mandate (e.g. paybox, loss minimizer), faces risks in connection with the fulfillment of that mandate. These risks typically go beyond those related directly to the failure of a member bank and can include risks stemming from operations and finances.

A. Definitions and Key Elements

To gain a fuller understanding of risk management for deposit insurers, it is helpful to consider the definitions for the following terms, which are used throughout the paper:

- **Risk** can be defined as the possibility of an event impeding a deposit insurer in the fulfillment of its mandate.

- **Organizational risks** can be defined as those risks that derive from a deposit insurer pursuing the fulfillment of its mandate. Organizational risks can relate to the health of the deposit insurer's member banks, to its operations, its financial activities, its reputation, and to other matters.

- **Organizational risk management** can be defined as the process of identifying, assessing, managing, monitoring, and reporting on a deposit insurer's organizational risks. At times in this paper, the term "organizational risk management" has, for the sake of convenience, been shortened to "**risk management**".[1]

- **Significant risks** can be defined as those organizational risks whose likelihood and impact could impede a deposit insurer in the fulfillment of its mandate.

[1] This term could create confusion for some deposit insurers, which use the term "risk management" to refer specifically to the management of risks posed by the insurer's member banks. Where the term "risk management" has been used in this paper, it should be taken to refer to all a deposit insurer's risks, not just those posed by its member banks.

- **Enterprise Risk Management (ERM)** describes a specific framework for organizational risk management. It can be defined as a process, applied on an *enterprise-wide basis*, to ensure and demonstrate that a deposit insurer's significant risks are being consistently and continuously identified, assessed, managed, monitored, and reported on in a *coordinated manner across the organization*.

B. Scope and Purpose

Given the importance of risk management in building an effective deposit insurance system, there is an interest in exploring the various approaches taken by deposit insurers to address the risks they face in their activities. To this end, this research paper describes the different processes which deposit insurers currently use to identify, assess, manage, monitor, and report on the risks to which they are exposed. The paper is directed at countries considering the establishment of a deposit insurance system, or enhancing a system that is already in place.

The paper considers the risk management processes at six deposit insurers, which have formed a subcommittee on organizational risk management ("the Subcommittee") under the auspices of the IADI Research and Guidance Committee. They are: the Federal Deposit Insurance Corporation (FDIC) in the US; the Autorité des marchés financiers (AMF) in Quebec; the Canada Deposit Insurance Corporation (CDIC); the Malaysia Deposit Insurance Corporation (MDIC); the Instituto para la Protección al Ahorro Bancario (IPAB) in Mexico; and the Savings Deposit Insurance Fund (SDIF) in Turkey. These deposit insurers are of differing sizes and structures, with varying mandates, and have adopted (or are in the process of adopting) different approaches for managing their organizational risks.

The intent of this paper is not to issue guidance on organizational risk management or enterprise risk management, specifically. Deposit insurers have only recently begun to adopt various forms of organizational risk management, and it would be premature to write about successes and pitfalls at this time. Rather, the aim of this paper is to provide deposit insurers that wish to develop or enhance their risk management processes with a survey of risk management processes currently being undertaken by other deposit insurers, and to do this in such a manner that the information contained in this paper may be reflective of, and adaptable to, a broad range of circumstances and structures.

C. Summary of Findings

1. In some jurisdictions, deposit insurers are compelled by legislation to implement an organizational risk management process. In others, deposit insurers implement organizational risk management as a prudent business practice.

2. Deposit insurers in the Subcommittee typically have established formal risk management policies at governing body level.

3. Deposit insurers in the Subcommittee typically have established cross-divisional committees for coordinating their respective organizational risk management processes.

4. Deposit insurers in the Subcommittee typically have established processes for initial risk identification and for identifying risks on an ongoing basis thereafter.

5. All deposit insurers in the Subcommittee have defined and categorized risks in a common language across their respective operations.

6. Deposit insurers in the Subcommittee assess the importance of their risks as a function of the likelihood of a risk event, and the potential impact of that risk event, should it occur.

7. Deposit insurers in the Subcommittee typically have established separate policies for different risks.

8. It is typically the case at deposit insurers in the Subcommittee that risks are managed or "owned" by the individuals charged with carrying out and overseeing the relevant operations.

9. Deposit insurers in the Subcommittee typically report on the findings of their risk management processes to senior management, and/or the governing body.

10. A number of deposit insurers in the Subcommittee report on the management of their significant risks to external stakeholders, such as the authority from which the deposit insurer receives its mandate, and the deposit-taking public.

II. Introduction

The International Association of Deposit Insurers (IADI) was established in 2002 with a mission to "contribute to the enhancement of deposit insurance effectiveness by promoting guidance and international cooperation." As part of its work, IADI undertakes research and, where appropriate, suggests guidance on deposit insurance issues. The objective of this paper is to review the organizational risk management frameworks and processes currently used by deposit insurers.

All organizations that operate in the public or private sector are confronted with the need to identify, assess, manage, monitor, and report in some manner on the risks to which they are exposed. Likewise, a deposit insurer, irrespective of its mandate (e.g. paybox, loss minimizer), faces risks in connection with the fulfillment of that mandate. These risks typically go beyond those related directly to the failure of a member bank and can include risks stemming from operations and finances.

Definitions and Key Elements

To gain a fuller understanding of risk management for deposit insurers, it is helpful to consider the definitions for the following terms, which are used throughout the paper:

- **Risk** can be defined as the possibility of an event impeding a deposit insurer in the fulfillment of its mandate.

- **Organizational risks** can be defined as those risks that derive from a deposit insurer pursuing the fulfillment of its mandate. Organizational risks can relate to the health of the deposit insurer's member banks, to its operations, its financial activities, its reputation, and to other matters.

- **Organizational risk management** can be defined as the process of identifying, assessing, managing, monitoring, and reporting on a deposit insurer's organizational risks. At times in this paper, the term "organizational risk management" has, for the sake of convenience, been shortened to "**risk management**".[2]

- **Significant risks** can be defined as those organizational risks whose likelihood and impact could impede a deposit insurer in the fulfillment of its mandate.

[2] This term could create confusion for some deposit insurers, which use the term "risk management" to refer specifically to the management of risks posed by the insurer's member banks. Where the term "risk management" has been used in this paper, it should be taken to refer to all a deposit insurer's risks, not just those posed by its member banks.

- **Enterprise Risk Management (ERM)** describes a specific framework for organizational risk management. It can be defined as a process, applied on an *enterprise-wide basis*, to ensure and demonstrate that a deposit insurer's significant risks are being consistently and continuously identified, assessed, managed, monitored, and reported on in a *coordinated manner across the organization*.

Scope and Purpose

Given the importance of risk management in building an effective deposit insurance system, there is an interest in exploring the various approaches taken by deposit insurers to address the risks they face in their activities. To this end, this research paper describes the different processes which deposit insurers currently use to identify, assess, manage, monitor, and report on the risks to which they are exposed. The paper is directed at countries considering the establishment of a deposit insurance system, or enhancing a system that is already in place.

The paper considers the risk management processes at six deposit insurers, which have formed a subcommittee on organizational risk management ("the Subcommittee") under the auspices of the IADI Research and Guidance Committee. They are: the Federal Deposit Insurance Corporation (FDIC) in the US; the Autorité des marchés financiers (AMF) in Quebec; the Canada Deposit Insurance Corporation (CDIC); the Malaysia Deposit Insurance Corporation (MDIC); the Instituto para la Protección al Ahorro Bancario (IPAB) in Mexico; and the Savings Deposit Insurance Fund (SDIF) in Turkey. These deposit insurers are of differing sizes and structures, with varying mandates, and have adopted (or are in the process of adopting) different approaches for managing their organizational risks.

The intent of this paper is not to issue guidance on organizational risk management or enterprise risk management, specifically. Deposit insurers have only recently begun to adopt various forms of organizational risk management, and it would be premature to write about successes and pitfalls at this time. Rather, the aim of this paper is to provide deposit insurers that wish to develop or enhance their risk management processes with a survey of risk management processes currently being undertaken by other deposit insurers, and to do this in such a manner that the information contained in this paper may be reflective of, and adaptable to, a broad range of circumstances and structures.

III. Rationale for a Risk Management Process

From the standpoint of an organization, an effective risk management framework brings a number of benefits. First and most importantly, a formalized risk management framework can help develop a common understanding of risk across the deposit insurer's operations. That is, a risk decision-taker in one area of an insurer's operations is aware of the risk implications of his or her decisions for other aspects of the deposit insurer's operations. In addition, a formalized risk management framework can facilitate the development of a common risk lexicon, ensure that risks are being identified and that appropriate timely action is being taken to address them, and prioritize risks such that resources can be allocated to the risks that are considered most significant. From a governance perspective, risk management has increasingly become an expectation, in that it provides reassurance to the deposit insurer's governing body, to the authority from which the deposit insurer receives its mandate, and to the deposit-taking public that the deposit insurer is aware of the risks to which it is exposed and that it has a framework in place to monitor and manage those risks. Importantly, an organizational risk management framework can also cast light on areas where the deposit insurer must manage its risks better.

There are, however, some notable drawbacks to organizational risk management. It can require time from senior management, taking them away from their day-to-day responsibilities. And a framework that is poorly designed for the deposit insurer's size, mandate, and structure can create the potential for unnecessary reporting and red tape. Deposit insurers seeking to develop an organizational risk management framework should consider the framework's efficiency along with its effectiveness.

IV. Establishing a Risk Management Framework

Organizational risk management is increasingly viewed by international organizations, financial institutions, private-sector organizations, and think tanks as a prudent business practice.[3] Being aware of organizational risks,

[3] In Section 5, E(5) of its *Guidelines on corporate governance of state-owned enterprises*, the Organisation for Economic Co-operation and Development calls upon state-owned enterprises, which include many deposit insurers, to "disclose material information on all matters described in the OECD Principles of Corporate Governance and in addition focus on areas of significant concern for the state as an owner and the general public. Examples of this information include [*inter alia*]: any material risk factors and measures taken to manage such risks." In the private sector, financial institutions, such as banks and insurance companies, have been leading the way in risk management development. In the US, compliance requirements in respect of Section 404 of the Sarbanes-Oxley Act have also led to the development of internal control procedures, with which all US-listed companies must comply. These internal control procedures are similar to those that make up an effective organisational risk management framework. In fact, one can make the point that an internal control framework is encompassed within and is an integral part of organizational risk management.

being able to set tolerances for those risks and manage risks within those tolerances, and being able to leverage risk opportunities, where possible, represent some of the benefits of an effective risk management process. Also, in some jurisdictions the implementation of a risk management process is a compliance requirement for deposit insurers. This requirement can come in the form of legislation, guidelines, or other external means.

In Mexico, IPAB is required by regulation to identify, assess, and manage any risk that could impair the achievement of its objectives.[4] In Canada, CDIC is not called upon by statute or regulation to implement a risk management process, but takes guidance from the Treasury Board Secretariat – the country's federal central agency governing public sector entities – which recommends that government organizations identify, assess, manage, and report on their risks. In the US, the FDIC's assessment of its external risks (see section on "Risk Identification" below) is rooted legally in its Congressional requirement to examine and rate insured banks every 12 to 18 months. The SDIF has issued a bylaw, under which it is required to implement an organizational risk management process. Neither the AMF nor the MDIC are required by outside authorities to implement a risk management system, but both do so as a matter of good business practice.

For the majority of deposit insurers studied in this paper, the deposit insurer's governing body has established a formal policy setting out its expectations regarding the risk management process. The FDIC, MDIC, CDIC and IPAB all have governing body-level policies in place covering each organization's risk management process. CDIC's policy, for example, calls upon management to do the following: identify and assess the insurer's significant risks; assist the governing body in understanding those risks and the ways in which they can be managed; propose risk management policies to the governing body; review those policies on an annual basis; manage significant risks in accordance with the governing body's risk management policies; and provide the governing body with reports to enable it to assess whether the deposit insurer has an effective risk management process in place.

A risk management policy at governing body level can formalize the governing body's responsibility for directing and overseeing the deposit insurer's management of its risks. It can also make clear the roles assigned to management and the governing body in the process.

The types of risk management frameworks implemented by Subcommittee members reflect the size and complexity of each member's operations. A risk management framework can be structured so as to minimize unnecessary costs and reduce bureaucracy. CDIC, for example, an organization of roughly 80 people, has one full-time dedicated individual responsible for coordinating its enterprise risk management system. At other,

[4] The regulation is issued by the Mexican Civil Service Department.

larger deposit insurers, the number of employees required to coordinate and administer the risk management system might be greater, but it is helpful to have a risk management coordination function which seeks to minimize the burden placed on those individuals actually responsible for taking risk decisions.

IPAB, CDIC, MDIC, and the FDIC have all established cross-divisional committees for coordinating their organizational risk management processes. Such committees typically meet on a regular basis to permit members to discuss the key risks facing their respective operations. This type of committee can serve to disseminate risk information and help create a common risk understanding and lexicon across the organization.

V. Risk Identification

In any risk management program, it is essential for an organization to know what its risks are. Deposit insurers such as the FDIC, IPAB, MDIC and CDIC have developed formal processes for identifying key risks.

The FDIC has divided its risks into external risks and internal risks. External risks (i.e. risks to FDIC members) are identified by the Division of Supervision and Consumer Protection, the Division of Insurance and Research, and the Division of Resolutions and Receiverships, and aggregated across divisions by interdivisional risk committees. External risks include: credit risk, market risk, interest rate risk, and operational risk (including compliance risk, internal control risk, fraud risk, corporate governance risk, information technology risk, and environmental risk). Internal risks (i.e. risks to FDIC operations) are identified by the FDIC's Office of Enterprise Risk Management. The Office of Enterprise Risk Management has identified risks relating to the implementation of statutory deposit insurance reforms, privacy issues, information security, contract administration, continuity of operations, and consumer protection issues.

In Mexico, risks are identified by business units through analysis of IPAB's processes and activities. The Risk Management Unit is in charge of assisting business units in the identification process. IPAB has identified risks relating to: the monitoring of and intervention into banks; markets; assets and liabilities; liquidity; credit; personnel; internal relationships; relationships with third parties; systems; technology; process; facilities and premises; and external events.

In Canada, key risks are identified by business units and aggregated by CDIC's Enterprise Risk Management Committee (a committee composed of the Chief Executive Officer and senior management). CDIC identifies risks relating to its insurance powers (i.e. the risk of a misalignment between its statutory objectives and the powers it has to carry out those objectives),

assessment, intervention, liquidity, market, credit, people, information, technology, processes, compliance, business continuity planning, security, and reputation.

In Turkey, the SDIF has created a working group comprising a representative from each department. The group has identified numerous risks for the various departments, and then developed a number of broad risk categories (see Appendix I). Among other things, it has identified risks relating to on- and off-balance sheet assets and liabilities of the SDIF; interest rate risk; exchange rate risk; intervention risk; staff-related risks; process risk; technology risk; reputation risk; risks from potential terrorism or economic or political instability; risks arising out of a misalignment between the SDIF's legal mandate and its operations; and contract risk.

In Quebec, the AMF has identified risks relating to insurance powers, licensing, assessment, intervention, finances, treasury, human resources, availability and timeliness of information, technology, compliance, outsourcing, business continuity, confidentiality of information, external communication, and external relationships.

Risk identification does not imply that a deposit insurer needs to assess, develop management policies for, and report on every risk it faces. In all cases, members of the Subcommittee focussed on risks that were significant to the fulfillment of their mandates.

Of course, operating environments for deposit insurers are by no means static. The Subcommittee members have, therefore, found it helpful to seek to identify potential new risks on an ongoing basis. For example, CDIC and MDIC conduct annual environmental scans, which consider emerging internal and external issues that could impact their operations going forward. IPAB and MDIC also carry out quarterly reviews in order to identify potential new significant risks. IPAB seeks to identify new risks whenever new activities are undertaken.

A key benefit of a risk management process, at any organization, is that it can instill an awareness of risk into the organization's strategic and operational decision-making, such that a risk decision-maker in one division of an organization is aware of the risks facing other operations in the organization, and the effect that his or her decision could have on those operations. To this end, members of the Subcommittee have found it helpful to define and categorize risks in a language that is common across all the deposit insurer's operations.

For example, CDIC, MDIC and the AMF have assigned their risks to broad risk categories, such as deposit insurance risk, financial risk,

operational risk, and reputation risk.[5] IPAB has the following risk categories: deposit insurance risk, financial risk, and operational risk. The SDIF has financial risk, strategic risk, external risk, and legal risk. The FDIC has divided its risks into internal risks, which affect its own operations, and external risks, which affect the health of FDIC-insured banks (and hence the FDIC's own insurance risk exposure).

VI. Risk Assessment

Having identified and categorized the risks they face, members of the Subcommittee typically assess the importance of those risks. One approach used to evaluate the importance of a risk event is to determine the likelihood of a given risk event and its potential impact, should it occur. Hence, risks with a high impact and high likelihood of occurrence would be an organization's most important risks; while risks with a low impact and/or low likelihood of occurrence would be its least significant risks. IPAB, for example, divides its risks into immediate-attention risks (i.e. risks that are frequent and have high impact, the occurrence of which could impair IPAB's ability to achieve its statutory objectives or corporate plan); continual-attention risks (i.e. risks that are frequent but have low impact, the occurrence of which could delay the accomplishment of goals); follow-up risks (i.e. risks that are not frequent but have high impact, the occurrence of which will have some effect on goals); and risks under control (i.e. risks that are not frequent and have low impact, the occurrence of which might delay the accomplishment of goals). CDIC divides risks into high-, medium-, or low-impact and likelihood. It defines high-impact risks as those that could inflict a financial loss of at least 10 times CDIC's financial materiality threshold, cause a long-term loss of CDIC's reputation, or seriously impair CDIC's ability to achieve its statutory objectives or corporate plan. It defines high-likelihood risks as risk events likely to occur at least once in the next fiscal year.

There is a certain amount of theoretical debate among risk management practitioners as to whether assessments of an organization's risks should be conducted in a top-down or bottom-up manner. Arguments

[5] IPAB and CDIC have very similar definitions for deposit insurance risk, financial risk, and operational risk:

IPAB uses the following definitions: deposit insurance risk – risk arising from IPAB's role as a deposit insurer and from the possibility of bank failure; financial risk – risk associated with the management of IPAB assets and liabilities, both on- and off-balance sheet; and operational risk – risk of exposure attributed to the possibility of inadequate or failed internal process, people and systems, or external events.

CDIC uses the following definitions: insurance risk – risk of loss, including costs incurred in the event of an intervention, associated with insuring deposits; financial risk – risk associated with managing CDIC's assets and liabilities, both on- and off-balance sheet; operational risk – CDIC's risk of loss resulting from inadequate or failed internal processes, people, and systems, or from external events; reputational risk – risk of an event significantly affecting stakeholders' perceived trust and confidence in CDIC, and which could result in a financial or other loss to CDIC.

can be made for both approaches. In reality, most of the deposit insurers in the Subcommittee use a combination of both approaches.

A top-down method envisions risk identification and assessment being undertaken by senior managers. Senior managers have the advantage of being able to take a high-level view of the deposit insurer's operations. That is, they might be better able to "see the forest for the trees", and thereby understand better the relative importance of risks in a given business line against the risks the organization faces as a whole. This process also could yield opportunities for risk leveraging and reducing the amount of resources expended on risks that are deemed to be less important. Top-down risk assessment can be particularly powerful at small deposit insurers, where senior managers have a hands-on knowledge of what all the employees within their respective reporting streams are doing at a given time.

At larger organizations, where a senior manager might not reasonably be expected to have a hands-on knowledge of work being done by everyone within his or her chain of command, a top-down approach might be less effective. An upward flow of risk information might be more helpful, by providing the senior manager who takes the risk decisions with the confidence that risks have been assessed thoroughly at each step up the chain. Also, a bottom-up risk assessment process involves more junior staff in the risk management process than might be the case with a top-down process, thereby heightening the importance of risk management throughout all levels of the organization. One drawback to a bottom-up process is that, while more thorough, it could prove more costly than a top-down method. Risk aggregation at lower levels within the organization also creates the potential for incorrect prioritization of risks by more junior employees, who might not be able to achieve a high-level view of the insurer's operations.

VII. Risk Management

The members of the Subcommittee have all established risk management policies for their respective deposit insurers. The specific policies for managing significant risks vary from deposit insurer to deposit insurer, depending on the organization's mandate and risk tolerances.

At the FDIC, the National Risk Committee, which is composed of senior officials, is charged with coordinating responses to external risks, including strategies for FDIC-supervised and FDIC-insured institutions. IPAB has separate policies for deposit insurance risks, financial risks, and operational risks. Business units are called upon quarterly to analyze their processes and activities in order to evaluate their risks, disclose new risks, and assess the effectiveness of controls for existing risks. If necessary, additional adjustments are approved by the Risk Committee.

MDIC has a broad formal policy at Board level, which specifies that the Board will: obtain an understanding of the principal risks of the corporation's business; ensure that appropriate and prudent risk management systems have been implemented, and review systems and policies regularly; and obtain reasonable assurance, on a regular basis, that systems and policies are being adhered to and continue to effectively manage the risks affecting the Corporation. MDIC's Audit Committee is required to meet a number of other requirements imposed by its charter, specifically in respect of its risk management process, and MDIC also has in place an ERM Charter which sets out the accountability, responsibility, independence and authority of the Chief Risk Officer and ERM function. In addition, MDIC has established an enterprise risk management committee made up of senior management. The aim of the committee is to champion and oversee enterprise risk management implementation across MDIC, and manage and monitor risk exposures and ERM activities. The strategic planning and enterprise risk management working committee helps the enterprise risk management committee to facilitate and coordinate all ERM activities at operational level. This allows MDIC to manage risks using both top-down and bottom-up approaches.

CDIC has a Board-level risk management policy very similar to that at MDIC. This policy also sets out the board's expectations of management as regards enterprise risk management: CDIC's Board policy calls upon management to identify and assess the significance of the risks attendant upon CDIC's mandate, objectives, strategies, plans, and operations; recommend risk management policies to the Board; review those policies at least annually; manage risks in accordance with those policies; and provide the Board with timely, relevant, accurate, and complete reports at least annually, and as otherwise required. CDIC has specific policies in place governing each of its significant risks. CDIC also has an enterprise risk management committee comprising senior management.

The AMF has developed policies at business unit level on insurance risk, intervention risk, financial risk, human resources risk, technology risk, externalization risk, business continuity risk, and security risk.

While all the Subcommittee members have charged an individual (e.g. Chief Risk Officer) or team of individuals (e.g. risk committee) with coordinating the deposit insurer's risk management framework, in general risks are managed or "owned" by the individuals charged with carrying out and overseeing the related operations.

VIII. Risk Monitoring and Reporting

Having identified, assessed, and taken steps to manage the significant risks to which they are exposed, deposit insurers in the Subcommittee then

typically report on their findings: internally, to senior management and the governing body, where applicable; and externally to stakeholders, including the authority from which the deposit insurer receives its mandate, and the deposit-taking public.

Internal Reporting

Reporting to senior management and the governing body could take the form of a document that sets out the deposit insurer's risks, draws conclusions on their significance, and describes the steps being taken to manage them. The FDIC, for example, provides an assessment of its external risks to its Board of Directors on a semi-annual basis. In addition, each Divisional and Office Director of the FDIC is required to provide the Chairman of the Board with an assurance statement on the adequacy of the internal, management, and financial system controls for his or her respective operations. In Quebec, the AMF receives a monthly report on the status of its fund – the management of which it outsources according to its enabling Law — and a Report and Monitoring Committee reports every three months on internal processes and activities, and progress made toward implementing the organization's strategic plan. At IPAB, the Risk Committee meets regularly to analyze reports on the assessment of risks and their controls. In turn, the Risk Committee reports the most significant risks to the Internal Audit unit, while keeping the Board of Directors informed. At MDIC, the Chief Risk Officer submits an ERM report to the audit committee and the Board of Directors annually. The report includes a review of risk criteria, risk management policies, key changes in business environment, changes of existing risk ratings, new risks identified, and state of completion of mitigation plans, as well as updated risk profiles, risk ratings, and corresponding mitigation plans. In addition, the Chief Risk Officer regularly updates the Board of Directors on risk related matters and ERM activities and is required to report at all Audit Committee meetings. At CDIC, management provides the Board of Directors with an annual ERM report that presents CDIC's significant risks and management's assessment of those risks. The report to the Board sets out the work carried out by management during the past year, the results (including a summary for each risk that sets out the prior year's risk rating and trend, the current environment related to the risk, and management's current risk rating and trend assessments), and recommended new or amended Board risk policies. CDIC's management supports its annual reporting to its Board of Directors with a document, signed by the CEO and chair of the enterprise risk management committee, which attests to management's ERM process and results.

External Reporting

In keeping with the principle of transparency and so as to create the proper external incentives to manage risks, a number of deposit insurers also report on the management of their significant risks to external stakeholders,

such as the authority from which the deposit insurer receives its mandate, and the deposit-taking public.

Members of the Subcommittee report their risks to the public in a number of different ways. The FDIC produces a semi-annual external risk assessment, which is released to the public and posted on the FDIC website. Once a year, IPAB must present a formal and detailed report on its risk management process to the board of directors and to the Mexican Civil Service Department. IPAB also provides a general assessment of its risk management strategy and policies to rating agencies in order to comply with its credit assessment process. MDIC publishes the analysis of its significant risks in both its corporate plan and annual report. This links the ERM process with exercises, enabling management to prioritize and align corporate initiatives by addressing significant risks. In Canada, CDIC reports on its ERM process, its significant risks, the way those risks are managed, and its assessment of those risks in its annual report. Also, as part of its annual reporting, it publishes a document, signed by the CEO and chair of its ERM committee, which attests to management's ERM process and results.

IX. Summary of Findings

1. In some jurisdictions, deposit insurers are compelled by legislation to implement an organizational risk management process. In others, deposit insurers implement organizational risk management as a prudent business practice.

2. Deposit insurers in the Subcommittee typically have established formal risk management policies at governing body level.

3. Deposit insurers in the Subcommittee typically have established cross-divisional committees for coordinating their respective organizational risk management processes.

4. Deposit insurers in the Subcommittee typically have established processes for initial risk identification, and for identifying risks on an ongoing basis thereafter.

5. All deposit insurers in the Subcommittee have defined and categorized risks in a common language across their respective operations.

6. Deposit insurers in the Subcommittee assess the importance of their risks as a function of the likelihood of a risk event, and the potential impact of that risk event, should it occur.

7. Deposit insurers in the Subcommittee typically have established separate policies for different risks.

8. It is typically the case at deposit insurers in the Subcommittee that risks are managed or "owned" by the individuals charged with carrying out and overseeing the relevant operations.

9. Deposit insurers in the Subcommittee typically report on the findings of their risk management processes to senior management, and/or the governing body.

10. A number of deposit insurers in the Subcommittee report on the management of their significant risks to external stakeholders, such as the authority from which the deposit insurer receives its mandate, and the deposit-taking public.

References

1. The Conference Board. *Emerging governance practices in enterprise risk management*. New York: The Conference Board; 2007.

2. Economist Intelligence Unit. *Best practice in risk management: a function comes of age*. London and New York: The Economist Intelligence Unit, Ltd; 2007.

3. Institute of Management Accountants. *Enterprise risk management; tools and techniques for effective implementation*. Montvale (New Jersey): Institute of Management Accountants; 2007.

4. James Lam and Associates. *Emerging best practices in developing key risk indicators and ERM reporting*. Boston: James Lam and Associates; 2006.

5. OECD. *OECD Guidelines on corporate governance of state-owned enterprises*. Paris: OECD Publishing; 2005.

Appendix: Complete Submissions of Subcommittee Members

Federal Deposit Insurance Corporation (USA)

Background Information:

1. **In which year was your deposit insurer established?**
   1933

2. **How many individuals does your deposit insurer employ?**
   4,475 as of 2/28/07

3. **Does your deposit insurer have in place a formal process to identify and evaluate (impact and likelihood) of significant risks?**

   a) Yes

   If yes, how regularly is this process carried out?

   The FDIC's process of identifying and evaluating (impact and likelihood) of significant risks is ongoing, and certain activities that are a part of the process take place at regular intervals.

4. **Does your deposit insurer have a committee(s) (at the management or governing body level) responsible for directing and coordinating risk management activities?**

   a) Yes, the FDIC's National Risk Committee

Risk Identification

1. **Does the deposit insurer employ a process for identifying risks related to the fulfilment of its mandate (including risks stemming from the conduct of its operations)?**

Yes. The FDIC has extensive processes for identifying risks related to its mission, which is to "promote[s] the safety and soundness of insured depository institutions and the U.S. financial system by identifying, monitoring and addressing risks to the deposit insurance funds."

The FDIC's external risk assessment activities rely on each of the FDIC's three "driver" divisions -- the Division of Supervision and Consumer Protection (DSC), the Division of Insurance and Research (DIR), and the

Division of Resolutions and Receiverships (DRR). Each of these driver divisions has extensive systems, personnel structures, and reporting mechanisms to monitor and analyze different aspects of major business risks facing the banking industry. Since external risks may overlap divisional responsibilities, the FDIC relies on its supervisory examination program as well as a series of interdivisional risk management committees to maximize the interdivisional coordination of risk management activities through the agency.

The FDIC also has a process for identifying internal risks to the agency. These activities are conducted by the FDIC's Office of Enterprise Risk Management (OERM). OERM conducts studies and evaluations of selected programs, making appropriate recommendations to improve their operational effectiveness and monitoring the implementation of accepted recommendations. OERM reviews the results of studies and evaluations undertaken by other independent organizations, such as the U.S. Government Accountability Office (GAO) and the Office of the Inspector General (OIG). OERM also reviews the results of the divisions' program and evaluation studies to identify key recommendations and monitor the implementation of accepted recommendations. In some cases, OERM partners with the divisions to conduct joint program evaluations.

If yes,

2. Please list and define the risks that the deposit insurer has identified.

The list of external risks that the FDIC identifies and monitors changes over time. The following are some of the types of risks that have been identified and monitored by the FDIC. These risk assessments are rolled up and reported on to senior management through interdivisional risk management committees: Credit Risk, Market Risk, Interest Rate Risk, Operational Risk (including Compliance Risk, Internal Control Risk, Fraud Risk, Corporate Governance Risk, Information Technology Risk, Environmental Risk, Regulatory/Legal Risk), and other risks.

Several examples of identified internal risks currently being addressed consist of : implementation of Deposit Insurance Reform, privacy issues, security controls over FDIC's information security programs, contract administration (acquisition workforce planning, acquisition procedures, administration of contracts, contract management systems), continuity of operations, and consumer protection issues.

3. Please describe the process that the deposit insurer initially followed to identify these risks.

The external risks identified and monitored at the FDIC have evolved over time and change as market conditions and industry evolution and trends

dictate. As with external risks, the internal risk assessment process also has evolved over time and has migrated from an extensive focus on targeted audit functions to a collaborative risk assessment process and Enterprise Risk Management focus.

4. **Please describe the process (including the frequency that the process is applied) that the deposit insurer follows to identify potential new risks and changes to existing risks.**

The FDIC relies on its ongoing supervisory examination process and its interdivisional risk management committees, which meet regularly, to identify emerging risks. These processes ensure the identification of potential new risks and changes to existing risks in a timely manner.

With respect to internal risks, OERM requires FDIC divisions and offices to implement a risk management program to support managers in reaching program goals and objectives, and in using resources efficiently and effectively. The programs are designed to be cost-effective, flexible and integral to the FDIC's cycle of planning, budgeting, management, accounting, and auditing. All systems of management and accounting controls are evaluated on an on-going basis, and deficiencies, when detected, are corrected promptly.

Risk Assessment

5. **Please describe the criteria used by the deposit insurer to assess the importance (significance) of its risks.**

FDIC risk committees consider a wide range of risk factors, including economic conditions and trends, credit risk, market risk and operational risk, as a prelude to identifying a level of concern, a level of exposure, and supervisory strategy. Strategy options include such tools as publishing research or circulating relevant information to the banking community, making the factor a priority in on-site examinations, or highlighting the factor for off-site monitoring activities.

Risk Management

6. **Does the deposit insurer have formal policies in place governing the management of its risks? If yes, Please describe the nature of the content of these policies (i.e. Do they address how each risk is to be managed and who is responsible for managing each risk).**

Yes, the National Risk Committee, comprised of senior FDIC officials, identifies and evaluates the most significant external business risks facing FDIC and the banking industry. Also, where necessary, the committee

develops a coordinated response to these risks, including strategies for both FDIC-supervised and FDIC-insured institutions. Among other things, the National Risk Committee assembles the Regional Risk Committee reports into a consolidated national risk assessment. The National Risk Committee also receives reports and analyses from the Risk Analysis Center, an interdivisional forum for discussing significant, cross-divisional, risk-related issues.

Risk Monitoring and Reporting

7. Please describe the nature and frequency of any monitoring and internal reports that the deposit insurer makes to its senior management and/or to its governing body about the insurer's risks (including the nature and frequency of any formal sign-off by senior management of the deposit insurer respecting the content of the risk reports).

A Risk Case representing a thorough assessment of the external risks faced by the agency is developed and presented to the FDIC Board of Directors twice a year. In addition, the various interdivisional risk management committees each report regularly to senior management and to the Board of Directors on activities undertaken and risk assessments and findings. More frequent reporting takes place on an as needed basis. Periodically, presentations are made to the FDIC Audit Committee on the internal control process, audit follow-up and resolution, and point-in-time issues. Internal review and audit results are presented to management when completed on a continual basis. Annually, Division/Office directors are required to provide the FDIC Chairman an assurance statement on the adequacy of internal, management, and financial systems controls for their Division/Office operations. The statement considers the Division's/Office's overall activities in conjunction with the results of management's on-going evaluations of internal control operations, programs, and systems along with audits and reviews conducted by the FDIC OIG, GAO, or other external firms.

8. Please describe the nature and frequency of any reports that the deposit insurer makes to external stakeholders about the deposit insurer's risks (including the nature and frequency of any formal sign-off by the deposit insurer respecting the content of the risk reports).

The Risk Case, which represents the agency's biannual external risk assessment, is released to the public and posted on the agency website. With respect to internal risks, the FDIC submits an Annual Report to the President of the United States, the President of the U.S. Senate, and the Speaker of the U.S. House of Representatives in accordance with: the provisions of section 17(a) of the Federal Deposit Insurance Act, the Chief Financial Officers Act of 1990, Public Law 101-576, the Government

Performance and Results Act of 1993, the provisions of Section 5 (as amended) of the Inspector General Act of 1978, and the Reports Consolidation Act of 2000. The FDIC also annually prepares and publishes FDIC's Corporate Annual Performance Plan that sets out specific annual performance goals, indicators and targets for each of FDIC's three major business lines – Insurance, Supervision, and Receivership Management. The Annual Performance Plan is driven by the Mission and Strategic Goals outlined in FDIC's Strategic Plan.

Risk Governance

9. Is the deposit insurer called upon by legislation, regulation, guidelines or other external means within its jurisdiction to implement a process for identifying, assessing, managing, monitoring and reporting on its risks? If yes, Please describe these externally imposed requirements.

On-site examination is the core of the FDIC's risk management activities. Each insured institution is examined and rated every 12-18 months, as required by Congress. Periodic on-site examination provides the best means of determining an institution's financial condition as well as its adherence to laws and regulations.

10. Has the deposit insurer's governing body formalized its expectations respecting the implementation of a process for identifying, assessing, managing, monitoring and reporting on its risks? If yes, please describe these expectations and how have they been communicated to the deposit insurer.

The roles and responsibilities of Divisions and Offices are included in the FDIC By-Laws that have been adopted by the FDIC Board of Directors.

11. Has the deposit insurer dedicated an individual, or a team of individuals, to implement and coordinate the process for identifying, assessing, managing, monitoring and reporting on its risks? If yes, please describe the specific responsibilities assigned and who has been assigned these responsibilities.

Yes. As mentioned above, to identify, monitor, and assess external risk, the FDIC relies on its supervisory examination program as well as a series of interdivisional risk management committees to maximize the interdivisional coordination of risk management activities through the agency. These include the following:

- National Risk Committee (NRC): The NRC identifies and evaluates the most significant external business risks facing the FDIC and the banking industry and, where necessary, develops a coordinated response to these risks, including appropriate policies and

operating strategies with regards to FDIC supervised and insured institutions. The NRC is composed of senior executives in the agency and meets once per month or more often as necessary.

- Risk Analysis Center (RAC): The RAC reports to the NRC and is an interdivisional forum charged with coordinating risk identification and prioritization processes of the three driver divisions: DSC, DIR, and DRR. It provides real-time monitoring of identified and emerging risks and serves as a clearinghouse for risk-related information and as a command center during crisis situations. The RAC is managed by a team of senior officials from DSC, DIR, and DRR and meets on an as needed basis.
- Financial Risk Committee (FRC): The FRC is responsible for recommending the appropriate contingent loss reserve (CLR) for the Deposit Insurance Fund (DIF) on a quarterly basis. The CLR is the FRC's estimate of the FDIC's probable losses attributable to failures of FDIC-insured institutions in the coming 12 months. The FRC consists of senior level FDIC representatives from DIR, DSC, DRR, and the Division of Finance (DOF). The FRC recommends a CLR to the Chief Financial Officer.
- Regional Risk Committees (RRC): RRCs operate in each of the FDIC's six regions and identify and assess existing and emerging risks and determine whether any actions need to be taken in response to those trends and risks. The RRCs convey findings to headquarters, senior management through the RAC and NRC. The RRCs meet and report findings to the RAC and NRC twice a year.
- Resolutions Policy Committee (RPC): The RPC was created to ensure that the FDIC achieves a maximum state of readiness to deal with the potential or actual failure of the Nation's largest insured depository institutions. The RPC is composed of senior executives of the agency and meets monthly.

With respect to internal risks, OERM was created to administer the FDIC Enterprise Risk Management Program that monitors and manages risks, addresses internal control deficiencies, conducts program evaluations of the Corporation's major business lines, and conducts Corporate internal control reviews; provide staff support to the FDIC Audit Committee and handle special projects assigned by the Committee; serve as liaison to the Office of the Inspector General and the Government Accountability Office staff working on audits of Corporate operations; and to oversee audit follow-up and resolution activities.

L'Autorité des marchés financiers (Québec)

Context:

Before beginning to answer the questionnaire, we think it is important to put in context the deposit insurance function of the AMF within the AMF itself as an integrated regulator.

The AMF was created by the merging of five organizations, notably the Quebec Securities Commissions (CVMQ), the Inspector General of Financial Institutions (IGIF), the Financial Services Office (BSF), the Québec Deposit Insurance Board (RADQ) and the Financial Services Compensation Fund (FISF). When merging together those organizations under the same roof and the same name into a regulatory organization, the AMF integrated their functions into seven branches, including four directorates. One of these, Consumer Assistance and Compensation, assists and compensates consumers of financial products and services and administers the funds of the deposit insurance program, among others.

In order to avoid any complications, this text will use the terms Organization and DIF. The former refers to the Financial Market Authority (AMF in French) as a whole while the latter refers to the Deposit Insurance program of the AMF. This emphasis on the word "program" is due to the fact that the AMF is now an integrated regulator with many programs and that the DIF is no longer a legal person. Rather, the DIF is run by the Compensation Division with the help of other divisions, including the Directorate of Solvency notably for the standard aspect and the surveillance of the financial institutions.

Background Information:

1. **In which year was your deposit insurer established?**
   In 1967

2. **How many individuals does your deposit insurer employ?**
   15 .

3. **Does your deposit insurer have in place a formal process to identify and evaluate (impact and likelihood) of significant risks?**

   a) Yes
   b) **Yes, but the process is still in development**
   c) No

   If yes, how regularly is this process carried out?
   ——————————————

4. **Does your deposit insurer have a committee(s) (at the management or governing body level) responsible for directing and coordinating risk management activities?**

   a) Yes
   b) **Yes, but the roles and responsibilities of the committee are not formalized**
   c) No

Risk Identification

1. **Does the deposit insurer employ a process for identifying risks related to the fulfillment of its mandate (including risks stemming from the conduct of operations)?**

   Over the course of the years, the DIF has established different policies and processes that directly or indirectly deal with risks, that identify those risks, and that aim at mitigating them. Those policies will be integrated to the risk management system of the Organization.

2. **Please list and define the risks that the deposit insurer has identified.**

The DIF does deal with risks and manage them as part of our day-to-day operations. By looking at the different processes, programs and policies we have in place, we were able to discern some of the specific risks we manage.

- The Organization manages the Deposit insurance fund and has to be sure that it is has the capacity to manage its insurance risks and that it has the power to intervene in the event of a crisis.
- Every time the Directorate of Solvency processes new licenses, it needs to be certain of the financial soundness of the candidate institution in order not to face potential problems.
- With almost 600 credit unions and banking institutions in Québec, the Directorate of Solvency has the obligation to closely inspect every 12 months and monitor periodically all institutions, so that potential problems can be detected in advance and problematic institutions dealt with without occurring losses
- Since institutions can become insolvent or have financial problems that threaten the stability of the financial system, the DIF needs to be ready to intervene directly. Accordingly, it faces the risk that its intervention could be inadequate or incomplete.
- The DIF faces many financial risks. Most importantly, it faces the risk of being inadequately funded or having insufficient liquidity to fulfill its mandate in the case of an intervention or financial crisis.

- The funds of the DIF need to be managed in such a way that they do not incur losses, whether that be from external economic shocks, the use of new financial instruments, wrong exposures to risks, etc.
- The DIF has to be certain that the qualifications of its employees are adequate and that employees are up-to-date with the latest knowledge in their respective fields. It also needs to be certain that its personnel behave professionally and respect ethical principles, notably confidentiality.
- The Organization deals daily with significant amounts of information, either flowing within the organization or between external parties and professionals inside the organization. There is a constant risk that vital information is not available when needed or that the information falls into the wrong hands.
- In a world of information processing, computers and IT are a vital element of any efficient organization. There is always the risk that software, a computer, a server, a connection, etc., could fail and that the normal operations could be affected as a result.
- With many interdependent divisions, synergy in the day to day operations of the Organization is very important for the carrying out of projects, policies or processes, which must go uninterrupted. There is always a risk that internal controls are inefficient and that a problematic situation goes unnoticed.
- Being an integrated regulator, the Organization administers a number of acts and regulations (securities, deposit insurance, distribution, credit unions, etc).
- The DIF delegates some of its operations to third parties. Fund management is delegated to an external manager according with its enabling Law, HR is managed by the HR department, financial affairs are delegated to the Finance department, and so on.
- The Organization faces the risk that its daily operations could be slowed or halted by an external event, such as an important temporary electrical breakdown, a public health crisis (such as a pandemic avian flu) or other such event over which the Organization has no control.
- The Organization deals with enormous amounts of data and information, most of which are confidential. It thus faces the risks that some information could be leaked out to the public because disrespect of confidentiality on the part of an employee or due to external intrusion into the Organization's IT systems or its premises.
- The Organization communicates to many external stakeholders and in the process risks being misunderstood.
- Many of the DIF's employees maintain professional relations (either on-site or through distance communications) with external partners or stakeholders, and in the process there is always a risk that those relationships could create a conflict of interest with the AMF.
- The DIF faces external risks by delegating the inspection of the most important registered institutions to an external self-monitoring bureau.

- The DIF delegates its investments to an external manager, so it faces the risk that this manager does not follow adequate investment practices.

3. Please describe the process that the deposit insurer initially followed to identify these risks.

Given that the DIF function is carried out by more than one division, there have been a number of processes leading to the creation of frameworks or policies aimed at mitigating risks, with these policies or frameworks stemming from a number of different origins. Most divisions come up with policies and practices to mitigate risks.

For example, in the case of identifying financial risks at registered institutions, the solvency branch created a risk matrix to identify what kind of risks must be analyzed in order to determine whether an institution is financially sound.

The Organization also uses Plans (Strategic Plan 2005-2008, the Delegation Plan, The Continuity of activities plan) to analyze and assess the challenges and risks it will face in the years ahead in the different areas where it operates.

Refer to question 6 below for more details on policies and practices aimed at mitigating risks.

4. Please describe the process (including the frequency that the process is applied) that the deposit insurer follows to identify potential new risks and changes to existing risks.

DIF conducts studies on the finances of the DIF program, notably the fund's capitalization, the way the fund is financed and the potential costs of a financial crisis.

Risk Assessment

5. Please describe the criteria used by the deposit insurer to assess the importance (significance) of its risks.

Criteria are in development. The Organization is drafting an intervention plan in case of a liquidity crisis of a financial institution. The Organization is also developing a risk management system.

Risk Management

6. Does the deposit insurer have formal policies in place governing the management of its risks? If yes, please describe the nature of

the content of these policies (i.e. do they address how each risk is to be managed and who is responsible for managing each risk).

Over the course of time, many policies and practices have been put in place to address the risks that we mentioned above in question #2.

Insurance risks:

- The DIF can count on the reserves of an external Stabilization Fund to reduce its insurance risk. This fund reduces payout risks and amounts. One of its main missions is to help to absorb losses due to the liquidation of some registered institutions.
- To reduce insurance risks further, the DIF has the right to borrow money from the government and states that the latter can guarantee its liabilities
- The Solvency branch has put in place a surveillance **Risk Matrix** that aims at efficiently managing risk analysis and making sure that registered institutions are financially sound.
- The Risk Matrix uses 8 types of risks: credit, market, liquidity, conception and premium setting, registration, operational, legal and strategic.

Intervention risks:

- The DIF has a **Policy for the intervention in a troubled institution**, that sets out the principles necessary for fast and efficient interventions:
  - Identification of troubled institutions with the help of continual surveillance of institutions and early warning indicators (these tell the DIF that an institution might have difficulties)
  - Follow-up of extra-provincial institutions in collaboration with other actors (such as the CDIC)
  - In cases where intervention is needed, the Policy allows for the identification of the responsibilities of internal actors and gives different intervention options (assistance, acquisition/take over, liquidation)
  - The Policy requires institutions under its jurisdiction to send the DIF all the information necessary for assessment of registered institutions.

Financial risks:

- The DIF has a very liquid **Investment Policy**.
- The Policy is very conservative. It was established with the principal of asset protection rather than returns or growth.

Human risks:

- In the **Strategic Plan 2005-2006,** one of the Organization's goals is to mobilize its personnel, notably by aiming at offering competitive wages, at increasing knowledge and competencies and by rewarding efforts.
- The Organization has a **Policy for the improvement and training of human resources,** the goal of which is to bring employees' knowledge and competencies up to date. This policy is a framework for training, integration, and HR improvements. The policy allows for the creation of an HR development committee whose main goal is to make proposals to the Department in terms of HR development programs.
- The Organization has an **Ethics and Conduct Code** that establishes ethical rules and norms employees must follow. Amongst other things, it stipulates that employees must exhibit discretion and protect confidentiality in their day-to-day work and abide by the policies put in place by the AMF.

Technology risk

- The Organization has put in place a **Technology Policy** aimed at minimizing risks that can be caused by the use of information technology. Its goal is to make IT users sensitive to security issues, to the consequences of security breaches as well as to their roles and obligations in the daily process of IT security and protection.
- The Organization also has a **Directive relating to the access of the Organization info-structure.** This latter policy stipulates that:
    - The Organization must have adequate measures in place to assure the protection of its info-structure against any unauthorized use and to guard against any threat or risk likely to have a direct effect on the availability, integrity or confidentiality of information.
    - It also provides a framework that prohibits unauthorized access to any software or operating system able to bypass applications

Externalization risks

- Since 1969, the DIF has been party to an agreement with another deposit insurer with regards to some of its registered institutions. This agreement makes explicitly clear what responsibilities the two partners have, particularly with regards to inspection and transmission of information.
- The external manager of the DIF's funds operates according to the principles set in the **Investment Policy,** which are determined by the DIF.

- In terms of liquidation, and according to Law, the DIF uses the official liquidator for the reimbursement of depositors.

Business Continuity Risk

- Since information management is vital for the Organization and its activities, the **Information Security Policy** was created in order to, guarantee continuity of the Organization's daily activities without any interruption or information losses.
- The Organization has policies in place to deal with emergency situations. One major line of policy is the creation of a series of **Business Continuity Plans,** the aim of which is to set up a framework of responses in cases of emergency crises. The latest, the **Pandemic Plan,** aims at protecting employees (security risks) through prevention while at the same time insuring the continuity of business activities as much as possible during a major avian flu pandemic.

Security risk

- The Directive relating to the access of the Organization's info-structure, the Technological policy as well as the Ethics and Conduct Code are all part of a global framework aimed at maintaining a high level of security and confidentiality with regard with information the DIF deals with.

Finally, the Organization, as an integrated regulator, has developed internal controls at all levels in order to avoid any kind of conflicts of interests in the management of it day-to-day operations and mandates. The **Delegation Plan** is aimed at this task. (See below question 10).

Risk Monitoring and Reporting

7. Please describe the nature and frequency of any monitoring and internal reports that the deposit insurer makes to its senior management and/or to its governing body about the insurer's risks (including the nature and frequency of any formal sign-off by senior management of the deposit insurer respecting the content of the risk reports).

Many internal reports are sent to the managers.

a. In terms of financial risks, the external manager (in charge of the DIF's assets) has to report every year on its activities. At least twice a year, the DIF meets with the External manager so that the latter can report on the management of the fund.

b. Also, according to the Regulation, the Stabilization Fund reports to the DIF every year on its activities.

c. In terms of internal process risks, the Organization has a **Report and Monitoring Committee** whose responsibility it is to report every 3 months on internal processes and activities, and, more specifically, on progress made by each unit regarding the Strategic Plan.

8. **Please describe the nature and frequency of any reports that the deposit insurer makes to external stakeholders about the deposit insurer's risks (including the nature and frequency of any formal sign-off by the deposit insurer respecting the content of the risk reports).**

The annual report of the Organization includes the activities of the DIF.

Risk Governance

9. Is the deposit insurer called upon by legislation, regulation, guidelines or other external means within its jurisdiction to implement a process for identifying, assessing, managing, monitoring and reporting on its risks? If yes, Please describe these externally imposed requirements.

No. But as a matter of good business practice, the Organization is implementing a risk management system.

10. Who has the deposit insurer made responsible for organizational risk management? And, has the deposit insurer dedicated an individual, or a team of individuals, to implement and coordinate the process for identifying, assessing, managing, monitoring and reporting on its risks? If yes, please describe the specific responsibilities assigned and who has been assigned these responsibilities.

Policies are aimed at creating "risk owners" who are accountable for certain risks. The **Delegation Plan,** mentioned above, was created by senior management of the Organization in order to delegate the decision-taking process related to the administration of the many acts regulating financial markets to the right decision maker. In doing so, the Organization has created de facto "risk owners" who are delegated decision powers from the CEO. Finally, the internal auditor is conducting a research project on ERM for the Organization

Canada Deposit Insurance Corporation (Canada)

Background Questions

1. **In which year was your deposit insurer established?**

   1967

2. **How many individuals does your deposit insurer employ?**

   80

3. **Does your deposit insurer have in place a formal process to identify and evaluate impact and likelihood of significant risks?**

   a) Yes
   b) Yes, but the process is still in development
   c) No

   If yes, how regularly is this process carried out? Annually

4. **Does your deposit insurer have a Risk Management committee (or a committee of similar capacity) with responsibility for directing and coordinating risk management activities with the governing body?**

   a) Yes
   b) Yes, but the roles and responsibilities of the committee are not formalized
   c) No

Risk Identification

1. **Does the deposit insurer employ a process for identifying risks related to the fulfillment of its mandate (including risks stemming from the conduct of its operations)?**

   Canada Deposit Insurance Corporation ("CDIC") began implementing an Enterprise Risk Management system in 2003. CDIC has focussed its process on the identification, assessment, management, and reporting of risks that could impede CDIC's fulfillment of its mandate.

These include risks stemming from CDIC's operations and risks in addition to those posed by CDIC's member banks. CDIC's process originally consisted of conducting an initial assessment to obtain a high-level understanding of CDIC's significant risks and how they are being managed. Subsequently CDIC conducted more detailed ongoing risk assessments. These were coordinated by an Enterprise Risk Management Committee ("ERM Committee") composed of the Chief Executive Officer and senior management

2. Please list and define the risks that the deposit insurer has identified.

CDIC has identified four primary risk categories, three of which comprise underlying sub-risks. Those risk categories (with their respective sub-risks) are:

- **Insurance Risk:** CDIC's risk of loss, including costs incurred in the event of an intervention, associated with insuring deposits.
    - **Insurance Powers Risk:** The risk that CDIC does not have the necessary powers to support the management of its insurance risk in accordance with CDIC's statutory objectives.
    - **Assessment Risk:** The risk that CDIC does not promptly or systematically identify member institutions that pose an unacceptable level of insurance risk
    - **Intervention Risk:** The risk that CDIC cannot or does not take timely and effective action with respect to an unacceptable level of insurance risk posed by a member institution, or with respect to failed member institutions.
- **Financial Risk:** The risk associated with managing CDIC's assets and liabilities, both on- and off-balance sheet.
    - **Liquidity Risk:** The risk that funds will not be available to CDIC to honor its cash obligations (both on- and off-balance sheet) as they arise.
    - **Market Risk:** The risk of loss, attributable to adverse changes in the values of financial instruments and other investments or assets owned directly or indirectly by CDIC, whether on- or off-balance sheet, as a result of changes in market rates (such as interest rates and foreign exchange rates) or prices.
    - **Credit Risk:** The risk of loss attributable to counterparties failing to honor their obligations, whether on- or off-balance sheet, to CDIC.

- **Operational Risk**: CDIC's risk of loss resulting from inadequate or failed internal processes, people and systems, or from external events.

    - **People Risk:** The risk resulting from inadequacies in the competencies, capacity or performance, or from the inappropriate treatment, of CDIC personnel.

    - **Information Risk:** The risk that timely, accurate and relevant information is not available to facilitate informed decision making and/or the exercise of effective oversight.

    - **Technology Risk:** The risk that CDIC's technology does not appropriately support the achievement of its statutory objects and the conduct of its affairs.

    - **Process Risk:** The risk resulting from the incorrect execution of, a breakdown in, or a gap in, a policy, practice or control respecting CDIC's processes.

    - **Legal / Compliance Risk:** The risk that CDIC fails to identify, consider, fulfill or comply with its legal and other obligations and requirements in the conduct of its affairs.

    - **Business Continuity Risk:** The risk that a disruption impacting CDIC's personnel, information, premises, technology or operations will impede its ability to achieve its statutory objects and conduct its affairs.

    - **Security Risk:** The risk that CDIC fails to ensure the safety of its personnel and the security and integrity of its assets, including the confidentiality of its information.

- **Reputation Risk:** The risk of an event significantly affecting stakeholders perceived trust and confidence in CDIC, and which could result in a financial and other loss to CDIC.

3. ***Please describe the process that the deposit insurer initially followed to identify these risks.***

As an initial process, individual interviews were conducted with each executive and non-executive member of CDIC's Management team to obtain views about the key risks facing these individuals' direct areas of responsibility and those facing CDIC as a whole. In turn, these results were aggregated and consolidated in the form of a list of risks, risk categories and related definitions.

4. **Please describe the process (including the frequency that the process is applied) that the deposit insurer follows to identify potential new risks and changes to existing risks.**

CDIC conducts annual environmental scans as part of its corporate planning process. Such environmental scans seek to identify internal and external issues that could impact CDIC's operations going forward. Among other things, those issues could to relate to human and other resources, the economy, CDIC membership and legislative matters. Risks identified therein are recorded in a catalogue of corporate risks and confirmed by the ERM Committee.

Risk Assessment

5. **Please describe the criteria used by the deposit insurer to assess the importance (significance) of its risks.**

CDIC assesses the significance of a risk by considering two criteria: a) the potential adverse impact of a worst-case risk event on CDIC's achievement of its mandate and plans, financial situation, and/or reputation; and b) the probability of an adverse risk event occurring.

The assessment of impact and likelihood are based on a three-point scale qualitatively applying the following criteria:

	Impact Criteria: Of a Worst Case Adverse Risk Event		
	Financial	Reputation	Objectives / Priorities
High	Loss of at least 10 times CDIC's materiality threshold	Sustained (long-term) loss of CDIC's reputation	Serious impairment of CDIC's ability to achieve its statutory objects / Corporate Plan
Moderate	Loss between CDIC's materiality threshold and 10 times CDIC's materiality threshold	Sustained (short-term) but Unsustained (long-term) loss of CDIC's reputation	Moderate impairment of CDIC's ability to achieve its statutory objects / Corporate Plan
Low	Loss less than CDIC's materiality threshold	Minimal (short-term) loss of CDIC's reputation	Minimal impact on CDIC's ability to achieve its statutory objects / Corporate Plan

	Likelihood Criteria: Of a Worst Case Adverse Risk Event
High	The risk event is likely to occur at least once in the next fiscal year
Moderate	The risk event may occur at least once in the next fiscal year
Low	The risk event is unlikely to occur at least once in the next fiscal year

Risk Management

6. **Does the deposit insurer have formal policies in place governing the management of its risks? If yes, please describe the nature of the content of these policies (i.e. Do they address how each risk is to be managed and who is responsible for managing each risk?)**

In respect of enterprise risk management in general, CDIC's Board of Directors' Charter calls upon the Board to obtain an understanding of the significant risks to which CDIC is exposed, to establish risk management policies for those risks, to review such policies at least annually and to obtain reasonable assurance that CDIC's ERM process is appropriate and effective and that risk management policies are being adhered to.

The Board Charter also sets out expectations of management in respect of ERM. It calls upon Management to identify and assess the significance of the risks attendant upon CDIC's mandate, objects, strategies, plans and operations; recommend risk management policies to the Board; review those policies at least annually; manage risks in accordance with those policies; and provide the Board with timely, relevant, accurate and complete reports at least annually and, otherwise, as required.

CDIC has a Board risk policy in place governing each significant risk. Each of these policies serves to clarify the following: what risk management decisions are to be made; who is authorized to make these decisions; risk tolerance parameters and reporting expectations, in cases where decision-making is delegated to management; and, in cases where decision-making power is retained by the Board, the Board's expectations respecting management's supporting role in the decision-making process.

Risk Monitoring and Reporting

7. **Please describe the nature and frequency of any monitoring and internal reports that the deposit insurer makes to its senior management and/or to its governing body about the insurer's**

risks (including the nature and frequency of any formal sign-off by senior management of the deposit insurer respecting the content of the risk reports).

In accordance with its responsibilities laid out in the CDIC Board Charter, Management provides the Board of Directors with an annual ERM report that presents CDIC's significant risks and management's assessment of these risks. Management identifies risks and reports on risk ownership (i.e. the individual responsible for managing the risk in question); residual risk from the year previous; risk exposure; risk environment; risk rating; and risk rating trend.

As the Charter states, the Board has an obligation to obtain reasonable assurance that CDIC has an effective enterprise risk management process and that risk management policies are being adhered to. To this end, beginning in 2007, Management will provide the Board with a representation at fiscal year-end. The timing of the representation will enable the Board to be in a position to consider CDIC's risks, including any risk management issues, prior to approving CDIC's annual financial statements and considering CDIC's Annual Report. The signatories of the representation will be the President and CEO and the Chair of the Enterprise Risk Management Committee.

8. **Please describe the nature and frequency of any reports that the deposit insurer makes to external stakeholders about the deposit insurer's risks (including the nature and frequency of any formal sign-off by the deposit insurer respecting the content of the risk reports).**

As part of the Management Discussion and Analysis section of its Annual Report, CDIC reports on its ERM process, its significant risks, how those risks are managed and its assessment of those risks. CDIC's Annual Report is signed by the Chairman of the Board and by the President and Chief Executive Officer.

Risk Governance

9. **Is the deposit insurer called upon by legislation, regulation, guidelines or other external means within its jurisdiction to implement a process for identifying, assessing, managing, monitoring and reporting on its risks? If yes, please describe these externally imposed requirements.**

CDIC is not called upon by statute or regulation to implement a process for identifying, assessing, managing, monitoring and reporting on its risks. But CDIC subjects itself to guidance from Treasury Board Secretariat, which suggests that government organizations ought to identify, assess, manage, and report on their risks.

10. **Who has the deposit insurer made responsible for organizational risk management? And, has the deposit insurer dedicated an individual, or a team of individuals, to implement and coordinate the process for identifying, assessing, managing, monitoring and reporting on its risks? If yes, please describe the specific responsibilities assigned and who has been assigned these responsibilities.**

CDIC's Board of Directors, Management and Internal Audit each play a role in the ERM process. The Responsibilities of CDIC's Board, Management, and Internal Audit are set out as follows:

The Board:

The Board has recorded its risk governance responsibilities under the CDIC Board Charter. The Board has also mandated the Audit Committee to assist it in discharging its responsibilities.

Management:

The Board charter also clarifies the Board's expectations of management in assisting the Board in discharging its ERM responsibilities. Specifically, the Board charter calls upon management to:

- Identify and assess CDIC's significant risks;
- Assist the Board in understanding CDIC's significant risks and their management;
- Propose risk management policies to the Board;
- Manage the risks in accordance with the Board's risk management policies; and
- Provide the Board with reports to enable it to assess whether CDIC has an appropriate and effective enterprise risk management process.

CDIC's President and Chief Executive Officer ("CEO"), supported by CDIC's officers and their teams, is ultimately accountable to the Board for Management's risk management responsibilities.

One individual in management is responsible for the coordination and facilitation of CDIC's ERM process and for advancing and improving that process once it is in place. That individual assists risk owners and their teams in identifying risks related to their responsibilities, assessing those risks, putting in place the necessary practices and controls to manage risk, and in reporting ERM results to the Board

An executive-level ERM Committee confirms CDIC's significant risks; the environment within which each risk is managed; the potential impact and likelihood of each risk; Management's risk exposure and trend assessments; any risk management initiatives to be undertaken; and Management-proposed Board risk management policies.

Direct responsibility for managing CDIC's risks falls to the owners of each respective significant risk and their teams. But because CDIC's risks cross divisional and functional lines, the ERM process provides a means of facilitating assurance that risks are managed on a consistent corporate-wide basis.

Audit and Consulting Services:

Management's ERM process and results are subject to validation by CDIC's internal audit function as well as to reviews by the Office of the Auditor General of Canada.

CDIC's Audit & Consulting Services has been charged by the Audit Committee of the CDIC Board of Directors with fulfilling the following role with respect to ERM:

- Reviewing the management of key risks;
- Evaluating the reporting of key risks;
- Evaluating risk management processes;
- Giving assurance that risks are correctly evaluated; and
- Giving assurance on the risk management processes.

These responsibilities are in line with a position statement issued by the Institute of Internal Auditors titled "The Role of Internal Audit in Enterprise-wide Risk Management". The position statement affirms that internal audit's core role with regard to ERM is to provide independent and objective assurance to the Board on the effectiveness of an organization's ERM activities to help ensure key business risks are being managed appropriately and that the system of internal control is operating effectively.

11. **Has the deposit insurer's governing body formalized its expectations respecting the implementation of a process for identifying, assessing, managing, monitoring and reporting on its risks? If yes, please describe these expectations and how they have been communicated to the deposit insurer.**

The expectations of the CDIC Board of Directors respecting the implementation of a process for identifying, assessing, managing, monitoring and reporting on its risks are set out in CDIC's Board Charter.

Please see response to Question #6

Malaysia Deposit Insurance Corporation (Malaysia)

Background Information:

1. In which year was your deposit insurer established?
August 2005

2. How many individuals does your deposit insurer employ?
70 (as at 10August 2009)

3. Does your deposit insurer have in place a formal process to identify and evaluate (impact and likelihood) of significant risks?

a) Yes
b) Yes, but the process is still in development
c) No

If yes, how regularly is this process carried out?
A comprehensive and formal process of identification and evaluation of significant risks is carried out annually. The ERM oversight structure comprises an Enterprise Risk Management ("ERM") Committee which membership comprises of senior management to: champion and provide oversight for ERM implementation across MDIC; and manage and monitor risk exposures and ERM activities. The Strategic Planning and Enterprise Risk Management Working Committee at operational level supports the ERM Committee to facilitate and coordinate all ERM activities from the operational level. The Working Committee meets every quarter to monitor and to report on-going risks and to identify potential new risks. This structure is designed to provide for continuous monitoring, review, update of current risks and identification of emerging risk using a combination of top down and bottom up approach. While senior management has overall responsibility for risk management, the ERM division is responsible for driving the process. Since, MDIC is a small organization, our approach is to build ERM awareness throughout the organization and each employee has a responsibility to bring existing or new emerging risk to the attention of the respective risk champions or risk facilitators in their division.

4. **Does your deposit insurer have a committee(s) (at the management or governing body level) responsible for directing and coordinating risk management activities?**

a) Yes (An ERM Division drives the ERM process through the ERM Committee and Strategic Planning and ERM Working Committee. Please refer to Q3 for more details on the committees.)
b) Yes, but the roles and responsibilities of the committee are not formalized
c) No

Risk Identification

1. **Does the deposit insurer employ a process for identifying risks related to the fulfillment of its mandate (including risks stemming from the conduct of its operations)?**

Yes, the risks are being identified currently through an annual formal process. ERM project is one of the key initiatives of MDIC in 2007 and moving forward. MDIC applies the Australian/New Zealand Standard 4360:2004 as the primary standard for our risk management framework and as a generic guide for establishing and implementing our risk management process.

If yes,

2. **Please list and define the risks that the deposit insurer has identified.**

Catalogue of MDIC Corporate Risks

No	Risk Category	Sub-Risk Category and Underlying Risk Events
1.	Strategic and Governance Risk: The group of risks affecting the medium to long term plan and priorities of MDIC or the risks contribute towards ineffective governance structures and processes in the Corporation.	a) External Risk: External uncontrollable events which will threaten the ability of MDIC to meet its mandate and conduct of its business and affairs.
		b) Governance Risk: Risk events pertaining to MDIC's relationship with bank stakeholders, board and management relationship, and internal control environment.
		c) Strategic Risk: Risk events in relation to adverse strategic decisions, improper implementation of decisions, or lack of responsiveness to environmental changes.

No	Risk Category	Sub-Risk Category and Underlying Risk Events
		d) Business Continuity Risk: The risk events in relation to disruption or which impact on MDIC's personnel, information, premises, technology or operations and impede its ability to achieve its mandate and conduct of its business and affairs.
2.	Insurance Risk: The group of risks related to MDIC's capability in carrying out assessment, monitoring, intervention, and other related risk associated with insuring deposits.	a) Assessment, Monitoring & Intervention Risk: Risk events associated with risk assessment, early intervention, and the readiness of MDIC in various areas such as IT systems, data, funding framework, crisis communication plan, mission critical personnel in the event of an intervention.
		b) Insurance Powers Risk: Risk events in relation to the effectiveness of the MDIC Act and related laws.
3.	Reputation Risk: The group of risks which have negative impact on stakeholders' perceived trust and confidence in MDIC carrying out its mandate.	a) Media Coverage Risk: Risk events in relation to media comments, reporting and effectiveness of our integrated communication plan.
		b) Image / Perception Risk: Risk events in relation to public awareness and understanding of MDIC's role.
4.	Financial Risk: The group of risks that result from ineffective or inefficient management of financial resources, budgets, cash flows, all other assets and liabilities items, both on-and off-balance sheet.	a) Market Risk: The risk of loss in relation to adverse movements in market rates or prices.
		b) Liquidity Risk: The risk that funds will not be available to MDIC on a timely manner to honor its obligations as they arise.

No	Risk Category	Sub-Risk Category and Underlying Risk Events
5.	Operational Risk: The group of risks that result from inadequate or failed internal processes, people, IT/systems, compliance/ legal, or from external events.	a) Compliance & Legal Risk: The risk events in relation to MDIC fails to identify, consider, fulfill or comply with laws, circulars, internal policies and other obligations and requirements, in the conduct of its business and affairs.
		b) Information Risk: The risk events in relation to the failure of MDIC to protect the security of confidential information.
		c) Information Technology Risk: The risk events in relation to the IT systems of MDIC that affect the ability to appropriately support MDIC's achievement of its mandate and the conduct of its business and affairs.
		d) Process Risk: The risk events pertaining to the incorrect execution of, a breakdown in, or a gap in, a policy, practice or control in MDIC processes.
		e) People Risk: The risk events resulting from inadequacies in the competencies, capacity or performance, or from the inappropriate treatment, of MDIC personnel.
		f) Physical Security Risk: The risk events in relation to MDIC failing to ensure the safety of its personnel and the security of its assets.

3. **Please describe the process that the deposit insurer initially followed to identify these risks.**

   As a start, we sent out an ERM questionnaire in mid- 2007 to obtain feedback on the risks or challenges faced by divisions and employees. Subsequently, based on the feedback from the ERM questionnaire, individual interviews and focus group discussions were conducted to obtain clarifications and to ensure all significant risks affecting MDIC have been identified. These results were then consolidated and categorized according to their relevant definitions into an MDIC risk profile. Board members' inputs were also solicited through the Board Audit Committee and Board meetings.

4. **Please describe the process (including the frequency that the process is applied) that the deposit insurer follows to identify potential new risks and changes to existing risks.**

   Following the initial process in Question 3, MDIC subsequently established a formal process by 3rd quarter 2007. We have established a top down and bottom up approach. We carry out comprehensive and formal risk identification and evaluation process annually. In addition, the ERM Committee (comprising senior management) and the Strategic Planning and ERM Working Committee (comprising employees at operational level) meet quarterly respectively to review MDIC's risk profile, identify potential new risks and changes to existing risks to ensure MDIC's risk exposures are managed and monitored. MDIC also conducts an annual environment scan as part of our corporate planning exercise. Given our small size, all employees are educated on ERM and every employee has a responsibility to identify and escalate risks upward, downward or laterally.

Risk Assessment

5. **Please describe the criteria used by the deposit insurer to assess the importance (significance) of its risks.**

   We considered Financial Soundness of Member Institution(s); Financial Loss; Operational Requirements and Continuity; Employee; Public Confidence / Reputation; Achievement of Corporate Initiatives as criteria to be used in measuring the impact of a risk.

Risk Management

6. **Does the deposit insurer have formal policies in place governing the management of its risks? If yes, Please describe the nature of the content of these policies (i.e. Do they address how each risk is to be managed and who is responsible for managing each risk).**

   Yes, we have a broad formal policy at the Board level which specifies that the Board will:

   a. obtain an understanding of the principal risks of the corporation's business;
   b. ensure that appropriate and prudent risk management systems to manage these risks have been implemented and review these regularly; and
   c. obtain reasonable assurance, on a regular basis, that systems are being adhered to and continue to effectively manage the risks affecting the Corporation.

In support of the above, the Audit Committee Charter states that the Chief Risk Officer ("CRO") functionally reports directly to the Audit Committee and administratively to the CEO. The charter requires the Audit Committee to:

- **a.** ensure that sound policies, procedures and practices are implemented for the management of key corporate risks;
- **b.** receive sufficient information to understand the nature and magnitude of significant risks to which the Corporation is exposed;
- **c.** review with Management and advise the Board on the Corporation's policies developed and implemented to manage the Corporation's risk exposures, and review such policies at least once a year to ensure that they remain appropriate and prudent;
- **d.** on a regular basis, obtain reasonable assurance that the Corporation's risk management policies for significant risks are being adhered to;
- **e.** report to the Board on: the significant risks; the policies and controls in place to manage these significant risks; and the overall effectiveness of the risk management process;
- **f.** periodically consider the respective roles of the AG and internal audit function concerning risk management at the Corporation and annually evaluate the AG's and internal audit function's respective performance in relation to such roles: and
- **g.** request reports from the internal audit function validating Management's risk assessment.

The CRO shall have regular reporting duties to the Audit Committee as well as to the full Board of Directors. At least annually, the CRO will submit an ERM report to the Audit Committee and the Board of Directors. This ERM report consists of a summary of all the ERM activities carried out during the year and most importantly the significant risk profile. The document serves to capture all the details pertaining to the significant risk profile of MDIC, including the risk rating details, the existing controls, risk mitigation strategy and the corresponding mitigating action plans or initiatives developed. In addition, the CRO will update the Audit Committee and the Board of Directors regularly on risk related matters and ERM activities. A Report on ERM is on the agenda for all Audit Committee meetings.

MDIC also has in place an ERM Charter which sets out the accountability, responsibility, independence and authority of the CRO and ERM function.

Risk Monitoring and Reporting

7. Please describe the nature and frequency of any monitoring and internal reports that the deposit insurer makes to its senior management and/or to its governing body about the insurer's risks (including the nature and frequency of any formal sign-off by senior management of the deposit insurer respecting the content of the risk reports).

The roles and responsibilities, oversight structure, reporting process, and ERM guidelines have been formalized. The individual risk policy is in the process of being developed.

In line with the Board Governance policy, management is expected to:

a. provide the Board regularly (and at least annually) with reports that will enable the Board to understand the management of the Corporation's significant risks;
b. recommend risk management policies for the Corporation's significant risks to the Board, review these policies periodically (and at least annually) to ensure that they remain appropriate and prudent and report to the Board on the results of these reviews;
c. provide the Board regularly (and at least annually) with reports that will enable the Board to be aware of any situation in which those risks that are not being managed in accordance with established policies and assess whether the Corporation's risk management policies remain appropriate and prudent in the circumstances and are being followed.
d. provide the Board regularly (and at least annually) with reports that will enable the Board to assess whether the Corporation has an appropriate and effective enterprise risk management process.

Details of meeting frequency and reporting structure are as follows:

Committee	Frequency of meetings	Reports / Briefing Received
Board of Directors	BOD meets not less than 4 times a year CRO to update the Board on significant risks to MDIC through the Audit Committee at	Routine Report ❑ Annual ERM Report ▪ Review of risk criteria ▪ Review risk management policies ▪ Key changes in business environment ▪ Changes of existing risks ratings ▪ New risks identified ▪ Status of completion of mitigation plans ▪ Updated risk profile and new mitigation plans

Committee	Frequency of meetings	Reports / Briefing Received
	least once a year and regularly on ERM activities.	❑ Annual audit report by ACS on the appropriateness and effectiveness of ERM process and framework. <u>Ad-hoc Report</u> ❑ ERM ad-hoc report: (as and when required) ▪ New significant risks which is of serious concern to MDIC ▪ Significant delay and derailment of completion of mitigation plans of significant risks to MDIC.
Audit Committee	Audit Committee meets not less than 4 times a year CRO to update the Audit Committee on risk related matters and ERM activities at every Audit Committee meeting. Ad-hoc report/ briefing as and when required to update on emerging critical risks.	❑ Regular reporting and update on ERM activities and risk related matters by the CRO ❑ Briefing on: ▪ Updates of assessment and ratings of existing risks ▪ Status of completion of existing mitigation plans ▪ New risks identified ▪ Changes in MDIC internal and external environment ❑ Annual review and recommend to the BOD for approval on: ▪ Risk Criteria ▪ Risk management policies ▪ Key changes in business environment ▪ Changes of existing risks ratings ▪ New risks identified ▪ Status of completion of mitigation plans ▪ Updated risk profile and new mitigation plans ❑ Review the audit report by Audit and Consulting Services (“ACS”) division on the appropriateness and effectiveness of the ERM process and framework.
Enterprise Risk Management (“ERM”) Committee	ERM Committee meets once a quarter Ad-hoc meeting as and when required to discuss on emerging critical risks.	❑ Reporting and update on ERM activities by ERM Division based on the input from PERM Working Committee on: ▪ Updates of assessment and ratings of existing risks ▪ Status of completion of existing mitigation plans ▪ New risks identified ▪ Changes in MDIC internal and external environment ❑ Annual review and recommend to the BOD for approval on:

Committee	Frequency of meetings	Reports / Briefing Received
		▪ Risk Criteria ▪ Risk management policies ▪ Key changes in business environment ▪ Changes of existing risks ratings ▪ New risks identified ▪ Status of completion of mitigation plans ▪ Updated risk profile and new mitigation plans ▪ Review and discuss the internal audit findings by ACS on the appropriateness and effectiveness of ERM process and framework.
Strategic Planning & ERM Working Committee ("PERM Working Committee")	PERM Working Committee meets at least four times a year to review risk profile and identify new risks and to update the ERM Committee. Ad-hoc meeting as and when required to discuss emerging new risks.	❑ Results of Risk Questionnaire from MDIC employees from respective divisions. ❑ Status of mitigation plans as reported by respective division

8. **Please describe the nature and frequency of any reports that the deposit insurer makes to external stakeholders about the deposit insurer's risks (including the nature and frequency of any formal sign-off by the deposit insurer respecting the content of the risk reports).**

   An analysis of MDIC's significant risks are published in our Corporate Plan and Annual Report.

Risk Governance

9. Is the deposit insurer called upon by legislation, regulation, guidelines or other external means within its jurisdiction to implement a process for identifying, assessing, managing, monitoring and reporting on its risks? If yes, Please describe these externally imposed requirements.

No.

10. Has the deposit insurer's governing body formalized its expectations respecting the implementation of a process for identifying, assessing, managing, monitoring and reporting on its risks? If yes, please describe these expectations and how have they been communicated to the deposit insurer.

The expectations of the MDIC Board of Directors as set out in the Board Governance policy with regard to Significant Risks to the Corporation are as follows:

Management will:

a. identify and assess the significance of the risks to the achievement of the Corporation's objects, strategies, plans and operations;
b. provide the Board regularly (and at least annually) with reports that will enable the Board to understand the management of the Corporation's significant risks;
c. recommend risk management policies for the Corporation's significant risks to the Board, review these policies periodically (and at least annually) to ensure that they remain appropriate and prudent and report to the Board on the results of these reviews;
d. provide the Board regularly (and at least annually) with reports that will enable the Board to be aware of any situations in which those risks are not being managed in accordance with established policies and assess whether the Corporation's risk management policies remain appropriate and prudent in the circumstances and are being followed.
e. provide the Board regularly (and at least annually) with reports that will enable the Board to assess whether the Corporation has an appropriate and effective enterprise risk management process.

These expectations are also highlighted in the Audit Committee Charter which states that the CRO, as the head of the ERM function, is responsible for the implementation, development and maintenance of the ERM framework for the Corporation. The ERM function assists and

provides information to the Committee regarding all ERM activities and outcomes of the ERM process, that is, the identification, assessment, evaluation, treatment, monitoring and communication of the significant risks affecting the Corporation. The ERM function also provides independent assessments in respect of the Corporation's risk management capabilities, and provides recommendations to improve these capabilities, where appropriate. The CRO shall have regular reporting duties to the Audit Committee as well as to the full Board of Directors.

11. **Has the deposit insurer dedicated an individual, or a team of individuals, to implement and coordinate the process for identifying, assessing, managing, monitoring and reporting on its risks? If yes, please describe the specific responsibilities assigned and who has been assigned these responsibilities.**

At MDIC, we recognized that everyone is responsible and plays a role in risk management. The ERM division's main responsibilities are to coordinate and facilitate MDIC's ERM activities, i.e. implement and coordinate the process for identifying, assessing, managing, monitoring and reporting on risks. Audit and Consulting Services Division will ensure that the risk management process has been carried out accordingly and provide independent validation. As mentioned above (Question no. 5), the Board of Directors and Audit Committee have their respective governance roles in risk management. The operations and support divisions will manage and report risk at the source.

The CRO, who heads the ERM function, reports directly to the Audit Committee and administratively to the Chief Executive Officer. In this connection, the CRO will make an annual representation to the Audit Committee and to the Board of Directors that the significant risks affecting the Corporation have been identified, assessed, evaluated, mitigated, monitored and communicated and provide an opinion on the overall systems of internal controls. This representation will be supported by respective management assertions so as to instill management accountability. Accordingly, all Heads of Division will make an annual management assertion that he or she is primarily accountable for the risks identified within his or her division, and that his or her division has identified, assessed, evaluated, monitored and mitigated all significant risks within the division and communicate the same to the CRO.

Instituto para la Protección al Ahorro Bancario (Mexico)

Risk Identification

1. **Does the deposit insurer employ a process for identifying risks related to the fulfillment of its mandate (including risks stemming from the conduct of its operations)?**

Yes. The Risk Committee [6] has implemented an organizational risk management strategy. The objective is to generate a wide spread certainty across the IPAB and its stakeholders that the Institution is capable of adequately coping with any unforeseen events that could affect its mission, by identifying in timely form risks and establishing controls to manage them.

In order to identify the risks that could impair the achievement of the objectives of the business units, each business unit is responsible for identifying its risks through the analysis of its respective processes and activities.

The Risk Management Unit is in charge of assisting business units in the identification process.

If yes,

2. **Please list and define the risks that the deposit insurer has identified.**

The Risk Committee has established three main risk categories based on the objectives of IPAB:

1) Deposit Insurance Risk - It emerges from IPAB's role as deposit insurer and from the possibility of bank failure(s). It includes**:**

- Assessment risk: the risk that IPAB does not systematically or promptly identify banks with financial problems.
- Intervention risk: the risk that IPAB does not respond appropriately to banks with financial problems.

2) Financial Risk - It is associated with managing IPAB assets and liabilities, both on- and off-balance sheet. It includes:

[6] The Risk Committee is integrated by six senior managers (including CEO) and it is led by the CEO. It was established to support the CEO in the risk management process.

- Market risk: the risk of loss in both on- and off-balance sheet, due to moves in market factors, including adverse changes in the interest rates and foreign exchange rates.
- Assets and liabilities risk: is related to IPAB's management of the debt derived from the financial crisis of 1995.
- Credit risk: the risk of loss attributable to counterparties failing to honor their obligations.
- Liquidity risk: The risk that funds will not be available for IPAB to honor its cash obligations as they arise.

3) Operational Risk - This risk exposure is attributed to the possibility of inadequate or failed internal process, people and systems, or from external events. It includes:

- o People Risks: losses caused by an employee or involving a group of employees.
- o Relationship Risks: losses due to problems in relations with third parties (regulators, suppliers, banks, other).
- o Risks in Systems, Technology and Processes: losses due to failure, breakdowns, or other interruptions in technology or processes.
- o Risks to Physical Assets**:** losses originated by damages to IPAB's premises and facilities, or losses of physical assets for which the IPAB is responsible.
- o Other External Risks: losses due to third parties that could impair the achievement of the IPAB's objectives, (regulation changes, economic changes, etc).

3. Please describe the process that the deposit insurer initially followed to identify these risks.

The Risk Committee initially designed and implemented a risk management strategy based on the specific characteristics of each risk category. Firstly, deposit insurance risks and financial risks were the priority. On a later stage, new policies to manage operational risks were implemented. More recently a new framework has been established to implement a more systematic and integrated organization-wide approach to risk management.

In the integrated approach all business units are required to identify, assess, control, report, and disclose the organizational risks (deposit insurance, financial, operational) related to their main activities and to the fulfillment of their objectives, and to assess the effectiveness of their risk controls. In this task, business units are assisted by the Risk Management Unit. As a result, IPAB has been able to integrate a database with all the risks that could affect the fulfillment of its objectives. The organizational risks are analyzed and the results are presented to the Risk Committee in order to evaluate the risk policies and strategies.

Deposit insurance risks were identified based on the activities related to banks monitoring and banking resolution process.

Financial risks were identified based on the structure of IPAB's balance sheet (foreign and domestic debt, domestic assets), debt management process and liquidity requirements.

Operational risks were identified based on each business unit processes, functions and responsibilities.

4. Please describe the process (including the frequency that the process is applied) that the deposit insurer follows to identify potential new risks and changes to existing risks.

Changes in existing risks are identified by monitoring and evaluating all risks categories that might affect the objectives of IPAB, as described in the answer to question 7.

New risks are expected every time the institution starts a new activity. If the situation requires it new procedures and controls have to be implemented. Likewise, IPAB carries out a quarterly revision to identify potential new significant risks.

As a result of implementing these processes, IPAB has a database with all the risks that could affect the fulfillment of its core activities.

Risk Assessment

5. Please describe the criteria used by the deposit insurer to assess the importance (significance) of its risks.

Risks are assessed based on their frequency and impact:

a. Immediate-attention Risks – they are frequent and have high impact. Should they occur, they could impair IPAB's ability to achieve its statutory objectives or corporate plan.
b. Continual-attention Risks – they are frequent but have low impact. If they occur, they could delay the accomplishments of goals.
c. Follow-up Risks - they are not frequent but have high impact. Should they occur, they will have some effects on goals.
d. Risks under control – they are not frequent and have low impact. If they occur, they might delay the accomplishments of goals.

Risk Management

6. **Does the deposit insurer have formal policies in place governing the management of its risks? If yes, Please describe the nature of the content of these policies (i.e. Do they address how each risk is to be managed and who is responsible for managing each risk).**

For deposit insurance risks, IPAB uses an early warning system based on the financial performance of insured banks.

For financial risks, IPAB's Board of Directors has established specific limits on risk exposure based on value at risk, counterparty risk and liquidity management methodologies. Positions are monitored and evaluated on a daily basis to assure compliance with the limits. The finance unit and risk management unit have specific responsibilities when limits are exceeded. To reduce exposure, positions have to be adjusted.

For operational risks, business units analyze its processes and procedures in order to assess their risks considering the expected impact and frequency. Controls are then set or adjusted based on the frequency and impact of a failure event.

At least every quarter, each business unit has to analyze its processes and activities in order to evaluate their risks, disclose new risks, and assess the effectiveness of controls of existing ones. If necessary, additional adjustments will be approved by the Risk Committee.

Risk Monitoring and Reporting

7. **Please describe the nature and frequency of any monitoring and internal reports that the deposit insurer makes to its senior management and/or to its governing body about the insurer's risks (including the nature and frequency of any formal sign-off by senior management of the deposit insurer respecting the content of the risk reports).**

Deposit insurance risks are monitored on a monthly basis and evaluated depending on the evolution of the economy and the financial performance of banks. The institution is currently working on new methodologies to estimate the probability of default and expected loss at default.

Financial risks are daily monitored and evaluated dependent on any changes in market conditions, the structure of the balance, portfolio investments, counterparty solvency and hedging strategies performance. Standard techniques like VaR, counterparty, credit and liquidity risk are implemented.

Operational risk are monitored and evaluated on a quarterly basis by each business unit. Reports are presented based on the severity and frequency of risks, as well as on the effectiveness of their controls.

In order to decide on the need to implement any change in policies and strategies, the Risk Committee evaluates the reports on the assessment of risks and their controls. The most significant risks are reported to the Internal Audit Unit to guarantee the full involvement of those in charge of monitoring and implementing controls. The board of directors is also kept informed.

8. Please describe the nature and frequency of any reports that the deposit insurer makes to external stakeholders about the deposit insurer's risks (including the nature and frequency of any formal sign-off by the deposit insurer respecting the content of the risk reports).

IPAB presents to the board of directors two semiannual reports to evaluate the achievement of goals and the fulfillment of its core objectives. In these reports, risk management activities are briefly discussed. Also, twice a year, the Risk Management Unit advises to the board of directors concerning IPAB's risks and the risk management process.

Once a year, IPAB provides a general assessment of its risk management strategy and policies to the rating agencies (S&P, Moody's, Fitch) to comply with their credit assessment process, related to debt management. Currently IPAB is the second largest internal debt issuer after the federal government.

Once a year, IPAB has to present a formal and detailed report on its risk management process to the board of directors and to the Civil Service Department.

Risk Governance

9. Is the deposit insurer called upon by legislation, regulation, guidelines or other external means within its jurisdiction to implement a process for identifying, assessing, managing, monitoring and reporting on its risks? If yes, Please describe these externally imposed requirements.

IPAB is required by a regulation[7] to identify, assess and manage any risk that could impair the achievement of its objectives. It is also required to

[7] The regulation is issued by the Mexican Civil Service Department.

evaluate the effectiveness of its risk controls as well as to implement any needed improvements within a specific time frame.

This task is carried out by IPAB in accordance with its responsibilities to establish and keep an institutional control that will allow it to achieve its goals and objectives.

10. Who has the deposit insurer made responsible for organizational risk management? And, has the deposit insurer dedicated an individual, or a team of individuals, to implement and coordinate the process for identifying, assessing, managing, monitoring and reporting on its risks? If yes, please describe the specific responsibilities assigned and who has been assigned these responsibilities.

The Board of Directors approves the risk management policies.

The Risk Committee is in charge of supporting the CEO in the risk management process; evaluating all risk management policies and strategies; and promoting the business units participation in the identification, assessment, control, information and disclosure of their risks.

In each business unit, a risk subcommittee was set up to support it in the management and control of its risks. Also, it is responsible for supporting Risk Committee in the accomplishment of the policies and strategies that had been determined by the Risk Committee.

The Risk Management Unit is in charge of coordinating the risk management processes and providing the required technical assistance to business units in the identification, assessment, control, information and disclosure and of its risks.

An Internal Audit Committee directly oversees the implementation of controls for all major risks -in accordance to assessments provided by the business units. Though is headed by IPAB's CEO, it has considerable supervisory powers and authority. Among its members are: the Head of Internal Audit Unit and representatives of the Ministries of Finance and Mexican Civil Service Department.

The Internal Audit Unit is in charge of evaluating that the institution has the necessary policies, procedures and infrastructure required for effective risk management. The unit is independent and directly reports to the ministry in charge of auditing the federal government and its agencies (Mexican Civil Service Department).

11. Has the deposit insurer's governing body formalized its expectations respecting the implementation of a process for identifying, assessing, managing, monitoring and reporting on its risks? If yes, please describe these expectations and how have they been communicated to the deposit insurer.

Yes. The objective is to generate wide spread certainty across IPAB and its stakeholders that the Institution is capable of adequately coping with any unforeseen events that could affect its mission, by identifying in time the risks and actions needed to manage them.

To gain the full involvement, commitment and support from managers and employees on the risk management strategy, senior managers clearly defined objectives and how they intend to achieve them. Thus, a risk management culture has been gradually integrated into the corporate culture of IPAB, from the Board of Directors down to all levels of management. Managers understand the major risks and challenges related to IPAB's core mission and are part of the decision-making process to ensure the availability of adequate coordination and accountability mechanisms to continually assess IPAB's core risks.

Savings Deposit Insurance Fund (Turkey)

Background Information:

1. **In which year was your deposit insurer established?**
   In 1983.

2. **How many individuals does your deposit insurer employ?**
   409.

3. **Does your deposit insurer have in place a formal process to identify and evaluate (impact and likelihood) of significant risks?**

   a) Yes
   b) Yes, but the process is still in development
   c) No

   If yes, how regularly is this process carried out? _____

4. **Does your deposit insurer have a committee(s) (at the management or governing body level) responsible for directing and coordinating risk management activities?**

a) Yes
b) Yes, but the roles and responsibilities of the committee are not formalized
c) No

Risk Identification

1. **Does the deposit insurer employ a process for identifying risks related to the fulfillment of its mandate (including risks stemming from the conduct of its operations)?**

Yes

If yes,

2. **Please list and define the risks that the deposit insurer has identified.**

We have identified 5 main risk categories:

- **Financial risks:** the risks related to management of on-balance sheet and off-balance sheet assets and liabilities of SDIF; the risks which emerge as a result of financial position and preferences of SDIF; the risks which arise from asset prices, interest rates, exchange rates, commodity prices, cash flows, credits, inflation and derivatives; losses that the SDIF may be exposed to when insuring deposits or costs that the SDIF may face during the bank interventions, and finally, any risk which may impede SDIF to use optimum alternatives to get maximum yield.
- **Operational Risks:** Any risks related to staff and workplace which may impede SDIF's fulfillment of main business activities (negligence, inexperience, bad intention, workload excess, low performance, low motivation etc.); any risks, losses or errors which may be emanated from business processes, technology and existing systems.
- **Strategic Risks:** the risks which may harm SDIF's reputation; the responsibilities which may emerge related to taken/untaken decisions in the framework of administrators' duties and positions; administrative, structural and organizational risks which may impede SDIF to reach its strategic goals and purposes.
- **External Risks:** the risks which emerge independent of SDIF's activities but have direct impacts on these activities; natural disasters, terrorism, legal regulations, economic and political instability, lack of coordination in financial safety net, debtors' negligence of commitments, changes in the sector etc.

- **Legal Risks:** deficiencies of legislation related to SDIF activities, misinterpretations or operations against the legislation; any risks which emerge from contracts that SDIF is a party and which impedes solution of legal problems.

3. **Please describe the process that the deposit insurer initially followed to identify these risks.**

   First we have created a working group in which each SDIF Department has a representative. Then we gathered risk items from the Departments. Finally, the group has discussed and determined risk categories.

4. **Please describe the process (including the frequency that the process is applied) that the deposit insurer follows to identify potential new risks and changes to existing risks.**

Risk Assessment

5. **Please describe the criteria used by the deposit insurer to assess the importance (significance) of its risks.**

   We will use a 5X5 matrix to assess the influence and likelihood of selected risk items.

Risk Management

6. **Does the deposit insurer have formal policies in place governing the management of its risks? If yes, Please describe the nature of the content of these policies (i.e. Do they address how each risk is to be managed and who is responsible for managing each risk).**

   No formal policies for the moment.

Risk Monitoring and Reporting

7. **Please describe the nature and frequency of any monitoring and internal reports that the deposit insurer makes to its senior management and/or to its governing body about the insurer's risks (including the nature and frequency of any formal sign-off by senior management of the deposit insurer respecting the content of the risk reports).**

   No monitoring and reports for the moment.

8. **Please describe the nature and frequency of any reports that the deposit insurer makes to external stakeholders about the deposit insurer's risks (including the nature and frequency of any formal sign-off by the deposit insurer respecting the content of the risk reports).**

   No reports to external stakeholders for the moment.

Risk Governance

9. **Is the deposit insurer called upon by legislation, regulation, guidelines or other external means within its jurisdiction to implement a process for identifying, assessing, managing, monitoring and reporting on its risks? If yes, Please describe these externally imposed requirements.**

   Yes. The deposit insurer is called upon by its bylaws namely "Organization Regulation" which is issued last year, to implement a process for identifying, assessing, managing, monitoring and reporting on its risks. In this Regulation, all departments should prepare reports, related to their duties, in the subjects that may be financially, legally or operationally risky about the Fund and send them to the Strategy Development Department who should follow and report the institutional risk information and consolidate them.

10. **Has the deposit insurer's governing body formalized its expectations respecting the implementation of a process for identifying, assessing, managing, monitoring and reporting on its risks? If yes, please describe these expectations and how have they been communicated to the deposit insurer.**

    No. There are no formal expectations for the moment.

11. **Has the deposit insurer dedicated an individual, or a team of individuals, to implement and coordinate the process for identifying, assessing, managing, monitoring and reporting on its risks? If yes, please describe the specific responsibilities assigned and who has been assigned these responsibilities.**

    No individual or team of individuals are dedicated to implement and coordinate the process for identifying, assessing, managing, monitoring and reporting on its risks. However, for the moment, a research process on ERM is conducted by Strategy Development Department.