ASSOCIATION OF SUPERVISORS
OF BANKS OF THE AMERICAS

OPERATIONAL RISK IN BANKING INSTITUTIONS

2009

Juventino Rosas # 70. Despacho 502. col. Guadalupe Inn. C.P. 01020, Mexico, D.F.
Tels. (52-55) 5662-0085, (5255) 5562-2134. Fax (5255) 5662-1093

OPERATIONAL RISK IN BANKING INSTITUTIONS

GROUP 6

ASSOCIATION OF SUPERVISORS
OF BANKS OF THE AMERICAS

| MEMBERS OF THE WORKING GROUP |

Mercedes Olano (President)	*Banco de España* (Spain)
Rafael Diaz (Technical Secretary)	**ASBA**
Rosalina Diaz	*Banco Central de la República Argentina* (Argentina)
Joao Faustino Marques	*Banco Central do Brasil* (Brasil)
Miguel Angel Villalobos	*Superintendencia Financiera de Colombia* (Colombia)
Teresa Gaona	*Banco Central de Paraguay* (Paraguay)
Alejandro Medina	*Superintendencia de Banca, Seguros y AFP* (Peru)
Thomas Odegard	**Board of Governors of the Federal Reserve System** (United States)
William Tiernay	**Board of Governors of the Federal Reserve System** (United States)
Daniel Frye	**Federal Deposit Insurance Corporation** (United States)
Daniel Fernandez	*Banco Central de Uruguay* (Uruguay)

| EDICIÓN DEL DOCUMENTO |

Rudy Araujo	**ASBA**
Rafael Diaz	**ASBA**

| TABLE OF CONTENTES |

| EXECUTIVE SUMMARY |

The highly competitive environment in the financial sector has driven banking institutions to venture into new financial markets and work with new products, which has increased the complexity of their operations and risk profile. A deeper analysis is required of all risks. In this regard, one of the biggest challenges faced by banking institutions is the adequate management and supervision of operational risk.

Given the importance of operational risk to effective banking system performance and stability, the Association of Supervisors of Banks of the Americas (ASBA), decided to study this issue. Its members agreed that ASBA form a Working Group ("Group") to study the current state of, and outlook for, operational risk management and supervision in the Region. The Group also had the mandate to establish, based on the experience of its members, a series of good practices and recommendations to improve the frameworks of operational risk regulation and supervision of the countries in the Region.

Initially, the Group analyzed basic elements of operational risk, including the regulatory and supervisory frameworks in the Region. Subsequently, the Group analyzed the role of the Board of Directors in the establishment of an operational risk management framework and that of the senior management in implementing it. In the third place, the tools used to identify, assess, monitor, and control operational risk were evaluated, and the way in which loss event information related to operational risk is recorded and classified.

The Group continued its work by analyzing the role of the internal audit in reviewing the operational risk framework and its implementation. The work concluded with a review of the disclosure of operational risk data in the Region and the challenges faced by member countries regarding operational risk on the road towards the implementation of Basel II .
Throughout the document, a considerable number of relevant practices and recommendations are presented. In this regard, some lines of action supported by the Group include the following.

1. The Region should attempt to converge toward a single definition of operational risk and have a similar classification of loss events arising from operational risk. The harmonization of these concepts would help bring about greater information-sharing and collaboration among supervisors, which would contribute to developing a more comprehensive view of operational risk in banking institutions.

2. Banking institutions and supervisors should no longer treat operational risk as a purely financial risk, but rather as a distinct type of risk that is present in all activities of the institution. Therefore, promoting the creation of specialized units to analyze this risk, both within banks and supervisory bodies, is encouraged. A structure must be established capable of implementing the broad framework adopted by a bank's Board of Directors for management of operational risk management. This structure would include clearly defined policies, processes and procedures to effectively measure, monitor and control operational risk.

3. The Board of Directors should define clear lines of responsibility and accountability regarding operational risk. Likewise, and with the help of senior management, the Board should create a culture within the organization that gives high priority to an effective operational risk management system and to enforcement of sound operational controls.

The Group believes that management of operational risk is more effective when the corporate culture stresses high standards of behavior and performance at all levels of the bank, which should be underscored and promoted by the Board of Directors and senior management.

4. Banking institutions should use all available tools to identify, evaluate, mitigate and control operational risk. Consequently, supervisory authorities, in addition to fostering the use of the various tools cited in this document, should promote broader use of stress testing and analysis of scenarios at medium- and smaller-sized institutions that will provide valuable input for, among other things, the evaluation of contingency plans.

5. The Group concurs with the Basel Committee that there must be a commitment on the part of banking institutions to ensure that personnel charge with operational risk management are duly qualified, with relevant experience, technical skills, and access to resources, and possess the ability to communicate effectively with personnel responsible for other risks (credit, market, etc.).

6. Banking institutions should record all operational losses or define a low threshold above which data on loss events will be collected to ensure that the data base on operational losses is as complete as possible.

7. Banking institutions must disclose information about its exposure and management of operational risk to all interested parties, including: Boards of Directors, senior management, supervisory authorities, investors, and the public at large. Disclosure of this information will reinforce principles of transparency and promote market discipline.

8. Lastly, banking institutions and supervisors should ensure that the framework defined for management of operational risk at the institution is subject to an efficient and comprehensive internal audit process conducted by personnel who are independent, appropriately trained and competent.

INTRODUCTION

The development and consolidation of ever larger and more sophisticated financial institutions has been driven principally by financial deregulation and globalization. These institutions carry out activities in multiple markets and have developed successively more complex risk profiles. As a consequence, the administration of operational risk now represents one of the biggest challenges that banks face.

In addition, the concept of operational risk concept has become much more important in the international financial community owing to the collapse of certain financial and non-financial institutions caused in part by operational problems. This does not mean that financial institutions in general do not prevent, manager or implement programs to reduce potential problems of an operational nature. Certain institutions and international organizations have advanced different initiatives that seek to make banking institutions consolidate loss events owing to operational risk and to make it be considered a distinct category of risk.

For preparing this document, the Group concentrated on studying the operational risk management conducted by the institutions in the Region and the duties performed by supervisory authorities. In order to obtain information for this analysis, the Group designed a 67-question survey divided into seven chapters that was sent to all Associated Members of ASBA. The survey was answered by the following 15 countries: Argentina, Brazil, Canada, Cayman Islands, Chile, Colombia, El Salvador, México, Nicaragua, Netherlands Antilles, Paraguay, Peru, Spain, the United States and Uruguay.

It should be noted that no special emphasis was placed on either measuring operational risk or calculating the capital requirements for operational risk under the new Basel II framework, although some of the progress in the Region is discussed. As a result, the Group recommends creating another group to pursue these issues in greater depth and expand upon the work that has been completed to date.

This document has seven chapters. Chapter 1 explores the general framework in which operational risk management is carried out in the Region, sets forth a definition for operational risk, and reviews the actions of different regulators regarding how this risk is supervised. Chapter 2 considers the role of the Board of Directors in the design of an adequate operational risk framework, and that of senior management regarding its implementation. Chapter 3 analyses the use of tools to identify, assess, monitor and control operational risk in the Region, while Chapter 4 looks at recording and classifying data on losses arising from operational risk. Chapter 5 focuses on the role of internal audit in evaluating the framework and practices relating to operational risk framework, while Chapter 6 analyses disclosure of operational risk data. In conclusion, Chapter 7 comments on the challenges that face member countries of the Region regarding operational risk on the road towards implementing the Basel II capital framework.

CHAPTER 1

Operational Risk: its Importance and its Regulatory and Supervisory Framework in the Region

The growing importance of operational risk has intensified the efforts to group together operational events under a distinct risk category. This has, in turn, convinced financial institutions to pay more attention to and dedicate more human and economic resources to the adequate management of operational risk.

In this first chapter, after providing a definition of operational risk, the general framework under which operational risk management is carried out in the Region is explored and the positioning of different regulators relative to the supervision of operational risk management is reviewed.

1.1
DEFINITION OF OPERATIONAL RISK

The first step required to deal with the issue is to establish a shared definition for operational risk. The Basel Committee defined operational risk as "the risk of loss resulting from inadequate or failed internal processes, people and systems, or from external events. The definition includes legal risk but excludes strategic and reputational risk."[1] The Group will use this definition for this document.

In addition, the Basel Committee has defined a series of types of operational risk events that are commonly considered as having the potential to result in substantial losses and that help to refine the definition of operational risk. These events are:

1. Internal Fraud: For example, intentional misreporting of positions, employee theft, and insider trading on an employee's own account.[2]

2. External fraud: For example, robberies, forgery, cheque kiting, and damage from computer hacking[3].

3. Employment practices and workplace safety: For example, workers compensation claims, violation of employee health and safety rules, organized labor activities, discrimination claims, and general liability.

4. Clients, products and business practices: For example, fiduciary breaches, misuse of confidential customer information, improper trading activities on the bank's account, money laundering, and sale of unauthorized products.

5. Damage to physical assets: For example, terrorism, vandalism, earthquakes, fires, and floods.

6. Business disruption and system failures: For example, hardware and software failures, telecommunication problems, and utility outages.

7. Execution, delivery and process management: For example, data entry errors, collateral management failures, incomplete legal documentation, unapproved access given to client accounts, non-client counterparty misperformance, and vendor disputes.

1 BIS. Basel Committee on Banking Supervision. Sound Practices for the Management and Supervision of Operational Risk. February 2003.
2 Alternative definition: Intentional acts to try to defraud or misappropriate assets from an entity or that circumvent laws or regulations, where at least an employee or an administrator of the entity is implicated.
3 Acts carried out by a person outside of the entity who is trying to defraud or misappropriate assets from the entity or circumvent laws or regulations.

1.2.
OVERVIEW

1.2.1
Definition

From the survey carried out by the Group, it became evident that most of the countries in the Region use a definition of operational risk definition quite similar to that of Basel II. Only one country, Colombia, has established a broader definition that includes reputational risk, which was expressly excluded by the Basel Committee. On the other hand, Uruguay has a more limited definition since it excludes legal risk. The survey also reveals that operational risk is considered relevant by the majority of regulators in the Region.

1.2.2.
Aspects of regulation and supervision of operational risk

Only two of the fifteen countries that responded to the survey have no regulations or guidelines for operational risk. Two of the countries that responded, in spite of not having passed any regulations, have established guidelines. All of the other countries have norms that, to a greater or lesser degree, regulate this type of risk.

There are important differences in the approaches of the different countries. In seven countries (Netherlands Antilles, Argentina, Chile, Colombia, Cayman Islands, Nicaragua and Uruguay) only the management of risk is regulated, while in six other countries (Brazil, Canada, Mexico, Peru, Spain and the the United States) additional capital requirements for operational risk have been established.

Among those countries that currently do not have regulations pertaining to operational risk, some are going to create or strengthen their norms or guidelines in the near future. El Salvador expects to issue various regulations regarding management of this type of risk in 2010, and will address the creation of a registry of losses at a later date; Cayman Islands will expand regulations to include capital requirements for operational risk; Paraguay will commence regulating this type of risk in 2010. In Canada, it is not believed necessary to issue new regulations for operational risk as they consider that existing guidelines are sufficient.

1.2.3.
Regulatory enforcement

In the majority of countries in the Region, it has been established that regulations are applied equally to all banks independently of their size and with flexibility based on the complexity of the institutions. It should be noted that while in general terms all entities are subject to the same regulations, in certain cases this varies for different-sized entities. In Mexico, although currently all entities are subject to the same regulation, in the near future, it is expected that specialized banks (niche banks) are to be established which will have regulation that is different in all aspects, including that related to operational risk management.

All of the countries that responded to the survey are carrying out a broad and in-depth review of operational risk during their regular examinations or by means of specific targeted reviews of this type of risk.

1.2.4
Specialized units for dealing with operational risk

Of the fifteen countries that answered the survey, only four (Argentina, Cayman Islands, Nicaragua and Paraguay) do not have a specialized unit within their supervisory agency to deal with operational risk. All of the other supervisors have specialized units that range from sophisticated departments with considerable resources, such as in the case of Canada and the United States, to recently created departments such as in the case of El Salvador. Various countries have medium-sized specialized units that share their experience with the general examiner's units and jointly review with the examiners the most technical aspects of this risk. It should be highlighted that those countries that do not have a specialized unit do not foresee creating one in the near future.

1.3
GOOD PRACTICES

The Basel Committee has acknowledged the importance of operational risk management and supervision, and this is reflected in the capital requirements established for this risk within Pillar 1 (minimum capital requirements) of Basel II.

In the previously mentioned document on sound practices for operational risk (2003), the Committee had already acknowledged that operational risk was treated differently by each banking institution and stated the expedience of trying to unify the different concepts into one shared definition.

Likewise, the Basel Committee has indicated that institutions should manage operational risk and that regulators must establish the obligations of the entities in this regard and supervise their enforcement. Specifically, the Committee established the following guidelines for supervisors.

1. Banking supervisors should require that banks, regardless of their size, manage operational risk.

2. Supervisors should carry out, directly or indirectly, an independent periodic assessment of bank policies, practices and procedures for managing operational risk.

3. Supervisors should ensure that those banks that are part of a financial group have operational risk management procedures that cover the whole group. In these cases, it might be necessary to cooperate and share information with other supervisors.

4. Supervisors should actively promote ongoing development of controls in banks, by monitoring and evaluating the latest advances achieved by banks and their development plans.

1.4
RECOMMENDATIONS

Many countries in the Region use a definition of operational risk that is quite similar to the one instituted by the new Basel II framework and, in general, the supervisors of the Region consider this a relevant risk. Even so, the Working Group believes that recommendations that can help to improve the regulation and supervision of this risk in the countries of the Region are warranted as follows.

1. It is important that the regulations of all countries in the Region converge towards a single definition of operational risk that would facilitate the harmonization of concepts and would improve the information-sharing and collaboration and among supervisors.

2. Supervisors should deepen their review of the management standards for operational risk management developed by the banks in their countries and promote the creation of specialized units capable of facing the growing complexity of this type of risk analysis.

3. In the context of globalization of financial groups that use different metrics in different markets and countries, collaboration and coordination among supervisors throughout the Region should be encouraged in order to ensure effective supervision of operational risk at the level of the financial group.

1.5.
CONFUSION OF OPERATIONAL RISK WITH OTHER RISKS

To close this initial chapter, we will review the issue of classification of operational risk within the measurement systems of market and credit risk, which could have significant consequences for banks.

Operational risk management is different from credit or market risk management because it affects potentially every activity and process in a financial institution. Therefore, its management cannot be completely centralized; it should be managed at both the corporate group level and within the business lines.

Examples of events of operational risk losses that are sometimes captured by the control and management systems of market risk include:

- losses resulting from unauthorized transactions of certain products and
- unwanted positions stemming from inadequate entry and acceptance of orders in the system of electronic business.

The closing of these positions can trigger losses or profits that are picked up by systems that measure market risk. These results should be allocated to operational risk and the losses allocated to the database of operational risk loss events.

On the other hand, many losses are incorrectly associated with credit risk when they should be associated with operational risk. An example would be the case of a bad loan, which from origination was poorly managed. In this case, both the event as well as the amount of the loss should be taken into account in the measurement and control systems for operational risk, even though the corresponding restructuring is attributed to credit risk.

In many cases, it is neither easy nor clear how to allocate an event to a specific risk because it affects all of them. It is possible that a severe operational risk event could be erroneously allocated to credit risk, which means that losses arising from credit risk increase due to factors not directly related to the creditworthiness of the borrower. Due to the rise in reported credit losses, managers could, for example, inadvertently reduce loans in a geographic region or economic sector or to a client.

CHAPTER 2

The Responsibility of the Board of Directors in the Design of an Adequate Operational Risk Framework and the Role of Senior Management in its Implementation

The Board of Directors is responsible for the design, approval, implementation and oversight of the internal guidelines for operational risk management. Therefore, it is paramount that the Board knows and understands its responsibilities. Similarly, senior management must be aware of the fact that they are jointly responsible for making sure that management of operational risk is carried out effectively.

2.1
THE DUTIES OF THE BOARD OF DIRECTORS AND SENIOR MANAGEMENT REGARDING OPERATIONAL RISK

The Basel Committee indicates that the main duties of the Board of Directors regarding operational risk will be the following:

- to authorize a framework to be applied throughout the organization to explicitly manage operational risk by establishing principles to identify, asses, monitor,and control or mitigate this type of risk;
- to establish a structure capable of putting into practice the framework adopted by the institution for operational risk management, setting up clear lines of responsibility and ensuring the enforcement of policies and procedures;
- to ensure that the defined operational risk management framework in the entity is subject to an effective and comprehensive internal audit process carried out by independent, trained and competent personnel, ensuring that the control function is not responsible for managing operational risk;
- to ensure that compensation policies and practices of banks are consistent with their respective company culture, long-term objectives and strategies and with the control environment;
- to provide senior management with unequivocal norms and guidance regarding the principles on which the framework for operational risk management is based and
- to approve policies and procedures and ensure their enforcement.

Along the same lines, the Basel Committee states that the main duties of senior management related to operational risk are the following:

- to put into practice the framework adopted by the Board of Directors for operational risk management by developing operational risk management policies, processes and procedures for all bank products, activities and controls;
- to establish clear lines of authority, responsibility and communication to encourage and maintain acceptance of operational risk management responsibilities;
- to ensure the availability of sufficient human and financial resources to manage operational risk effectively;
- to guarantee that the personnel in charge of operational risk management are duly qualified (have experience, technical skills and access to resources) and that they communicate effectively with personnel in charge of managing the other risks (credit, market, etc.) and
- to be aware of quality of controls on documentation and practices for carrying out transactions.

2.2
OVERVIEW

The data survey provided the following general overview of the Region regarding the role of the Board of Directors and senior management in relation to operational risk.

2.2.1
Comprehensive risk management and operational risk management integration in daily operations

As expected, in the Region a comprehensive risk management process that includes operational risk was more commonly found in the larger and more complex organizations than in the medium-sized and smaller ones.

Eleven countries reported that all or at least the majority of the large- and medium-sized banks have this comprehensive risk management in place, whereas only five countries said that all (Colombia, Mexico and the United States) or most (Chile and Peru) of the small banks have comprehensive management. The survey also indicated that in the smaller banks there are problems with the integration of operational risk management into the daily operations of the entities.

In the case of medium-sized banks, the situation is intermediate between the large and the small banks. (Only in the United States is operational risk management incorporated .into all medium-sized banks.) It should be pointed out that all countries reported that in at least some of their large banks comprehensive risk management exists that includes operational risk and operational risk management in the daily operations of the entities.

2.2.2
Operational risk management general framework

As regards the design and implementation by the Board of Directors of a general framework of operational risk management (and its periodic review), the survey produced the following results:

Ten countries reported that all or most of the Boards of Directors of the large- and medium-sized banks have set up this framework, while only 5 countries indicated that all (Colombia and the United States) or that most (Brazil, Netherlands Antilles and Peru) of the boards of directors of their small banks have set up such a framework.

One survey question asked if senior management was in charge of implementing the general framework for operational risk and developing policies, processes and procedures designed to introduce an operational risk management culture throughout the entity. The survey indicated that these conditions occur more frequently in large banks than in the medium or smaller banks. In this regard, only the United States responded that senior management implements this framework in all small banks.

It is also important to highlight that all countries reported that, at least in some of the large banks, the Board of Directors implements the operational risk management general framework.

2.2.3
Formal infrastructure for operational risk management

It is necessary that the Board of Directors ensure that an operational risk management infrastructure[4] exists, commensurate with the institution's risk profile. The survey shows that nine countries reported that all or most of the large banks have a formally established infrastructure, and a similar situation holds among medium-sized banks. Six countries reported that all or the majority of their small banks have an infrastructure. It should also be noted that only one country reported not having a formally established risk management infrastructure for any medium or small banks.

2.2.4.
Existence of regulation, guidelines or supervisory practices for operational risk in the Region

Chart 1 shows the approaches of bank supervisors in the Region regarding the issues presented, i.e., if there are supervisory regulations, guidelines, or practices regarding operational risk.

The responses to the survey indicated the existence of supervisory practices in most countries that cover the topics identified.

Regarding the existence of supervisory regulations, guidelines or practices relative to the topics analyzed, we can say that the situation in the Region is relatively good, since most of the countries reported the existence of one or more of the approaches to supervision.

In summary, the performance of the Board of Directors and senior management regarding the practice of comprehensive risk management and in providing an operational risk management infrastructure is better or more sophisticated in large banks than in small ones. This is consistent with the view that management is more complex in larger banks than in small ones.

However, this is not an ideal situation. Senior management of any entity, regardless of size, should establish a framework for operational risk management and should carry out comprehensive risk management commensurate with the bank's risk profile.

4 The setting up of duties and competencies of all the organization in operational risk implementation and control and its formalization and documentation, plus the establishment of operational risk independent units, etc.

CHART 1:

Existence of regulation, guidelines or supervisory practices for operational risk

INTRNAL RISK MANAGEMENT (INCLUDING OR)	RISK MANAGEMENT INFRAESTRUCTURE	BOARD OF DIRECTORS ESTABLISHES OPERATIONAL RISK MANAGEMENT FRAMEWORK	SENIOR MANAGEMENT IMPLEMENTS OPERATIONAL RISK MANAGEMENT FRAMEWORK	INTEGRATION OF OPERATIONAL RISK MANAGEMENT
Regulation Guidelines Supervision (4 countries)	Regulation Guidelines Supervision (4 countries)	Regulation Guidelines Supervision (4 countries)	Regulation Guidelines Supervision (4 countries)	Regulation Guidelines Supervision (2 countries)
Regulation Supervision (2 countries)	Regulation Supervision (3 countries)	Regulation Supervision (3 countries)	Regulation Supervision (3 countries)	Regulation Supervision (3 countries)
Regulation (2 countries)	Regulation (2 countries)	Regulation (2 countries)	Regulation (2 countries)	Regulation (2 countries)
Guidelines Supervision (3 countries)	Guidelines Supervision (2 countries)	Guidelines Supervision (2 countries)	Guidelines Supervision (2 countries)	Guidelines Supervision (5 countries)
Guidelines (1 country)	Guidelines (1 country)	Guidelines (1 country)	Guidelines (1 country)	Guidelines (1 country)
Supervision (1 country)	Supervision (1 country)	Supervision (1 country)	Supervision (1 country)	
No Answer (2 countries)	No Answer (2 countries)	No Answer (2 countries)	No Answer (2 countries)	No Answer (2 countries)

2.3
GOOD PRACTICES AND RECOMMENDATIONS

After analyzing the issue, the Group has developed the following good practices and recommendations.

1. The Board of Directors is responsible for the design and implementation of an adequate framework to prevent operational risk.

2. Banking institutions must treat operational risk not as part of a purely financial risk but rather as a distinct class of risk that is present in the various products, activities, processes and systems of all the business lines of the institution. Consequently, there must be a specialization in management of operational risk, and therefore management structures responsible for periodically approving and reviewing the operational risk management framework should be appointed in timely fashion.

3. The Board of Directors should establish clear lines of responsibility, accountability and reporting in relation to operational risk.

4. The Board of Directors and senior management are responsible for creating a corporate culture that places a high priority on effective management of operational risk and on the enforcement of sound operational controls. Operational risk management is

more effective when the institutional culture emphasizes high standards of behavior and performance at all levels of the bank, and this should be highlighted and promoted by the Board of Directors and senior management.

5. The Board of Directors should regularly review operational risk data to understand at all times the operational risk profile of the institution, as well as the strategic implications of such information. Therefore, the appropriate control units should produce periodic reports about operational risk exposure for the Board of Directors and senior management, regardless of the institution's size.

6. It is essential that supervisors ensure that banks of all sizes have good practices for operational risk management, including an independent review of the performance of the Board of Directors and senior management regarding risk management.

7. It is also important that those good practices adopted for operational risk management by the more sophisticated and/or complex institutions in the Region be disseminated to the less complex institutions, so that they can be used as a point of reference for improving their frameworks for operational risk management.

CHAPTER 3

Tools Used to Identify, Evaluate, Monitor and Control Operational Risk

In general, managers at banking institutions are cautious in the face of corporate initiatives that imply financial costs with low tangible returns. Therefore, it is sometimes difficult to demonstrate that implementing an operational risk management program adds value to an institution.

As a result, it is important to make the effort to generate a precise estimate of operational risk. The apparent lack of tangible evidence of the actual cost of operational risk can be explained, up to a certain point, due to the distribution of its impact on different areas of the bank.

Consistent with Principle 4 of the Sound Practices document of the Basel Committee, banks should use the relevant tools available to identify and evaluate the operational risk inherent in all products, activities, processes and systems.

Specific tools exist to support the identification, assessment, monitoring and control or mitigation of operational risk. These tools allow many banks to realize a much more complete analysis of operational risk and reduce their reliance on mechanisms of internal control within business lines, supplemented by the internal audit function, for managing operational risk. The BIS document, "Sound Practices for the Management and Supervision of Operational Risk", paper identifies several examples of such tools, including: self-assessment of risk, risk mapping, risk indicators, scenario analyses and the measurement or quantification of exposure to operational risk through a variety of approaches.

3.1
OVERVIEW

The data survey provided the following overview of the Region regarding operational risk management tools.

3.1.1
Operational risk management tools

Generally speaking, countries participating in the survey reported that entities of all sizes use methodologies and tools of operational risk management. However, as might be expected, implementation of methodologies and tools for managing exposure to operational risk was more prevalent among large, more complex institutions than was reported for mid- and small-sized entities, with small-sized entities as the least frequent users of such instruments.

For example, out of thirteen countries, six (Canada, Colombia, Netherlands Antilles, Peru, Spain and the United States) reported that all large banks have implemented methodologies and tools to manage operational risk. Three countries (Brazil, Cayman Islands and Chile) reported that most large banks have implemented such methodologies and tools, while an additional three (Argentina, Paraguay and Uruguay) reported that only some large banks have done so.

In contrast, only two countries (Colombia and the United States) indicated that all small banks have implemented operational risk methodologies and tools to manage opera-

tional risk, while only one country (Netherlands Antilles) reported that the majority of small banks use such tools. In addition, seven countries (Brazil, Canada, Cayman Islands, Chile, Peru, Spain and Uruguay) reported that only some small banks had implemented methodologies and tools to manage operational risk. Responses for medium banks generally fell between the figures reported for large and small banks.

In terms of specific practices or tools used, self-assessments (sometimes called "risk and control self-assessments") are the predominant form of operational risk management practices reported by the countries in the Region. Generally speaking, self-assessments are required within the Region on an annual basis unless circumstances demand them more often. A majority of countries reported that all or a majority of large and medium-sized banks and some small banks use self-assessments.

It is worth mentioning that while two countries (Colombia and the United States) reported that all their small banks had implemented the use of such methodologies and tools, two other countries said that none of their banks carry out self-assessments.

Generally speaking, countries in the Region typically do not make extensive use of scenario analysis nor do they depend much on internal models for the quantification of operational risk. With regard to scenario analysis, only four countries (Cayman Islands Colombia, Spain and the United States) reported their use in all or most of their large banks. The ten countries that answered this survey question indicated that only some or none of the medium or small banks use scenario analysis.

As for the use of internal models, their use is slightly more prevalent at large entities, with eight countries (Brazil, Canada, Cayman Islands Colombia, Paraguay, Spain, the United States and Uruguay) reporting that all or some large banks use internal models. In contrast, seven countries reported no use of internal models at medium and small banks.

Tools such as key risk indicators and risk maps are more widely used, the survey showed. As would be expected, use of these tools was more prevalent at larger entities. Nevertheless, use of these tools was reported for all size of banks in a majority of countries. With respect to key risk indicators, ten out of twelve countries (Brazil, Canada, Cayman Islands, Chile, Colombia, Netherlands Antilles, Peru, Spain, the United States and Uruguay) reported that all or most large banks use them. In addition, a majority of countries reported that most or some medium banks, and most or some small banks use risk indicators. Very similar results were reported for the use of risk maps.

Supervisors in the Region were asked to report on the use of regulation, guidance and well-established supervisory practices as means for strengthening or encouraging the use of specific operational risk management tools, such as those discussed above, by banks in their jurisdictions. In response, the use of regulatory practices was reported in five countries (Argentina, Colombia, Mexico, Netherlands Antilles and the United States), while the use of supervisory practices was reported in six countries (Brazil, Canada, Netherlands Antilles, Peru, Spain and Uruguay). In addition, the use of guides was reported in three countries (Canada, Netherlands Antilles and Uruguay).

Among the countries that did report the existence of regulation, guidance or well-established supervisory practices regarding operational risk, most indicated that they do not establish specific requirements for the use of particular tools. In these cases, the norms point more to best practices and make recommendations for minimum standards for the identification, quantification, control and mitigation of operational risk.

3.1.2
Information and documentation

Thirteen supervisors in the Region responded about reporting and documentation practices. In general, larger entities were found to be more diligent in terms of reporting their exposure to operational risk to the Board of Directors and to senior management, more so than were medium- and small-sized entities. However, responses varied widely and most countries reported that at least some entities have procedures for such reporting.

For example, seven countries (Canada, Chile Colombia, Netherlands Antilles, Peru, Spain and the United States) stated that all or most of their large banks report their exposure and ability to manage operational risk to their Board of Directors. Six countries (Brazil, Canada, Chile, Colombia, Netherlands Antilles and Peru) reported that all or most of their medium banks report this exposure. Only four countries reported that all or most of their small banks report those exposures to their Board of Directors.

Finally, most of the countries reported that all or most of their large banks have these systems well documented, while eight countries reported the same holds true for medium-sized banks. Only three countries reported that documentation of these systems also exists for small banks.

3.1.3
Contingencies and business continuity plans

Survey responses indicated the consistent use of contingency and business continuity plans among banking institutions in the Region. All countries reported the use of such plans among some banks of all sizes, especially to address cases of serious and negative episodes.

A majority of countries reported that all or most of the large banks have these plans in place. Similarly, eight countries (Canada, Cayman Islands Chile, Colombia, Netherlands Antilles, Peru, the United States, Peru and Uruguay) reported that all medium banks have contingency plans, while five countries (Brazil, El Salvador, Nicaragua, Paraguay and Spain) reported that most of their medium-sized banks have contingency plans. Finally, five countries (Cayman Islands, Colombia, Chile, Peru and Uruguay) reported that all their small banks have contingency plans, while an additional six countries (Brazil, Canada, El Salvador, Netherlands Antilles, Paraguay and Spain) reported that most of their small banks have these plans.

In general, these contingency and business continuity plans are analyzed at a a minimum of once a year, and in at least one country (Brazil), the large and medium banks conduct such tests every six months or more often. Several countries also reported that small banks conduct such testing less frequently than once a year.

3.2
GOOD PRACTICES AND RECOMMENDATIONS

After analyzing tools in use regarding operational risk, the Group established the following good practices and recommendations:

1. Each financial institution should implement the combination of tools that will help it improve its operational risk management, taking into account the entity's size, complexity and risk profile.

2. Regardless of the size of financial institutions, they should be capable of recognizing the areas in which they are most vulnerable to losses and evaluate the controls in place for reducing the probability or impact of such losses.

3. Although scenario analysis is more commonly used by large banks, even the smallest institution should be capable of considering internal or external scenarios that could represent a threat to the bank. A greater use of scenario analysis by medium and small institutions would help generate more and better information, which institutions can incorporate in the self-assessment process and for evaluating contingency plans. Likewise, self-assessments should be encouraged for small banking institutions.

4. It is important to disclose to the Board of Directors and senior management information about the exposure to operational risk of the institution and about its operational risk management. While the data for large banks could be quantitative in nature, qualitative data could be useful for small banks to create awareness in the Board of Directors and senior management of the potential vulnerabilities to operational risk of the institution and of its ability to manage the risk. It is also important to assess periodically the exposures to operational risk, given that internal and external conditions change constantly.

5. Although the use of contingency and business continuity plans appears to be quite widespread throughout the Region, it is important that supervisors require banks, independently of their size, to review these plans at least on an annual basis.

CHAPTER 4

Recording and Classifying Data on Losses Owing to Operational Risk

In line with the objective of effectively monitoring its exposure to operational risk, a financial institution should have adequate early warning indicators to detect increases in its exposures to risk. The accurate recording of loss events is the primary input for developing those indicators, so the reliability of these records is extremely important.

As a consequence, it is necessary to ensure that these records are complete and are structured in a way that facilitates data processing in order to develop a minimal group of indicators necessary for effectively managing operational risk.

4.1
OVERVIEW

The questionnaire provided the following overview of the Region in terms of data recording and classification.

4.1.1
Data gathering on operational loss events

As mentioned, a majority of large banks in the Region gather data on loss events due to operational risk. Indeed, seven countries (Brazil, Canada, Chile, Colombia, Netherlands Antilles, Spain and the United States) have confirmed that all of their large banks compile this type of information.

In addition, the survey finds that four countries (Colombia, Netherlands Antilles, Peru, and Uruguay) state that all their medium-sized banks gather data about operational losses, while two countries (Colombia and Netherlands Antilles) have stated that all of their small-sized banks do so.

Obviously, the largest banks have shown the greatest propensity to gather this type of data. This could be explained by the fact that the largest banks, unlike the medium or smaller ones, are planning in the near future to advance toward sophisticated models to quantify exposure to operational risk, and therefore, they will need to have sufficient data regarding operational risk loss events.

4.1.2
Lower monetary limit to consider a loss due to operational risk

Although only half of the countries answered the questionnaire on this topic,,it is evident that in a majority of cases, there is no minimum limit for recording loss events. In those few cases where a limit does exist, it is low ($1,000 in Argentina and $5,000 in the Cayman Islands). It has been observed that in general terms, whether or not there is a minimum limit, the same criteria are adopted for all business lines. In only a few cases are differentiated limits by product type in use.

4.1.3
Loss records

In general terms, it is quite evident that in those cases where a loss record for operational risk losses is maintained, the banks in the Region, regardless of size, use multiple dates (date of actual loss event, discovery date, date loss recorded) for recording those losses (Argentina, Brazil, Canada, Peru, Colombia, and Uruguay). The general trend is to gather both the gross value and the net value in the loss record.

Methodologies for grouping losses vary according to the size of the institution. Generally, larger institutions group together losses that are the result of the same event, while smaller banks do not.

A greater detail in the information reported in the data collection process (the use of various dates to register events, as well as the gross and net values of losses), will be an advantage in developing better numeric models for measuring operational risk in the future.

4.1.4.
Quasi-losses

Quasi-losses are operational events that do not result in financial losses; not because a warning indicator had identified the potential exposure, but rather for purely circumstantial reasons. Only eight countries that replied to the survey responded about recording quasi-losses. Among those that did respond, the survey showed that it is a common practice for banks of all sizes to record these events in their loss data base.

4.1.5
Reconciliation between the loss database and accounting

Reconciling the difference between the operational loss database and the accounting record is a very common practice among the countries that responded on this issue, regardless of the size of the bank. However, among the countries that replied to the survey, it is not common to compare the database of operational losses with other databases of losses.

4.1.6
Basel II 56-cell matrix

Among the countries that responded on this issue (Argentina, Brazil, Canada, and Uruguay), the use of a 56-cell matrix recommended by Basel II was a common practice, and this was even more pronounced among large banks. A minority of countries use of an alternative matrix similar to the one set forth in Basel II, and even fewer use a matrix that is not similar to that of Basel II.

Among the large banks that use the 56-cell matrix of Basel II, it is common practice to define policies for assigning the lines of business to the rows of the matrix. This practice is found to a lesser degree in medium- and small-sized banks. The allocation of possible loss events to the seven events defined by the Basel matrix is also very common. Therefore, it can be concluded that the Basel II framework is the main point of reference in the Region for developing data collection methodologies.

4.1.7
Consortiums or other systems for data sharing

Very few countries responded to the part of the questionnaire that corresponds to this topic. Among those that did, the consortium with the greatest membership is the ORX System. Other consortiums that were mentioned, but to a lesser degree, were ABA and GOLD.

4.1.8
Indicators used

As regards risk indicators used, only Brazil, Canada, Peru and Spain responded in detail to this point. The following is a list of certain indicators that were mentioned:

- number and value of transactions
- unconfirmed transactions
- transaction failures (frequency)
- severity indicators
- turnover
- overtime
- input per line
- headcount (number of employees)
- layoff/dismissal of personnel
- process efficiency
- account reconciliation
- manual processes
- incidents with customers
- application adjustment
- contracts with vendors

4.2
GOOD PRACTICES AND RECOMMENDATIONS

After analyzing the issue, the Group provides the following sound practices and recommendations.

1. Collect detailed information on all loss events due to operational risk and enter them in comprehensive databases. This will facilitate a much better assessment of the degree of exposure to operational risk and a better design of early warning systems.

2. Record all operational risk losses or, if this is not possible, define a low threshold for gathering data on loss events so that the database is as comprehensive as possible.

3. Register the different dates of the loss events (occurrence, detection, and posting), which will make it possible to have an idea of the periods linked to each stage in the evolution of losses.

4. Record not only the gross value but also the net value of the loss, which will provide a better idea of the success of the entity in managing, mitigating or decreasing the volume of gross losses.

5. Group together losses associated with the same event, which will offer an adequate way of measuring the full impact of an event.

6. Collect data, to the extent possible, on the quasi-loss events. The lack of considering quasi-losses could result in an underestimation of the operational risk exposures of banking organizations.

7. Reconcile the loss event database with the accounting records.

8. Assign operational losses of an institution to the 56-cell matrix defined in Basel II, allocating the loss events among the seven types defined by the matrix. Similarly, there must be policies for adapting the internal business units to the rows of the matrix.

CHAPTER 5

Internal Auditing of Operational Risk

Sound corporate governance dictates that an effective internal control system should be supplemented by independent and effective internal and external audit functions. Moreover, the experience of banking institutions indicates that it is vital to establish a constructive and efficient relationshiop between senior management, auditors and banking supervisors in order to ensure the effectiveness of audits and the supervisory function.

The Basel Committee indicates that the Board of Directors of a bank is responsible for ensuring that senior management establishes and maintains an adequate and efficient internal control system as well as a framework to ensure compliance with laws, regulations and policies. Therefore, it is necessary that the Board of Directors review internal control systems at least once a year.

For its part, the senior management team of a bank is charged with developing processes that identify, quantify, manage and control the risks that the bank incurs. The bank's senior management should inform the Board of Directors periodically about the scope and functioning of the internal control systems.

5.1
OVERVIEW

Supervisors in surveyed countries were asked if the internal audit makes a periodic review of the following items:

- the operational risk management framework and its implementation;
- policies, processes and procedures for operational risk management;
- the review and validation of tools used to identify, assess, monitor and control operational risk;
- the integration of the assessment system of this risk in daily management of the entity;
- the documents that inform the control units about the evolution of operational risk;
- the integrity and consistency of data;
- technological infrastructure and information systems that support the databases;
- contingency and business continuity plans and documentation about the system of operational risk.

In nine countries (Argentina, Brazil, Canada, Cayman Islands, Colombia, Nicaragua, Peru, Spain and the United States), the internal audit reviews periodically almost all the items listed above, be it in all or in most of the entities of those countries. For example, in Mexico, internal audit carries out a review at least once a year of the comprehensive management of risk, the scope of which includes most of the aspects previously described.

The survey pointed out that in half of the countries reviews of operational risk management are performed at least once a year. In general, the frequency of reviews is adjusted according to the size, complexity and risk level of the entities being audited.

Regarding the establishment of regulations, guidelines or supervisory practices related to the periodic review by the internal audit of operational risk, the survey results

show that, in a majority of cases, the audit responds to the supervisory guidelines or practices. Seven countries (Argentina, Chile, Colombia, Nicaragua, Peru, Spain and Uruguay) stated that they have special regulations about the tasks the internal audit has to carry out in relation to operational risk.

In this regard, the general regulation issued by the Bank of Spain in June 2008 contains specific provisions regarding operational risk and which aspects should be reviewed by the internal audit. At the same time, the Superintendency of Colombia, in its document, Reglas Relativas a la Administración del Riesgo Operativo (Rules Related to the Management of Operational Risk), has established that internal audit is one of the departments responsible for assessing the operational risk management system.

In Peru, the Reglamento de Auditoría (Regulation of Auditing) and the Requerimiento de Patrimonio Efectivo por Riesgo Operacional (Requirement of Cash Reserves for Operational Risk) establish the responsibilities of internal audit for management of operational risk.

The survey reveals that Chile and Uruguay have established some type of regulation that requires the internal audit make a periodic review of administration of operational risk.

5.2
GOOD PRACTICES AND RECOMMENDATIONS

After analyzing internal audit of operational risk management, the Group has established the following sound practices and recommendations for supervisors.

1. Bank supervisors should verify that sound and adequate audit systems are established that review the policies and procedures of operational risk management.

2. Banking supervisors should ensure that internal audit has included in its annual plan the comprehensive review of operational risk management and that the plan has been approved by the Board of Directors. Supervisors should also verify the content and scope of the plan to ensure that it has been adapted to the size, complexity and risk profile of the entity.

3. Reports issued by internal audit must be analyzed, and the supervisor should verify that these are sufficiently clear, that they point out the tasks that were carried out and include the weaknesses observed and recommendations. In addition, reports should include comments of the audited unit and a listing of corrective actions to be taken, the person in charge of them and the approximate date for completion.

4. Supervisors should verify that the internal audit makes a review to confirm that the established operational policies and procedures are effective for operational risk management and that the Board of Directors, through its audit committee, checks that the scope and frequency of the auditor's program are reflective of the bank's exposure to operational risk.

5. When banks use quantitative models, internal audit programs should verify the following: the inclusion of the operational risk model into daily management of the entity; enforcement of internal regulation about operational risk; assessment of the adequacy of the bank's information system and the relevance, quality and integrity of the data used in the model.

6. The internal auditing department is responsible for supervising the enforcement, suitability and effectiveness of internal

control procedures, including electronic data systems.

7. The auditing department should ensure that the Board of Directors has approved and periodically reviews the framework applied by the bank for operational risk management. This framework must explain clearly the methods for defining, assessing, monitoring and controlling this risk. The degree of formality and complexity of this framework should be commensurate with the risk profiles of the entity. Moreover, the framework should be periodically updated in accord with changes in the market, new products, activities of the bank and methods of processing transactions.

8. The audit department should verify that bank management has developed the methodology, criteria and procedures necessary for adequate development of the operational risk management model. The audit must also review that framework for management of operational risk, defined by the Board of Directors, is expressed in specific policies, processes and procedures.

9. The internal audit should assess the policies and procedures that make up the operational risk model to see that they include all the relevant bank activities and processes and whether they have been properly documented in a manual and communicated throughout the whole organization. At the same time, the audit must evaluate whether clear lines of authority and responsibility for operational risk management have been established and if sufficient resources and qualitative and quantitative tools have been allocated for managing this risk effectively.

10. The internal audit should determine whether adequate communication exists between those responsible for managing operational risk and those in charge of other risks, in order to avoid gaps or overlapping in the managing of risks and to make sure that adequate reporting mechanisms and formats have been designed and maintained.

11. The internal audit must verify the way in which the identification and measurement of operational risk are derived and how follow-up work is done to ensure that the process is effective for actively managing operational risks and reducing exposure to these types of risks.

12. The supervisor should verify follow-up and review whether effective, specific and timely actions are taken as a result of recommendations made by the auditing unit. The results of the follow-up should be included in reports presented to the Board of Directors, senior management and other areas of the bank that participate in the process.

13. The tasks of the internal audit should include a review to be sure that contingency plans exist as this will allow continuity of critical processes of the entity. Contingency plans should be reviewed to see that they are adequately updated, and their effectiveness should be tested periodically.

CHAPTER 6

Disclosure of Information

Recent events that triggered the collapse of some financial institutions have left little doubt about the importance of transparency and data disclosure related to the organization and management of risks assumed by entities in their daily operations. Therefore, requirements established by supervisors are critical, together with the daily practices of the entities and the demands of the functioning of markets.

In this chapter, progress in data disclosure in the Region regarding operational risk will be analyzed.

6.1 OVERVIEW

In most countries of the Region, requirements have been established so that the financial entities provide data to the supervisors, markets and the public in general about the framework for operational risk management. However, five countries (Cayman Islands, Chile, El Salvador Netherlands Antilles and Paraguay) reported that their regulations do not require any type of data disclosure about operational risk.

Among the countries that gave a positive answer, the disclosure requirements vary. But, they have in common that all report publicly on the organization and functioning of operational risk management.

In some cases, as in Argentina, it is the banking institution's responsibility to develop a disclosure policy and ensure that the content of the information is reflective of the volume, complexity and risk profile of the entity. On the contrary, in another group of countries that includes Brazil, Colombia and Peru, the supervisory authority dictates what type of operational risk data the entities must disclose.

Finally, the remaining countries that demand data disclosure on risk consider disclosure of operational risk data to third parties as part of a broader disclosure framework which includes a comprehensive discussion of the management of all risks. However, no specific requirements for disclosure on operational risk are mandated.

It should be highlighted that Canada and Spain, countries where Basel II capital requirement calculation methodologies have been implemented, demand that their banking entities publish the amount of capital requirements separately by type of risk and explain the methodology used for the calculation.

6.2 GOOD PRACTICES AND RECOMMENDATIONS

The Basel Committee establishes that banks should make available to the public sufficient information to allow market participants to evaluate their strategies for operational risk management and that this reinforces market discipline[5]. The Commit-

5 Sound Practices for the Management and Supervision of Operational Risk. Basel Committee. February 2003.

tee also establishes that the information to be disclosed should depend on the volume, risk profile and complexity of the bank's transactions.

According to the criteria of the Basel Committee, establishes that it is advisable that the information to be disclosed meet the following requirements:

- It should correspond to the accounting records. All complementary information that is published should be capable of being reconciled with the audited statements, which will be considered as a filter for validation.

- Information should be relevant. Relevant information is data where "...its omission or erroneous assertion could modify or influence the assessment of a user who depends on this information for making economic decisions." However, the bank is the entity that determines the relevance of the information to be disclosed.

- Information must be disclosed to the market periodically . In general, periodicity of disclosure is every six months, except in the case of objectives and policies that refer to risk management, and these may be published once a year.

The Committee understands that the entities should exclude disclosure of confidential information on their customers and proprietary information that, if shared with competitors, would reduce the value of the bank and undermine its competitive edge.

As we have seen, most of the countries in the Region have established requirements for data disclosure by their entities, yet many of them could improve the content of disclosures. In this regard, the Group makes the following recommendations.

1. Financial entities should include in their financial statements a separate section where they present a summary description of the operational risk policies and procedures, as well as the approaches used by the Board of Directors and senior management to quantify the risk and the measures adopted to mitigate it.

2. Supervisors should include in their manuals and formal procedures of in-situ and extra-situ examination a description of the tasks involved in operational risk supervision.

3. Supervisors should include in their periodic written reports the progress observed in the application of sound practices of operational risk management in the entities under their oversight, identifying their strengths and weaknesses.

4. In order to strengthen transparency, it is necessary to have a proper legal framework that supports initiatives to provide the public with information.

5. Information should be disclosed periodically at least once a year, and supervisors should verify the reliability and accuracy of the information that is disclosed.

The disclosure of information is an important element of sound operational risk management practices. Those countries that already require data disclosure should enhance these requirements by establishing minimal conditions for this information to be considered sufficient, adequate and released at regular intervals. For those countries that do not yet have data disclosure requirements, it is recommended that, to the extent possible, they incorporate the requirements mentioned above in their regulations.

CHAPTER 7

Challenges Towards Basel

Although the Group's work does not focus on studying specific capital requirements established by Basel II for covering operational risk, but rather on providing an overview of managing this risk and providing recommendations for supervision. Nonetheless, the Group considered it pertinent to explore in this chapter the degree of progress in implementing the New Capital Framework in the Region as it relates to operational risk.

7.1 OVERVIEW

In general, few countries in the Region have implemented operational risk capital requirements. Only six of the fifteen countries (Brazil, Canada, Mexico, Peru, Spain and the United States) that responded to the survey include in their regulations some type of capital requirement for this risk.

One of the first matters to take into account is that all the countries that have established capital requirements for operational risk have done so by concurring with the methods and requirements established by the Basel II framework although, in some cases, this framework has been adjusted conforms to the current economic and financial situation of the specific country.

Thus, for example, Brazil has decided to implement the simplest Basel II methods to calculate capital requirements in the areas of credit, market and operational risk. Regarding operational risk, the entities are offered the possibility of choosing between the Basic Indicator Approach and the Alternative Standardized Approach. The Standardized Approach has been excluded and a long-term schedule, which extends beyond 2012, has been considered for the implementation of the Advanced Measurement Approaches (AMA).

In Mexico, supervisors have decided to implement the simplest method, the Basic Indicator Approach. However, the regulators require that implementation of this method be carried out in conjunction with the development of certain tools for gathering data about operational risk events so that, in the future, the financial system is prepared to apply more advanced and complex methods. In the case of Peru, the Basic Indicator Approach, Alternative Standardized Approach, and AMA are available.

Canada and Spain have decided to implement Basel II for calculating operational risk capital requirements and to accept in their regulation the possibility that all methods established in Basel II can be utilized and that the entities themselves be the ones to decide the methodology that fits best with their risk management system.

On the contrary, the United States has only considered requiring implementation of the AMA by the largest entities. The possibility that the remaining banking companies continue using Basel I models or use a simpler approach to calculate their capital requirements for operational risk is under study. The process of deciding the capital requirements for operational risk is now in the preliminary stage and will have to pass through different screening and consultation procedures; therefore, there is no definitive date for its implementation.

Diverse situations exist among those countries that have still not implemented any capital requirement for operational risk. Some countries have already approved regulation on operational risk management and foresee establishing capital requirements for operational risk in the short term. For example, Cayman Islands

and Colombia have secheduled implementation before the second half of 2010. Other countrieshave not yet contemplated establishing any type of capital requirements for operational risk.

Although almost all of these countries express their intention to establish capital requirements for operational risk in the future, most have no definitive implementation date in mind or plan to do this after 2010.

In addition, there are two cases, Chile and El Salvador, where regulatory changes necessary for the application of Basel II affect national laws, so legislative bodies must first approve changes in the law, which involves delays and uncertainties for implementation of Basel II.

With respect to operational risk capital requirements, countries in the Region have opted for the application of the New Capital Framework of Basel (Basel II), even though the degree of progress and the speed of implementation are very distinct in the different countries. In this sense, the countries can be divided into four distinct groups:

- Those countries where all the Basel II methods for calculating operational risk capital requirements have been implemented.

- A second group of those countries where partial implementation has taken place. In those countries, only some Basel II methods have been established, those that supervisors consider the most appropriate to the situation of their financial system. In some cases, such as Mexico, the application of these methods goes hand-in-hand with the requirement that entities implement tools that gather information on operational risks that will allow the application of more advanced methods for calculating capital requirements for operational risk at a future date.

- A third group of countries is already studying the implications of incorporating operational risk in its overall management process and have established regulations to ensure that this risk is properly managed. These countries are studying how to establish operational risk capital requirements and have established a timeline for implementation.

- Finally, there is a fourth group of countries that, recognizing the importance of an adequate approach to manage and measure operational risk, has still not decided how or when to implement their own supervisory requirements for operational risk capital.

The distinct speeds and degree of implementation of operational risk capital requirements have much to do with the heterogeneity and diversity of financial systems in the Region. The less sophisticated financial systems have just initiated implementation of Basel I and so are still far removed from being able to initiate the transition towards Basel II.

It should also be noted that Basel II has been calibrated for the financial situation of the countries that are members of the Basel Committee and reflects, to a large degree, the characteristics of their financial systems. The financial situation of some of the countries in the Region can be very different, in which case their supervisors should adjust Basel II to their own specific needs. This adjustment process can be a very complex activity that would require, in the first place, carrying out an evaluation of the local financial system in order to later determine which of the facets of Basel II can best be adapted to the country.

Another difficulty to consider regarding the establishment of capital requirements for operational risk is the changing profile of some of the financial systems in the Region. The last decade has produced great changes in those systems: the concentration of assets in fewer entities of larger size, increasing globalization and the penetration of large international financial groups that, at times, have

displaced or are competing with local institutions. In recent years, acquisitions and mergers of financial institutions have taken place in the Region, creating complications for maintaining sound and harmonized databases which are indispensable for the correct application of Basel II in its most advanced alternatives.

Finally, as mentioned, in some countries the implementation of Basel II will require considerable time given that it entails legislative changes that would require having either a sufficient majority in their legislative bodies or a high-level political consensus, and neither is easy to obtain.

7.2 RECOMMENDATIONS

Taking this information into consideration, there is a clear will on the part of supervisors to implement operational risk capital requirements consistent with Basel II, even though the timeframe differs according to the country.

Of course, local supervisors are the most appropriate officials for setting an appropriate pace for implementation of capital requirements in their financial system because they are most familiar with local financial practicesand the legal and economic conditions of their respective countries.

The various international fora, such as ASBA, and cooperation and coordination among supervisors of the different countries of the Region provide adequate support for the exchange of ideas and experiences. Supervisors who have participated in drafting Basel II and who have implemented this framework will be able to share and communicate their knowledge and experiences to other supervisors.

In addition to obtaining support from international sources, the supervisors of the countries that have not yet implemented Basel II could establish the following measures:

1. First, it is essential that supervisors carry out an evaluation of the treatment of operational risk in the financial institutions of their jurisdiction. The supervisors must define the events that imply operational risk and should identify the processes, procedures and tools that these institutions have in place to manage operational risk.

2. Subsequently, and according to the degree of sophistication of different financial institutions for handling operational risk, measures to manage and control operational risk can be adopted. Later, supervisors can require the implementation of different tools to measure operational risk, which will allow entities to calculate operational risk capital requirements in the future. In this regard, it is important to learn from the experience of some countries whose financial institutions implemented measures of control and management of operational risk years ago and are now designing tools to establish capital requirements.

3. In the early stages of development of operational risk management, simple calculation methods for operational risk capital requirements can be applied so that the entities begin to become aware of this risk and to take the necessary steps regarding its control and oversight. Data should be gathered that will later serve as an input for more advanced models that can be put in place in the future.

4. In this regard, the gradual application of the different calculation methods for opera-

tional risk capital requirements (Basic Indicator Approach, Standardized or Alternative Standardized Approach, and the AMA) should take into account the degree of sophistication of the entities that make up the financial system in the different countries. As the entities become more sophisticated, they will be able to apply the more complex methods for calculating operational risk capital requirements.

To achieve all of these changes and practices requires the active participation of supervisors who will have to undertake, in many cases, a process of training and modernizing their staff so they can provide the necessary technical support to the entities in their country.

As previously note, a clear willingness to implement operational risk capital requirements exists in most of the countries in the Region, and the calculation of these risks will follow, in general terms, the principles of Basel II. However, local supervisors also seem to be adamant that the application of international standards be carried out only so long as the legal and financial characteristics of their banking systems are respected.

In this regard, the practical advances of some of the countries in the Region could serve as a guide, together with international standards, to help with the implementation of capital requirements in other countries that are still in the initial stages of the process. It would also be advantageous for these countries to have the support and advice from those international fora that specialize in operational risk.

CONCLUSIONS FOR SUPERVISORS IN THE REGION

Having analyzed different aspects of operational risk, the Group presents the recommendations that it considers essential so that supervisors in the Region can carry out an effective process of oversight of this risk.

1. Supervisors must require all banks and financial entities have an effective system in place that is able to identify, assess, monitor, control and mitigate operational risks in all their lines of business.

2. Operational risk management should not be dissociated from other risk management processes inherent to financial intermediation. On the contrary, operational risk management should be part of a comprehensive approach to risk management.

3. Supervisors must evaluate on an ongoing basis, through on-site and off-site examinations, that banks have strategies, policies, procedures and sound practices to adequately manage operational risk, and these must be recorded in writing and duly approved by the Board of Directors.

4. Supervisors should ensure that the operational risk management strategies, policies and procedures take into consideration the size, complexity and risk profiles of the supervised entities.

5. Supervisors should require that banks generate reports on operational risk that allow the Board of Directors, senior management and supervisors themselves, to carry out the oversight process for operational risk management and also monitor the implementation and application of adopted strategies, policies, and procedures regarding this risk.

6. Supervisors should encourage banks to disclose sufficient information to allow market participants to understand and evaluate the bank's exposure to risk, the quality of its management and the measures adopted to mitigate the exposure.

7. Financial institutions should record and accumulate historical data by business line and type of event in order to identify the following:

   - business unit risks
   - expected loss estimates
   - unexpected loss estimates
   - frequency of loss events
   - severity of loss events
   - trends in loss events

8. Data on the bank's historical experience of losses provide important information for assessing the bank's exposure to operational risk and are necessary to calculate capital requirements for this risk. It is important that supervisors provide guidance on how to design the records to collect these data.

MISSION

To develop, disseminate, and promote banking supervisory practices throughout the Americas in line with international standards. To support the development of banking supervision expertise and resources in the Americas, through the efective provision of training and technical cooperation services.

INSTITUTIONAL OBJECTIVES

The Association of Supervisors of Banks of the Americas is formed by the entities in charge of bankng supervision in each of the countries of the American continent and Spain. Its main objectives are:

- Promote and maintain close communication among the Association's Members, in order to facilitate co-operation among them, and to promote the improvement of their respective capabilities;
- Provide its members with a high-level discussion forum for the exchange of information, ideas, techniques, experiences and knowledge over their scope of competence ;
- Promote research as well as systematic and permanent training programs, with the purpose of establishing training standards in the region and providing technical co-operation services among its Members;
- Promote co-operation and exchange relationships with non-member bank supervisors, with similar associations as well as with international and multilateral institutions, engaged in activities similar to those of the Association; and
- Perform any general activity related to its purposes.