OPERATIONAL RISK MANAGEMENT MODULE

MODULE	OM Operational Risk Management
	Table of Contents

			Date Last Changed
OM-A	**Introduction**		
	OM-A.1	Purpose	01/2012
	OM-A.2	[This Chapter was deleted in October 2007]	10/2007
	OM-A.3	Module History	04/2012
OM-B	**General Guidance and Best Practice**		
	OM-B.1	[This Section was moved to Chapter OM-1]	10/2007
OM-1	**International Guidance and Best Practice**		
	OM-1.1	Guidance Provided by International Bodies	10/2007
OM-2	**General Guidance**		
	OM-2.1	Overview	01/2012
	OM-2.2	Developing an Appropriate Risk Management Environment	07/2011
	OM-2.3	Identification, Measurement, Monitoring and Control	07/2004
	OM-2.4	Succession Planning	07/2011
OM-3	**Outsourcing**		
	OM-3.1	Introduction	07/2011
	OM-3.2	Supervisory Approach	04/2012
	OM-3.3	Notifications and Prior Approval	01/2011
	OM-3.4	Risk Assessment	07/2011
	OM-3.5	Outsourcing Agreement	07/2011
	OM-3.6	Contingency Planning for Outsourcing	07/2011
	OM-3.7	Internal Audit Outsourcing	01/2011
	OM-3.8	Intra-group Outsourcing	01/2011
OM-4	**Electronic Money and Electronic Banking Activities**		
	OM-4.1	Electronic Banking	07/2011
OM-5	**Business Continuity Planning**		
	OM-5.1	Introduction	10/2007
	OM-5.2	General Requirements	10/2007
	OM-5.3	Board and Senior Management Responsibilities	07/2011
	OM-5.4	Developing a Business Continuity Plan	07/2011
	OM-5.5	BCP – Recovery Levels & Objectives	07/2011
	OM-5.6	Detailed Procedures for the BCP	07/2011
	OM-5.7	Vital Records Management	07/2011
	OM-5.8	Other Policies, Standards and Processes	07/2011
	OM-5.9	Maintenance, Testing and Review	07/2011

MODULE	OM Operational Risk Management
	Table of Contents (continued)

			Date Last Changed
OM-6	**Security Measures for Banks**		
	OM-6.1	Physical Security Measures	07/2011
	OM-6.2	Internet Security	04/2012
	Books and Records		
OM-7	OM-7.1	General Requirements	10/2011
	OM-7.2	Transaction Records	10/2007
	OM-7.3	Other Records	04/2011
	Basel II Operational Risk Qualitative Requirements		
OM-8	OM-8.1	Introduction	04/2008
	OM-8.2	Basic Indicator Approach	07/2011
	OM-8.3	Standardised Approach	04/2008

OM-A.1 Purpose

Executive Summary

OM-A.1.1 The Operational Risk Management Module sets out the Central Bank of Bahrain's ('CBB's') rules and guidance to Conventional Bank licensees operating in Bahrain on establishing parameters and control procedures to monitor and mitigate operational risks. The contents of this Module apply to all conventional banks, except where noted in individual Chapters.

OM-A.1.2 This Module provides support for certain other parts of the Rulebook, mainly:
(a) Principles of Business; and
(b) High-level Controls.

Legal Basis

OM-A.1.3 **This Module contains the CBB's Directive (as amended from time to time) relating to Operational Risk Management and is issued under the powers available to the CBB under Article 38 of the Central Bank of Bahrain and Financial Institutions Law 2006 ('CBB Law'). The Directive in this Module is applicable to all conventional bank licensees (including their approved persons).**

OM-A.1.4 For an explanation of the CBB's rule-making powers and different regulatory instruments, see Section UG-1.1.

OM-A.2 [This Chapter was deleted in October 2007]

OM-A.3 Module History

OM-A.3.1 This Module was first issued in July 2004 as part Volume one of the CBB Rulebook (Volume one). All directives in this Module have been effective since this date. Any material changes that have subsequently been made to this Module are annotated with the calendar quarter date in which the change was made; Chapter UG-3 provides further details on Rulebook maintenance and version control.

OM-A.3.2 When the CBB replaced the BMA in September 2006, the provisions of this Module remained in force. Volume 1 was updated in October 2007 to reflect the switch to the CBB; however, new calendar quarter dates were only issued where the update necessitated changes to actual requirements.

OM-A.3.3 The most recent changes made to this Module are detailed in the table below:

Summary of Changes

Module Ref.	Change Date	Description of Changes
OM-5.1	01/04/05	Physical security measures.
OM-4.2	01/10/05	Succession planning for locally incorporated banks.
OM-5.1	01/10/05	Clarification of security manager role for smaller banks.
OM-B & OM-1.2	01/04/06	Minor amendments concerning roles of Board and management.
OM-5.1.15-24	01/04/06	New security requirements for ATMs and reporting of security related complaints.
OM-A.2.1-6	01/10/07	Purpose (expanded)
OM-A.2.1-6	01/10/07	Key Requirements (deleted)
OM-2.1-2.2 & 2.4	01/10/07	Relocation of Succession Planning Requirements from OM-4
OM-5.1-OM-5.9	01/10/07	Business Continuity Planning (expanded)
OM-7	01/10/07	Books and Records Chapter transferred from Module GR
OM-8	01/04/08	Basel II Qualitative Operational Risk Requirements
OM	01/2011	Various minor amendments to ensure consistency in CBB Rulebook.
OM-A.1.3 and OM-A.1.4	01/2011	Clarified legal basis.
OM-7.1.4	04/2011	This Paragraph was deleted as Ministerial Order 23 does not apply to CBB licensees.
OM-7.3.4	04/2011	Clarified retention period of records for promotional schemes.
OM	07/2011	Various minor amendments to clarify Rules and have consistent language.
OM-2.4	07/2011	Amended CBB reporting requirements regarding succession planning.
OM-3.1.7	07/2011	Paragraph deleted as no longer applicable since standard conditions and licensing criteria document has now been incorporated as part of Volume 1.
OM-6.2	10/2011	Added new Section on internet security.
OM-7.1.7	10/2011	Corrected typo.
OM-A.1.3	01/2012	Updated legal basis.
OM-2.1.4	01/2012	Corrected cross reference.
OM-3.2.2	04/2012	Deleted last sentence of Paragraph as it repeats the requirement under Paragraph OM-3.3.1
OM-6.2.2	04/2012	Clarified penetration testing interval for internet security.

Evolution of the Module

OM-A.3.4 [Deleted in October 2007 updates]

OM-B.1 This Section was moved to Chapter OM-1.

OM-1.1 Guidance Provided by International Bodies

Guidance Provided by other International Bodies

OM-1.1.1 The papers below provide guidance which promotes best practice and can be generally applied by all licensees to their activities.

Basel Committee: Framework for Internal Controls Systems in Banking Organisations

OM-1.1.2 The paper (see www.bis.org/publ/bcbs40.pdf) issued in September 1998 presents the first internationally accepted framework for supervisors to use in evaluating the effectiveness of the internal controls over all on- and off-balance-sheet activities of banking organisations.

OM-1.1.3 The paper describes elements that are essential to a sound internal control system, recommends principles that supervisors can apply in evaluating such systems, and discusses the role of bank supervisors and external auditors in this assessment process.

Basel Committee: Sound Practices for the Management and Supervision of Operational Risk

OM-1.1.4 The paper (see www.bis.org/publ/bcbs96.pdf) issued in February 2003 by the Risk Management Group of the Basel Committee on Banking Supervision, outlines a set of principles that provide a framework for the effective management and supervision of operational risk, for use by banks and supervisory authorities when evaluating operational risk management policies and practices.

OM-1.1.5 The paper also recognises that clear strategies and oversight by the Board of Directors and senior management, a strong operational risk culture and internal control culture (including, among other things, clear lines of responsibility and segregation of duties), effective internal reporting, and contingency planning are all crucial elements of an effective operational risk management framework for banks of any size and scope.

OM-1.1 Guidance Provided by International Bodies (continued)

Basel Committee: Risk Management for Electronic Banking and Electronic Money Activities

OM-1.1.6 The paper (see www.bis.org/publ) issued in March 1998 provides guidelines for supervisory authorities and banking organisations as they develop methods for identifying, assessing, managing and controlling the risks associated with electronic banking and electronic money.

OM-1.1.7 The paper indicates that, while providing new opportunities for banks, electronic banking and electronic money activities carry risks as well as benefits and it is important that these risks are recognised and managed in a prudent manner.

Basel Committee: Risk Management Principles for Electronic Banking

OM-1.1.8 The paper (see www.bis.org/publ) issued in July 2003 recognizes new risks associated with the increase in distribution of financial services through electronic channels, or e-banking. To emphasize the importance of these risks, the Committee has placed responsibility on the shoulders of the Board and senior management to ensure their institutions have analysed, identified and modified operations to mitigate these risks.

OM-1.1.9 To facilitate these developments, the Committee has identified fourteen Risk Management Principles for Electronic Banking to help banking institutions expand their existing risk oversight policies and processes to cover their e-banking activities.

OM-1.1.10 The Risk Management Principles fall into three broad, and often overlapping, categories of issues that are grouped to provide clarity: Board and Management Oversight; Security Controls; and Legal and Reputational Risk Management.

Joint Forum: High Level Principles for Business Continuity

OM-1.1.11 This paper provides a broad framework for business continuity standards, and contains seven principles for regulators and industry participants to follow. It was published in August 2006 and is available in the "publications" section of the Basel Committee portion of the BIS website (www.bis.org).

OM-2.1 Overview

OM-2.1.1 This Chapter provides guidance and rules for operational risk and sets out requirements for an appropriate risk management environment, including business continuity, outsourcing and electronic banking. Operational risk is defined as the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. This definition includes legal risk, but excludes strategic and reputational risk.

OM-2.1.2 Operational risk is inherent in all types of banks' activities, and therefore all new products and services should be reviewed for operational risks prior to their implementation. As these risks are important and can result in substantial losses, bank auditors should include operational audits in the scope of all audits.

OM-2.1.3 The importance of operational risk has gained prominence as increasing reliance on sophisticated technology raises concerns of potential losses should unforeseen events cause technological failures. Banks have traditionally focused on controlling and mitigating credit and liquidity risks, however, enhanced levels of automation, while reducing costs and processing times, also pose potential risks. As such any one process or system failure may itself or through a series of systematic failures, cause financial or other losses to a bank. Therefore, it has become imperative that banks should establish policies and procedures to monitor and control operational risks.

OM-2.1.4 The CBB will use the papers mentioned in Paragraphs OM-1.1.1 to OM-1.1.11 as guidelines in evaluation of the internal control systems of banks operating in Bahrain. Such evaluations will be made through the CBB's normal supervisory processes (e.g. meetings with management, on-site examinations (Module BR) and the use of appointed experts (Section BR-6.5).

OM-2.2 Developing an Appropriate Risk Management Environment

OM-2.2.1 It must be standard practice for a bank's management to implement policies and procedures to manage risks arising out of a bank's activities. The bank must maintain written policies and procedures that identify the risk tolerances approved by the Board of Directors and must clearly delineate lines of authority and responsibility for managing the risks. Banks' employees and loan officers in particular must be fully aware of all policies and procedures that relate to their specific duties.

OM-2.2.2 The bank's strategy must define its tolerance for risk and lay out the Board's understanding of the specific characteristics of operational risk.

The Board of Directors

OM-2.2.3 The Board of Directors must be aware of the major aspects of the bank's operational risk as a distinct and controllable risk Category.

OM-2.2.4 The responsibilities of the Board of Directors of the bank must include:

(a) Approving the bank's operational risk strategy;
(b) Periodically reviewing the bank's operational risk strategy;
(c) Approving the basic structure of the framework for managing operational risk; and
(d) Ensuring that senior management is carrying out its risk management responsibilities.

OM-2.2 Developing an Appropriate Risk Management Environment (continued)

Senior Management

OM-2.2.5 **The responsibilities of the senior management of the bank must include:**

(a) Implementing the operational risk strategy approved by the Board of Directors;

(b) Ensuring that the strategy is implemented consistently throughout the whole banking organisation;

(c) Ensuring that all levels of staff understand their responsibilities with respect to operational risk management;

(d) Developing and implementing policies, processes and procedures for managing operational risk in all of the bank's products, activities, processes and systems;

(e) Developing succession plans for senior staff; and

(f) Developing Business Continuity Plans for the bank.

Management Information System

OM-2.2.6 The management information system of a banking organisation plays a key role in establishing and maintaining an effective operational risk management framework.

OM-2.2.7 *'Communication flow'* serves the purpose of establishing a consistent operational risk management culture across the bank. '*Reporting flow'* enables:

(a) Senior management to monitor the effectiveness of the risk management system for operational risk; and

(b) The Board of Directors to oversee senior management performance.

OM-2.3 Identification, Measurement, Monitoring and Control

OM-2.3.1 **As part of an effective operational risk management system, banks must:**

(a) Identify critical processes, resources and loss events;

(b) Establish processes necessary for measuring operational risk;

(c) Monitor operational risk exposures and loss events on an on-going basis; and

(d) Develop policies, processes and procedures to control or mitigate operational risk.

OM-2.3.2 Banks should assess the costs and benefits of alternative risk limitation and control strategies and should adjust their operational risk exposure using appropriate strategies, in light of their overall risk profile.

OM-2.4 Succession Planning

OM-2.4.1 Succession planning is an essential precautionary measure for a bank if its leadership stability – and hence ultimately its financial stability – is to be protected. Succession planning is especially critical for smaller institutions, where management teams tend to be smaller and possibly reliant on a few key individuals.

OM-2.4.2 **The CBB requires locally incorporated banks to document their Board-approved succession plans for their senior management team and have these ready at any time for onsite inspection by CBB staff.**

OM-2.4.3 **[This Paragraph was deleted in July 2011].**

OM-3.1 Introduction

OM-3.1.1 This Chapter sets out the CBB's approach to outsourcing by licensees. It also sets out various requirements that licensees must address when considering outsourcing an activity or function.

OM-3.1.2 **In the context of this Chapter, 'outsourcing' means an arrangement whereby a third party performs on behalf of a licensee an activity which was previously undertaken by the licensee itself (or in the case of a new activity, one which commonly would have been performed internally by the licensee). Examples of services that are typically outsourced include data processing, customer call centres and back-office related activities.**

OM-3.1.3 Most of the Directives in this Chapter are concerned with situations where the third party provider is outside the licensee's group. Section OM-3.8, however, sets out the CBB's requirements when a service is outsourced to a company within the licensee's group.

OM-3.1.4 **The requirements in this Chapter only apply to 'material' outsourcing arrangements. These are arrangements that, if they failed in any way, would pose significant risks to the on-going operations of a licensee, its reputation and/or quality of service provided to its customers. For instance, the outsourcing of all or a substantial part of functions such as customer sales and relationship management, settlements and processing, IT and data processing and financial control, would normally be considered 'material'.**

OM-3.1.5 Management should carefully consider whether a proposed outsourcing arrangement falls under this Chapter's definition of 'material'. If in doubt, management should consult with the CBB.

OM-3.1.6 **The requirements in this Chapter only apply to outsourcing arrangements entered into after May 2003. In the case of pre-existing outsourcing agreements, the CBB requires licensees to apply the requirements of this Chapter to the fullest extent possible when these arrangements are subsequently renewed.**

OM-3.1 Introduction (continued)

OM-3.1.7 [This Paragraph was deleted in July 2011].

OM-3.2 Supervisory Approach

OM-3.2.1 The CBB recognises the benefits that can potentially be achieved through outsourcing an activity to a third party provider. They can include reduced costs, enhanced service quality and a reduction in management time spent on non-core activities. However, outsourcing an activity also poses potential risks. These include the ability of the service provider to maintain service quality levels, reduced control over the activity and access to relevant information, and increased legal and client confidentiality risks.

OM-3.2.2 **The CBB's approach is to allow licensees the freedom to enter into outsourcing arrangements, providing these have been properly structured and associated risks addressed.**

OM-3.2.3 **The CBB expects licensees to have undertaken a thorough assessment of a proposal before formally submitting a notification to the CBB. However, the CBB is also willing to discuss ideas informally at an early stage of development, on a 'no-commitment' basis. It especially encourages an early approach when the proposed outsourcing is particularly material or innovative.**

OM-3.2.4 **Once an outsourcing arrangement has been implemented, the CBB requires a licensee to continue to monitor the associated risks and the effectiveness of its mitigating controls. It will verify this through the course of its normal on-site and off-site supervisory processes, such as prudential meetings and on-site examinations. The CBB also requires access to the outsourced activity, which it may occasionally want to examine itself, through management meetings or on-site examinations.**

OM-3.2.5 **Fundamental to the CBB's supervisory approach to outsourcing is that the Board and management of the licensee may not abdicate their responsibility for a licensee's business and the way its customers are treated. The Board and management remain ultimately responsible for the effectiveness of systems and controls in outsourced activities.**

OM-3.3 Notifications and Prior Approval

OM-3.3.1 A licensee must formally notify the CBB and seek its prior approval before committing to a new material outsourcing arrangement.

OM-3.3.2 The above notification must:

(a) Be made in writing to the licensee's normal supervisory contact;

(b) Contain sufficient detail to demonstrate that relevant issues raised in Section OM-3.4 onward of this Chapter have been addressed; and

(c) Be made at least 6 weeks before the licensee intends to commit to the arrangement.

OM-3.3.3 The CBB will review the information provided and provide a definitive response within 6 weeks of receiving the notification. Where further information is requested from the licensee, however, the time taken to provide this further information will not be taken into account. The CBB may also contact home or host supervisors of the licensee or the service provider, to seek their comments – in such cases, the 6-week turnaround is also subject to the speed of their response.

OM-3.3.4 Once an activity has been outsourced, a licensee must immediately inform its normal supervisory contact at the CBB of any material problems encountered with the outsourcing provider. In exceptional cases, the CBB reserves the right to direct a licensee to make alternative arrangements for the outsourced activity.

OM-3.4 Risk Assessment

OM-3.4.1 **Licensees must undertake a thorough risk assessment of an outsourcing proposal, before formally notifying the CBB and committing itself to an agreement.**

OM-3.4.2 **The risk assessment must – amongst other things – include an analysis of:**

(a) The business case;
(b) The suitability of the outsourcing provider; and
(c) The impact of the outsourcing on the licensee's overall risk profile and its systems and controls framework.

OM-3.4.3 In assessing the suitability of the outsourcing provider, the licensee should amongst other things consider its financial soundness, its technical competence, its commitment to the arrangement, and its reputation.

OM-3.4.4 **Once an outsourcing agreement has been entered into, licensees must regularly review the suitability of the outsourcing provider and the on-going impact of the agreement on their risk profile and systems and controls framework. Such reviews must take place at least every year.**

OM-3.4.5 **A licensee must nominate a member of senior management with day-to-day responsibility for handling the relationship with the outsourcing provider and ensuring that relevant risks are addressed. This person must be notified to the CBB as part of the notification required under Section OM-3.3 above.**

OM-3.5 Outsourcing Agreement

OM-3.5.1 The activities to be outsourced and respective contractual liabilities and obligations of the outsourcing provider and licensee must be clearly specified in an outsourcing agreement. This agreement must – amongst other things – address the following points:

(a) Control over outsourced activities

1. The Board and management of licensees are held ultimately responsible by the CBB for the adequacy of systems and controls in outsourced activities. Licensees must therefore ensure that they have adequate mechanisms for monitoring the performance of, and managing the relationship with, the outsourcing provider.
2. A service level agreement ("SLA") – setting out the standards of service to be provided – must form part of the outsourcing agreement. Where the outsourcing provider interacts directly with a licensee's customers, the SLA must – where relevant – reflect the licensee's own standards regarding customer care.
3. Mechanisms for the regular monitoring by licensees of performance against the SLA and other targets, and for implementing remedies in case of any shortfalls, must also form part of the agreement.
4. Clear reporting and escalation mechanisms must be specified in the agreement.
5. Where an outsourcing provider in turn decides to sub-contract to other providers, the original provider must remain contractually liable to the licensee for the quality and level of service agreed, and its obligations to the licensee must remain unchanged.

OM-3.5 Outsourcing Agreement (continued)

(b) Customer data confidentiality

1. Licensees must ensure that outsourcing agreements comply with all applicable legal requirements regarding customer confidentiality.
2. Licensees must ensure that the outsourcing provider implements adequate safeguards and procedures. Amongst other things, customer data must be properly segregated from those belonging to other clients the outsourcing provider may have. Outsourcing providers must give suitable undertakings that the company and its staff will comply with all applicable confidentiality rules. Licensees must have contractual rights to take action against the service provider in the event of a breach of confidentiality.
3. Licensees must assess the impact of using an overseas-based outsourcing provider on their ability to maintain customer data confidentiality, for instance, because of the powers of local authorities to access such data.

(c) Access to information

1. Outsourcing agreements must ensure that the licensee's internal and external auditors have timely access to any relevant information they may require to fulfill their responsibilities. Such access must allow them to conduct on-site examinations of the outsourcing provider, if required.
2. Licensees must also ensure that the CBB has timely access to any relevant information it may reasonably require under the law. Such access must allow the CBB to conduct on-site examinations of the outsourcing provider, if required.
3. Where the outsourcing provider is based overseas, the outsourcing provider must confirm in the outsourcing agreement that there are no regulatory or legal impediments to either the licensee's internal and external auditors, or the CBB, having the access described above. Should such restrictions subsequently be imposed, the licensee must communicate this fact to the CBB as soon as it becomes aware of the matter.

OM-3.5 Outsourcing Agreement (continued)

4. The outsourcing provider must commit itself, in the outsourcing agreement, to informing the licensee of any developments that may have a material impact on its ability to meet its obligations. These may include, for example, relevant control weaknesses identified by the outsourcing provider's internal or external auditors, and material adverse developments in the financial performance of the outsourcing provider.

(d) Business continuity

1. Licensees must ensure that service providers maintain, regularly review and test plans to ensure continuity in the provision of the outsourced service.
2. Licensees must have an adequate understanding of the outsourcing provider's arrangements, to understand the implications for its own contingency arrangements (see Section OM-3.6).

(e) Termination

1. Licensees must have the right to terminate the agreement should the outsourcing provider undergo a change of ownership (whether direct or indirect) that poses a potential conflict of interest; becomes insolvent; or goes into liquidation or administration.
2. Termination under any other circumstances allowed under the agreement must give licensees a sufficient notice period in which they can effect a smooth transfer of the service to another provider or bring it back in-house.
3. In the event of termination, for whatever reason, the agreement must provide for the return of all customer data – where required by licensees – or their destruction.

OM-3.6 Contingency Planning for Outsourcing Arrangements

OM-3.6.1 **Licensees must maintain and regularly review contingency plans to enable them to set up alternative arrangements – with minimum disruption to business – should the outsourcing contract be suddenly terminated or the outsourcing provider fails. This may involve the identification of alternative outsourcing providers or the provision of the service in-house. These plans must consider how long the transition would take and what interim arrangements would apply.**

OM-3.6.2 See Chapter OM-5 for further guidance on business continuity and contingency planning.

OM-3.7 Internal Audit Outsourcing

OM-3.7.1 Because of the critical importance of an effective internal audit function to a licensee's control framework, all proposals to outsource internal audit operations are to be considered material.

OM-3.7.2 The CBB will generally not permit licensees to outsource their internal audit function to the same firm that acts as their external auditors. However, the CBB may allow short-term outsourcing of internal audit operations to a licensee's external auditor, to meet unexpected urgent or short-term needs (for instance, on account of staff resignation or illness). Any such arrangement will be limited to a maximum of one year.

OM-3.7.3 Licensees who have existing outsourcing arrangements in place with their external auditors relating to the provision of internal audit services are required to find suitable alternatives when the existing arrangements terminate or come up for renewal.

OM-3.7.4 In all circumstances, Board and management of licensees must retain responsibility for ensuring that an adequate internal audit programme is implemented, and will be held accountable in this respect by the CBB.

OM-3.8 Intra-group Outsourcing

OM-3.8.1 **As with outsourcing to non-group companies, the Board and management of licensees are held ultimately responsible by the CBB for the adequacy of systems and controls in activities outsourced to group companies.**

OM-3.8.2 However, the degree of formality required – in terms of contractual agreements and control mechanisms – for outsourcing within a licensee's group is likely to be less, because of common management and enhanced knowledge of other group companies.

OM-3.8.3 **A licensee must formally notify the CBB at least 6 weeks before committing to a material intra-group outsourcing. The request must be made in writing to the licensee's normal supervisory contact, and must set out a summary of the proposed outsourcing, its rationale, and an analysis of its associated risks and proposed mitigating controls. The CBB will respond to the notification in the same manner and timescale as set in Section OM-3.3 above.**

OM-3.8.4 The CBB expects, as a minimum, an agreed statement of the standard of service to be provided by the group provider, including a clear statement of responsibilities allocated between the group provider and licensee.

OM-3.8.5 The CBB also expects a licensee's management to have addressed the issues of customer confidentiality, access to information and business continuity covered above (Section OM-3.5).

OM-4.1 Electronic Banking

OM-4.1.1 This Chapter refers to Basel Committee papers that the CBB requires relevant licensees to use as guidance on electronic banking activities.

OM-4.1.2 **The CBB considers that the following papers represent best practice and provide guidelines for recognising, addressing and managing risk associated with this area. Banks must take appropriate steps for the implementation of relevant recommendations set out therein:**

(a) 'Risk Management for Electronic Banking and Electronic Money Activities' issued in March 1998 (see OM-1.1 for further references to the paper);

(b) 'Risk Management Principles for Electronic Banking' issued in May 2001 (see OM-1.1 for further references to the paper).

OM-4.1.3 **Licensees must use the 'Risk Management Principles and Sound Practices' in the Basel Committee paper in OM-1.1 as guidelines to recognise and prudently manage risks associated with e-banking.**

OM-5.1 Introduction

Why do Financial Institutions Need Business Continuity Plans?

OM-5.1.1 All businesses may experience serious disruptions to their business operations. These disruptions may be caused by external events such as flooding, power failure or terrorism, or by internal factors such as human error or a serious computer breakdown. The probability of some events may be small, but the potential consequences may be massive, whereas other events may be more frequent and with shorter time horizons. The Joint Forum (the Basel Committee on Banking Supervision (BCBS), the International Organisation of Securities Commissions (IOSCO) and the International Association of Insurance Supervisors (IAIS)) have given additional background and context to the need for business continuity in its paper of August 2006 titled "High Level Principles for Business Continuity" (www.bis.org).

OM-5.1.2 According to the Joint Forum, in its paper, Business Continuity is "a whole of business approach for insuring that specified operations can be maintained or recovered in a timely fashion in the event of disruption. Its purpose is to minimize the operational, financial, legal, reputational, and other material consequences arising from a disruption". The objectives of a good business continuity plan ("BCP") are:

(a) To minimise financial loss to the licensee;

(b) To continue to serve customers and counterparties in the financial markets; and

(c) To mitigate the negative effects that disruptions can have on a licensee's reputation, operations, liquidity, credit quality, its market position, and its ability to remain in compliance with applicable laws and regulations.

OM-5.1.3 Banks play a critical role in an economy, in providing payment services, as holders of people's savings, and as providers of finance. Hence, a BCP is especially critical for banks. It helps ensure that their business operations are resilient and the effects of disruptions in service are minimized and thus helps maintain confidence in the banking system.

OM-5.1 Introduction (continued)

Scope and Key Elements of a BCP

OM-5.1.4 **The requirements of this Chapter apply to all retail and wholesale banks (whether locally incorporated or a branch).**

OM-5.1.5 Branch Licensees of foreign banks may apply alternative arrangements to those specified in this module, where they are subject to comprehensive BCP arrangements implemented by their head office or other member of their group, provided that:

(a) They have notified the CBB in writing what alternative arrangements will apply;

(b) They have satisfied the CBB that these alternative arrangements are equivalent to the measures contained in this chapter, or are otherwise suitable; and

(c) The CBB has agreed in writing to these alternative arrangements being used.

Implementation

OM-5.1.6 **The requirements in this Chapter must be complied with in full by 1 October 2007. Failure to comply with these requirements after that will trigger a supervisory response, which may include formal enforcement measures, as set out in Module EN (Enforcement).**

OM-5.1.7 For contingency planning relating to outsourcing activities, see Section OM-3.6.

OM-5.2 General Requirements

OM-5.2.1 **All conventional bank licensees must maintain a business continuity plan (BCP) appropriate to the scale and complexity of their operations. A BCP must address the following key areas:**

(a) Data back up and recovery (hard copy and electronic);
(b) Continuation of all critical systems, activities, and counterparty impact;
(c) Financial and operational assessments;
(d) Alternate communication arrangements between the licensee and its customers and its employees;
(e) Alternate physical location of employees;
(f) Communications with and reporting to the CBB and any other relevant regulators; and
(g) Ensuring customers' prompt access to their funds in the event of a disruption.

OM-5.2.2 **Effective BCPs must be comprehensive, limited not just to disruption of business premises and information technology facilities, but covering all other critical areas, which affect the continuity of critical business operations or services (e.g. liquidity, human resources and others).**

OM-5.2.3 **Licensees must notify the CBB promptly if their BCP is activated. They must also provide regular progress reports – as agreed with the CBB – until the BCP is deactivated.**

OM-5.2.4 The CBB recognises that BCPs involve costs, and that it may not be cost effective to have a fully developed and implemented BCP for all conceivable worst-case scenarios. However, the CBB expects licensees to plan for how they may cope with the complete destruction of buildings and surrounding infrastructure in which their key offices, installations, counterparties or service providers are located. The loss of key personnel, and a situation where back-up facilities might need to be used for an extended period of time are important factors in effective BCPs.

OM-5.2.5 Licensees may find it useful to consider two-tier plans: one to deal with near-term problems; this should be fully developed and able to be put into immediate effect. The other, which might be in paper form; should deal with a longer-term scenario (e.g. how to accommodate processes that might not be critical immediately but would become so over time).

OM-5.3 Board and Senior Management Responsibilities

Establishment of a Policy, Processes & Responsibilities

OM-5.3.1 A Bank's Board of Directors and Senior Management are collectively responsible for a bank's business continuity. The Board must endorse the policies, standards and processes for a licensee's BCP, as established by its senior management. The Board and senior management must delegate adequate resources to develop the BCP, and for its maintenance and periodic testing.

OM-5.3.2 Licensees must establish a Crisis Management Team (CMT) to develop, maintain and test their BCP, as well as to respond to and manage the various stages of a crisis. The CMT must comprise members of senior management and heads of major support functions (e.g. building facilities, IT, corporate communications and human resources).

OM-5.3.3 Licensees must establish (and document as part of the BCP) individuals' responsibilities in helping prepare for and manage a crisis; and the process by which a disaster is declared and the BCP initiated (and later terminated).

Monitoring and Reporting

OM-5.3.4 The CMT must submit regular reports to the Board and senior management on the results of the testing of the BCP (refer to section OM-5.9). Major changes must be developed by CMT, reported to senior management, and endorsed by the Board.

OM-5.3.5 The Chief Executive of a licensee must sign a formal annual statement submitted to the Board on whether the recovery strategies adopted are still valid and whether the documented BCP is properly tested and maintained. The annual statement must be included in the BCP documentation and will be reviewed as part of the CBB's on-site examinations.

OM-5.4 Developing a Business Continuity Plan

Impact Analysis

OM-5.4.1 **Licensees' BCPs must be based on (i) a business impact analysis (ii) an operational impact analysis, and (iii) a financial impact analysis. These analyses must be comprehensive, including all business functions and departments, not just IT or data processing.**

OM-5.4.2 The key objective of a Business Impact Analysis is to identify the different kinds of risk to business continuity and to quantify the operational and financial impact of disruptions on a licensee's ability to conduct its critical business processes.

OM-5.4.3 A typical business impact analysis is normally comprised of two stages. The first is to identify and prioritise the critical business processes that must be continued in the event of a disaster. The first stage should take account of the impact on customers and reputation, the legal implications and the financial cost associated with downtime. The second stage is a time-frame assessment. This aims to determine how quickly the licensee needs to resume critical business processes identified in stage one.

OM-5.4.4 Operational impact analysis focuses on the firm's ability to maintain communications with customers and to retrieve key activity records. It identifies the organizational implications associated with the loss of access, loss of utility, or loss of a facility. It highlights which functions may be interrupted by an outage, and the consequences to the public and customer of such interruptions.

OM-5.4.5 A Financial Impact Analysis identifies the financial losses that (both immediate and also consequent to the event) arise out of an operational disruption.

Risk Assessment

OM-5.4.6 **In developing a BCP, licensees must consider realistic threat scenarios that may (potentially) cause disruptions to their business processes.**

OM-5.4 Developing a Business Continuity Plan (continued)

OM-5.4.7 Licensees should analyse a threat by focusing on its impact on the business processes, rather than on the source of a threat. Certain scenarios can be viewed purely in terms of business disruption in specific work areas, systems or facilities. The scenarios should be sufficiently comprehensive to avoid the BCPs becoming too basic and thereby avoiding steps that could improve the resiliency of the licensee to disruptions.

OM-5.4.8 **In particular, the following specific scenarios must at a minimum, be considered in the BCP:**

- **Utilities are not available (power, telecommunications);**
- **Critical buildings are not available or specific facilities are not accessible;**
- **Software and live data are not available or are corrupted;**
- **Vendor assistance or (outsourced) service providers are not available;**
- **Critical documents or records are not available;**
- **Critical personnel are not available; and**
- **Significant equipment malfunctions (hardware or telecom).**

OM-5.4.9 **Licensees must distinguish between threats with a higher probability of occurrence and a lower impact to the business process (e.g. brief power interruptions) to those with a lower probability and higher impact (e.g. a terrorist bomb).**

OM-5.4.10 **As a starting point, licensees must perform a "gap analysis". This gap analysis is a methodical comparison of what types of plans the licensee requires in order to maintain, resume or recover critical business operations or services in the event of a disruption, versus what the existing BCP provides. Management and the Board can address the areas that need development in the BCP, using the gap analysis.**

OM-5.5 BCP – Recovery Levels & Objectives

OM-5.5.1 **The BCP must document strategies and procedures to maintain, resume and recover critical business operations or services. The plan must differentiate between critical and non-critical functions. The BCP must clearly describe the types of events that would lead up to the formal declaration of a business disruption and the process for activating the BCP.**

OM-5.5.2 **The BCP must clearly identify alternate sites for different operations, the total number of recovery personnel, workspace requirements, and applications and technology requirements. Office facilities and records requirements must also be identified.**

OM-5.5.3 Licensees should take note that they might need to cater for processing volumes that exceed those under normal circumstances. The interdependency among critical services is another major consideration in determining the recovery strategies and priority. For example, the resumption of the front office operations is highly dependent on the recovery of the middle office and back office support functions.

OM-5.5.4 **Individual critical business and support functions must establish the minimum BCP recovery objectives for recovering essential business operations and supporting systems to a specified level of service ("recovery level") within a defined period following a disruption ("recovery time"). These recovery levels and recovery times must be approved by the senior management prior to proceeding to the development of the BCP.**

List of Contacts and Responsibilities

OM-5.5.5 **The BCP must contain a list of all key personnel. The list must include personal contact information on each key employee such as their home address, home telephone number, and cell phone or pager number so they may be contacted in case of a disaster or other emergency.**

OM-5.5 BCP – Recovery Levels & Objectives (continued)

OM-5.5.6 **The BCP must contain all the necessary process steps to complete each critical business operation or service. Each process must be explained in sufficient detail to allow another employee to perform the job in case of a disaster.**

Alternate Sites for Business and Technology Recovery

OM-5.5.7 Most business continuity efforts are dependent on the availability of an alternate site (i.e. recovery site) for successful execution. The alternate site may be either an external site available through an agreement with a commercial vendor or a site within the Licensee's real estate portfolio. A useable, functional alternate site is an integral component of BCP.

OM-5.5.8 **Licensees must examine the extent to which key business functions are concentrated in the same or adjacent locations and the proximity of the alternate sites to primary sites. Alternate sites must be sufficiently remote from, and do not depend upon the same physical infrastructure components as a licensee's primary business location. This minimises the risk of both sites being affected by the same disaster (e.g. they must be on separate or alternative power grids and telecommunication circuits).**

OM-5.5.9 **Licensees' alternate sites must be readily accessible and available for occupancy (i.e. 24 hours a day, 7 days a week) within the time requirement specified in their BCP. Should the BCP so require, the alternate sites must have pre-installed workstations, power, telephones and ventilation, and sufficient space. Appropriate physical access controls such as access control systems and security guards must be implemented in accordance with Licensee's security policy.**

OM-5.5.10 Other than the establishment of alternate sites, licensees should also pay particular attention to the transportation logistics for relocation of operations to alternate sites. Consideration should be given to the impact a disaster may have on the transportation system (e.g. closures of roads). Some staff may have difficulty in commuting from their homes to the alternate sites. Other logistics, such as how to re-route internal and external mail to alternate sites should also be considered. Moreover, pre-arrangement with telecommunication companies for automated telephone call diversion from the primary work locations to the alternate sites should be considered.

OM-5.5 BCP – Recovery Levels & Objectives (continued)

OM-5.5.11 Alternate sites for technology recovery (i.e. back-up data centres), which may be separate from the primary business site, should have sufficient technical equipment (e.g. workstations, servers, printers, etc.) of appropriate model, size and capacity to meet recovery requirements as specified by licensees' BCPs. The sites should also have adequate telecommunication (including bandwidth) facilities and pre-installed network connections as specified by their BCP to handle the expected voice and data traffic volume.

OM-5.5.12 Licensees should avoid placing excessive reliance on external vendors in providing BCP support, particularly where a number of institutions are using the services of the same vendor (e.g. to provide back-up facilities or additional hardware). Licensees should satisfy themselves that such vendors do actually have the capacity to provide the services when needed and the contractual responsibilities of the vendors should be clearly specified. Licensees should recognise that outsourcing a business operation does not transfer the associated business continuity management responsibilities.

OM-5.5.13 The contractual terms should include the lead-time and capacity that vendors are committed to deliver in terms of back-up facilities, technical support or hardware. The vendor should be able to demonstrate its own recoverability including the specification of another recovery site in the event that the contracted site becomes unavailable.

OM-5.5.14 Certain licensees may rely on a reciprocal recovery arrangement with other institutions to provide recovery capability (e.g. Cheque sorting and cash handling). Licensees should, however, note that such arrangements are often not appropriate for prolonged disruptions or an extended period of time. This arrangement could also make it difficult for Licensees to adequately test their BCP. Any reciprocal recovery agreement should therefore be subject to proper risk assessment and documentation by licensees, and formal approval by the Board.

OM-5.6 Detailed Procedures for the BCP

OM-5.6.1 Once the recovery levels and recovery objectives for individual business lines and support functions are determined, the development of the detailed BCP should commence. The objective of the detailed BCP is to provide detailed guidance and procedures in a crisis situation, of how to recover critical business operations or services identified in the Business Impact Analysis stage, and to ultimately return to operations as usual.

Crisis Management Process

OM-5.6.2 **A BCP must set out a Crisis Management Plan (CMP) that serves as a documented guidance to assist the CMT in dealing with a crisis situation to avoid spill over effects to the business as a whole. The overall CMP, at a minimum, must contain the following:**

(a) A process for ensuring early detection of an emergency or a disaster situation and prompt notification to the CMT about the incident;

(b) A process for the CMT to assess the overall impact of the crisis situation on the licensee and to make quick decisions on the appropriate responses for action (i.e. staff safety, incident containment and specific crisis management procedures);

(c) Arrangements for safe evacuation from business locations (e.g. directing staff to a pre-arranged emergency assembly area, taking attendance of all employees and visitors at the time and tracking missing people through different means immediately after the disaster);

(d) Clear criteria for activation of the BCP and/or alternate sites;

(e) A process for gathering updated status information for the CMT (e.g. ensuring that regular conference calls are held among key staff from relevant business and support functions to report on the status of the recovery process);

(f) A process for timely internal and external communications; and

(g) A process for overseeing the recovery and restoration efforts of the affected facilities and the business services.

OM-5.6 Detailed Procedures for the BCP (continued)

OM-5.6.3 If CMT members need to be evacuated from their primary business locations, the licensee should set up a command centre to provide the necessary workspace and facilities for the CMT. Command centres should be sufficiently distanced from the licensee's primary business locations to avoid being affected by the same disaster.

Business Resumption

OM-5.6.4 **Each relevant business and support function must assign at least one member to be a part of the CMT to carry out the business resumption process for the relevant business and supported function. Appropriate recovery personnel with the required knowledge and skills must be assigned to the team.**

OM-5.6.5 Generally, the business resumption process consists of three major phases:

(a) The mobilisation phase – This phase aims to notify the recovery teams (e.g. via a call-out tree) and to secure the resources (e.g. recovery services provided by vendors) required to resume business services.

(b) The alternate processing phase – This phase emphasizes the resumption of the business and service delivery at the alternate site and/or in a different way than the normal process. This may entail record reconstruction and verification, establishment of new controls, alternate manual processes, and different ways of dealing with customers and counterparties; and

(c) The full recovery phase – This phase refers to the process for moving back to a permanent site after a disaster. This phase may be as difficult and critical to the business as the process to activate the BCP.

OM-5.6.6 For the first two phases above, clear responsibilities should be established and activities prioritised. A recovery tasks checklist should be developed and included in the BCP.

Technology Recovery

OM-5.6.7 Business resumption very often relies on the recovery of technology resources that include applications, hardware equipment and network infrastructure as well as electronic records. The technology requirements that are needed during recovery for individual business and support functions should be specified when the recovery strategies for the functions are determined.

OM-5.6 Detailed Procedures for the BCP (continued)

OM-5.6.8 Licensees should pay attention to the resilience of critical technology equipment and facilities such as the uninterruptible power supply (UPS) and the computer cooling systems. Such equipment and facilities should be subject to continuous monitoring and periodic maintenance and testing.

OM-5.6.9 **Appropriate personnel must be assigned with the responsibility for technology recovery. Alternative personnel need to be identified as back up for key technology recovery personnel in the case of the latter unavailability to perform the recovery process.**

Disaster Recovery Models

OM-5.6.10 There are various disaster recovery models that can be adopted by licensees to handle prolonged disruptions. The traditional model is an "active/back-up" model, which is widely used by many organizations. This traditional model is based on an "active" operating site with a corresponding alternate site (back-up site), both for data processing and for business operations.

OM-5.6.11 A split operations model, which is increasingly being used by major institutions, operates with two or more widely separated active sites for the same critical operations, providing inherent back up for each other (e.g. branches). Each site has the capacity to take up some or all of the work of another site for an extended period of time. This strategy can provide nearly immediate resumption capacity and is normally able to handle the issue of prolonged disruptions.

OM-5.6.12 The split operations model may incur higher operating costs, in terms of maintaining excess capacity at each site and added operating complexity. It may also be difficult to maintain appropriately trained staff and the split operations model can pose technological issues at multiple sites.

OM-5.6.13 The question of what disaster recovery model to adopt is for individual licensees' judgment based on the risk assessment of their business environment and the characteristics of their own operations.

OM-5.7 Vital Records Management

OM-5.7.1 Each BCP must clearly identify information deemed vital for the recovery of critical business and support functions in the event of a disaster as well as the relevant protection measures to be taken for protecting vital information. Licensees must refer to Chapter OM-7 when identifying vital information for business continuity. Vital information includes information stored on both electronic and non-electronic media.

OM-5.7.2 Copies of vital records must be stored off-site as soon as possible after creation. Back-up vital records must be readily accessible for emergency retrieval. Access to back-up vital records must be adequately controlled to ensure that they are reliable for business resumption purposes. For certain critical business operations or services, licensees must consider the need for instantaneous data back up to ensure prompt system and data recovery. There must be clear procedures indicating how and in what priority vital records are to be retrieved or recreated in the event that they are lost, damaged or destroyed.

OM-5.8 Other Policies Standards, and Processes

Employee Awareness and Training Plan

OM-5.8.1 **Licensees must implement an awareness plan and business continuity training for employees to ensure that all employees are continually aware of their responsibilities and know how to remain in contact and what to do in the event of a crisis.**

OM-5.8.2 Key employees should be involved in the business continuity development process, as well as periodic training exercises. Cross training should be utilised to anticipate restoring operations in the absence of key employees. Employee training should be regularly scheduled and updated to address changes to the BCP.

Public Relations & Communication Planning

OM-5.8.3 **Licensees must develop an awareness program and formulate a formal strategy for communication with key external parties (e.g. CBB and other regulators, investors, customers, counterparties, business partners, service providers, the media and other stakeholders) and provide for the type of information to be communicated. The strategy needs to set out all the parties the licensee must communicate to in the event of a disaster. This will ensure that consistent and up-to-date messages are conveyed to the relevant parties. During a disaster, ongoing and clear communication is likely to assist in maintaining the confidence of customers and counterparties as well as the public in general.**

OM-5.8.4 **The BCP must clearly indicate who may speak to the media and other key external parties, and have pre-arrangements for redirecting external communications to designated staff during a disaster. Important contact numbers and e-mail addresses of key external parties must be kept in a readily accessible manner (e.g. in wallet cards or licensees' intranet).**

OM-5.8.5 Licensees may find it helpful to prepare draft press releases as part of their BCP. This will save the CMT time in determining the main messages to convey in a chaotic situation. Important conversations with external parties should be properly logged for future reference.

OM-5.8 Other Policies, Standards and Processes (continued)

OM-5.8.6 As regards internal communication, the BCP should set out how the status of recovery can be promptly and consistently communicated to all staff, parent bank, head office, branches and subsidiaries (where appropriate). This may entail the use of various communication channels (e.g. broadcasting of messages to mobile phones of staff, Licensees websites, e-mails, intranet and instant messaging).

Insurance and other Risk Mitigating Measures

OM-5.8.7 **Licensees must have proper insurance coverage to reduce the financial losses that they may face during a disaster. Licensees must regularly review the adequacy and coverage of their insurance policies in reducing any foreseeable risks caused by disasters (e.g. loss of offices, critical IT facilities and equipment).**

Government and Community

OM-5.8.8 Licensees may need to coordinate with community and government officials and the media to ensure the successful implementation of the BCP. This establishes proper protocol in case a city- wide or region- wide event impacts the licensee's operations. During the recovery phase, facilities access, power, and telecommunications systems should be coordinated with various entities to ensure timely resumption of operations. Facilities access should be coordinated with the police and fire department and, depending on the nature and extent of the disaster.

Disclosure Requirements

OM-5.8.9 **Licensees must disclose how their BCP addresses the possibility of a future significant business disruption and how the licensee will respond to events of varying scope. Licensees must also state whether they plan to continue business during disruptions and the planned recovery time. The licensees might make these disclosures on their websites, or through mailing to key external parties upon request. In all cases, BCP disclosures must be reviewed and updated to address changes to the BCP.**

OM-5.9 Maintenance, Testing and Review

Testing & Rehearsal

OM-5.9.1 A BCP is not complete if it has not been subject to proper testing. Testing is needed to ensure that the BCP is operable. Testing verifies the awareness of staff and the preparedness of differing departments/functions of the bank.

OM-5.9.2 **Licensees must test their BCPs at least annually. Senior management must participate in the annual testing, and demonstrate their awareness of what they are required to do in the event of the BCP being involved. Also, the recovery and alternate personnel must participate in testing rehearsals to familiarise themselves with their responsibilities and the back-up facilities and remote sites (where applicable).**

OM-5.9.3 **All of the BCP's related risks and assumptions must be reviewed for relevancy and appropriateness as part of the annual planning of testing. The scope of testing must be comprehensive enough to cover the major components of the BCP as well as coordination and interfaces among important parties. A testing of particular components of the BCP or a fully integrated testing must be decided or depending on the situation. The following points must be included in the annual testing:**

(a) Staff evacuation and communication arrangements (e.g. call-out trees) must be validated;

(b) The alternate sites for business and technology recovery must be activated;

(c) Important recovery services provided by vendors or counterparties must form part of the testing scope;

(d) Licensees must consider testing the linkage of their back up IT systems with the primary and back up systems of service providers;

(e) If back up facilities are shared with other parties (e.g. subsidiaries of the licensee), the licensee needs to verify whether all parties can be accommodated concurrently; and

(f) Recovery of vital records must be performed as part of the testing.

OM-5.9 Maintenance, Testing and Review (continued)

OM-5.9.4 Formal testing reviews of the BCP must be performed to assess the thoroughness and effectiveness of the testing. Specifically, a post-mortem review report must be prepared at the completion of the testing stage for formal sign-off by Licensees' senior management. If the testing results indicate weaknesses or gaps in the BCP, the plan and recovery strategies must be updated to remedy the situation.

Periodic Maintenance and Updating of a BCP

OM-5.9.5 Licensees must have formal procedures to keep their BCP updated with respect to any changes to their business. In the event of a plan having been activated, a review process must be carried out once normal operations are restored to identify areas for improvement. If vendors are needed to provide vital recovery services, there must be formal processes for regular (say, annual) reviews of the appropriateness of the relevant service level agreements.

OM-5.9.6 Individual business and support functions, with the assistance of the CMT, must review their business impact analysis and recovery strategy on an annual basis. This aims to confirm the validity of, or whether updates are needed to, the BCP requirements (including the technical specifications of equipment of the alternate sites) for the changing business and operating environment.

OM-5.9.7 The contact information for key staff, counterparties, customers and service providers must be updated as soon as possible when notification of changes is received.

OM-5.9 Maintenance, Testing and Review (continued)

OM-5.9.8 Significant internal changes (e.g. merger or acquisitions, business re-organisation or departure of key personnel) must be reflected in the plan immediately and reported to senior management.

OM-5.9.9 Copies of the BCP document must be stored at locations separate from the primary site. A summary of key steps to be taken in an emergency situation must be made available to senior management and other key personnel.

Audit and Independent Review

OM-5.9.10 The internal audit function of a licensee or its external auditors must conduct periodic reviews of the BCP to determine whether the plan remains realistic and relevant, and whether it adheres to the policies and standards of the licensee. This review must include assessing the adequacy of business process identification, threat scenario development, business impact analysis and risk assessments, the written plan, testing scenarios and schedules, and communication of test results and recommendations to the Board.

OM-5.9.11 Significant findings must be brought to the attention of the Board and Senior Management within three months of the completion of the review. Furthermore, Senior Management and the Board must ensure that any gaps or shortcomings reported to them are addressed in an appropriate and timely manner.

OM-6.1 Physical Security Measures

External Measures

OM-6.1.1 The content of this Section is applicable to all retail banks licensed by the CBB in the Kingdom of Bahrain.

OM-6.1.2 All head offices are required to maintain Ministry of Interior ("MOI") guards on a 24 hours basis. All branches must maintain a 24 hour MOI guard. However, if branches satisfy the criteria mentioned in Paragraphs OM-6.1.3 to OM-6.1.22 below, they may maintain MOI guards during opening hours only. Furthermore, banks will be allowed to replace MOI armed guards with private security guards subject to the approval of the MOI. Training and approval of private security guards will be given by the MOI. Head Offices must always have a 24 hour MOI guard.

OM-6.1.3 Public entrances to head offices and branches must be protected by measures such as steel rolling shutters, or the external doors must be of solid steel or a similar solid material of equivalent strength and resistance to fire.

OM-6.1.4 Other external entrances must have steel doors or be protected by steel rolling shutters. Preferably, all other external entrances must have the following security measures:

(a) Magic eye;
(b) Locking device (key externally and handle internally);
(c) Door closing mechanism;
(d) Contact sensor with alarm for prolonged opening time; and
(e) Combination access control system (e.g. access card and key slot or swipe card and password).

OM-6.1 Physical Security Measures (continued)

OM-6.1.5 If additional security measures to those mentioned in OM-6.1.3 and OM-6.1.4 such as security cameras, motion detectors or intruder alarms are installed, the requirement for steel external doors or protection by steel rolling shutters is waived.

OM-6.1.6 External windows must have security measures such as anti blast films and movement detectors. For ground floor windows, banks may also wish to add steel grills fastened into the wall.

OM-6.1 Physical Security Measures (continued)

OM-6.1.7 Branch alarm systems must have the following features:

(a) PIR motion detectors;
(b) Door sensors;
(c) Anti vibration/movement sensors on vaults;
(d) External siren; and
(e) The intrusion detection system must be linked to the bank's (i.e. head office) monitoring unit and also the MOI Central Monitoring Unit.

Internal Measures

OM-6.1.8 Teller counters must be screened off from customers by a glass screen of no less than 1 meter in height from the counter work surface or 1.4 meters from the floor.

OM-6.1.9 All areas where cash is handled must be screened off from customers and other staff areas.

OM-6.1.10 Access to teller areas must be restricted to authorised staff only. The design of the teller area must not allow customers to pass through it.

OM-6.1.11 Panic alarm systems for teller staff must be installed. The choice between silent or audible panic alarms is left to individual banks. Kick bars and/or hold up buttons must be spread throughout the teller and customer service areas and the branch manager's office. The panic alarm must be linked to the MOI Central Monitoring Unit.

OM-6.1 Physical Security Measures (continued)

Cash Safety

OM-6.1.12 Cash precious metals and bearer instruments must be kept in fireproof cabinets/safes. Preferably, these cabinets/safes must be located in strong rooms.

OM-6.1.13 Strong rooms must be made of reinforced solid concrete, or reinforced block work. Doors to strong rooms must be steel and preferably also have a steel shutter fitted. Dual locking devices must be installed in strong room doors. Strong room doors must be located out of the sight of customers.

OM-6.1.14 Strong rooms must not contain any other openings except the entry door and where necessary, an air conditioning outlet. The air conditioning outlet must be protected with a steel grill.

OM-6.1.15 ATMs should not normally be replenished during customer opening hours. Replenishment of off-site ATMs must be performed by specialised service providers, comprising a crew of at least two persons. ATM replenishment staff must carry a mobile phone or communication device in case of emergency.

OM-6.1.16 All cash movements between branches, to and from the CBB and to off-site ATMs must be performed by specialised service providers.

OM-6.1.17 All ATMs must be properly maintained and covered by service or maintenance agreements. All ATMs must be inspected daily by bank staff to check that they are functioning properly and have not been tampered with.

OM-6.1.18 All banks must maintain a list of all maintenance, replenishment and inspection visits by staff or other authorised parties.

OM-6.1.19 All ATMs must be fitted with fraud detection and inhibiting devices (mandatory after year end 2006).

OM-6.1 Physical Security Measures (continued)

CCTV Network Systems

OM-6.1.20 All head offices and branches must have a CCTV network which is connected to a central monitoring unit located in the head office, and to the MOI Central Monitoring Unit.

OM-6.1.21 The location and type of CCTV cameras is left to the discretion of banks. At a minimum, CCTV cameras must cover the following areas:

(a) Main entrance;
(b) Other external doors;
(c) Any other access points (e.g. ground floor windows) ;
(d) The banking hall;
(e) Tellers' area;
(f) Strongroom entrance; and
(g) ATMs (by way of internal or external cameras)

OM-6.1.22 Notices of CCTV cameras in operation must be put up for the attention of the public. CCTV records must be maintained for a minimum 45-day period. The transmission rate (in terms of the number of frames per second) must be high enough to make for effective monitoring. Delayed transmission of pictures to the Central Monitoring Unit is not acceptable. The CCTV system must be operational 24 hours per day.

OM-6.1 Physical Security Measures (continued)

Training and Other Measures

OM-6.1.23 Banks must establish the formal position of security manager. This person will be responsible for ensuring all bank staff are given annual, comprehensive security training. Banks must produce a security manual or procedures for staff, especially those dealing directly with customers. For banks with three or more branches, this position must be a formally identified position. For banks with one or two branches, the responsibilities of this position may be added to the duties of a member of management.

OM-6.1.24 The security manager must maintain records on documented security related complaints by customers and take corrective action or make recommendations for action on a timely basis. Actions and recommendations must also be documented.

OM-6.1.25 Banks must consider safety and security issues when selecting premises for new branches. Key security issues include prominence of location (i.e. Is the branch on a main street or a back street?), accessibility for emergency services, and assessment of surrounding premises (in terms of their safety or vulnerability), and the number of entrances to the branch. All banks are required to hold an Insurance Blanket Bond (which includes theft of cash in its cover).

OM-6.2 Internet Security

OM-6.2.1 Retail banks providing internet banking services must regularly test their systems against security breaches and verify the robustness of the security controls in place. These tests must be conducted by security professionals, such as ethical hackers, that provide penetration testing services and a vulnerability assessment of the system.

OM-6.2.2 The penetration testing referred to in Paragraph OM-6.2.1, must be conducted at least once every six months.

OM-6.2.3 The vulnerability assessment report, along with the steps taken to mitigate the risks must be maintained by the bank for a 5-year period from the date of testing and must be provided to the CBB upon request.

MODULE	OM:	Operational Risk Management
CHAPTER	OM-7:	Books and Records

OM-7.1 General Requirements

OM-7.1.1 **The requirements in Section OM-7.1 apply to Bahraini conventional bank licensees, with respect to the business activities of the whole bank (whether booked in Bahrain or in a foreign branch). The requirements in Section OM-7.1 also apply to overseas conventional bank licensees, but only with respect to the business booked in their branch in Bahrain.**

OM-7.1.2 **With reference to Articles 59 and 60 of the CBB Law, all conventional bank licensees must maintain books and records (whether in electronic or hard copy form) sufficient to produce financial statements and show a complete record of the business undertaken by a licensee. These records must be retained for at least 10 years according to Article 60 of the CBB Law.**

OM-7.1.3 OM-7.1.2 includes accounts, books, files and other records (e.g. trial balance, general ledger, nostro/vostro statements, reconciliations and list of counterparties). It also includes records that substantiate the value of the assets, liabilities and off-balance sheet activities of the licensee (e.g. client activity files and valuation documentation).

OM -7.1.4 [This Paragraph was deleted in April 2011].

OM-7.1.5 **Unless otherwise agreed with the CBB in writing, records must be kept in either English or Arabic; or else accompanied by a certified English or Arabic translation. Records must be kept current. The records must be sufficient to allow an audit of the licensee's business or an on-site examination of the licensee by the CBB.**

OM -7.1.6 If a licensee wishes to retain certain records in a language other than English or Arabic without translation, the licensee should write to the CBB, explaining which types of records it wishes to keep in a foreign language, and why systematically translating these may be unreasonable. Generally, only loan contracts or similar original transaction documents may be kept without translation. Where exemptions are granted by CBB, the licensee is nonetheless asked to confirm that it will make available certified translations of such documents, if requested by CBB for an inspection or other supervisory purpose.

OM -7.1.7 Translations produced in compliance with Rule OM-7.1.5 may be undertaken in-house, by an employee or contractor of the licensee, provided they are certified by an appropriate officer of the licensee.

OM-7.1 General Requirements (continued)

OM-7.1.8 **Records must be accessible at any time from within the Kingdom of Bahrain, or as otherwise agreed with the CBB in writing.**

OM-7.1.9 Where older records have been archived, or in the case of records relating to overseas branches of Bahraini conventional banks, the CBB may accept that records be accessible within a reasonably short time frame (e.g. within 5 business days), instead of immediately. The CBB may also agree similar arrangements for overseas conventional banks, as well as Bahraini conventional banks, where elements of record retention and management have been centralised in another group company, whether inside or outside of Bahrain.

OM-7.1.10 All original account opening documentation, due diligence and transaction documentation should normally be kept in Bahrain, if the business is booked in Bahrain. However, where a licensee books a transaction in Bahrain, but the transaction documentation is handled entirely by another (overseas) branch or affiliate of the licensee, the relevant transaction documentation may be held in the foreign office, provided electronic or hard copies are retained in Bahrain; the foreign office is located in a FATF member state; and the foreign office undertakes to provide the original documents should they be required.

OM-7.1.11 Licensees should also note that to perform effective consolidated supervision of a group (or sub-group), the CBB needs to have access to financial information from foreign operations of a licensee, in order to gain a full picture of the financial condition of the group: see Module BR (CBB Reporting), regarding the submission of consolidated financial data. If a licensee is not able to provide to the CBB full financial information on the activities of its branches and subsidiaries, it should notify the CBB of the fact, to agree alternative arrangements: these may include requiring the group to restructure or limit its operations in the jurisdiction concerned.

OM-7.1.12 **In the case of Bahraini conventional banks with branch operations overseas, where local record-keeping keeping requirements are different, the higher of the local requirements or those contained in this Chapter must be followed.**

OM-7.2 Transaction Records

OM-7.2.1 **Conventional bank licensees must keep completed transaction records for as long as they are relevant for the purposes for which they were made (with a minimum period in all cases of five years from the date when the transaction was completed – see Module Section FC-7.1). Records of completed transactions must be kept in their original form (whether in hard copy and / or electronic format), for at least five years from the date of the transaction.**

OM-7.2.2 For example, if the original documents are paper, they must be kept in their original form. Electronic payments and receipts may be kept electronically without the need for hard copies. The record format selected must be capable of producing complete and accurate financial, management and regulatory reports, and allow monitoring and review of all transactions.

OM-7.2.3 **Rule OM-7.2.1 applies to all transactions entered into by a Bahraini conventional bank licensee, whether booked in Bahrain or in an overseas branch. With respect to overseas conventional bank licensees, it applies only to transactions booked in the Bahrain branch.**

OM-7.2.4 In the case of overseas conventional bank licensees, Rule OM-7.2.1 therefore only applies to business booked in the Bahrain branch, not in the rest of the company.

OM-7.3 Other Records

Corporate Records

OM-7.3.1 **Conventional bank licensees must maintain the following records in original form or in hard copy at their premises in Bahrain:**

(a) Internal policies, procedures and operating manuals;

(b) Corporate records, including minutes of shareholders', Directors' and management meetings;

(c) Correspondence with the CBB and records relevant to monitoring compliance with CBB requirements;

(d) Reports prepared by the conventional bank licensee's internal and external auditors; and

(e) Employee training manuals and records.

OM-7.3.2 In the case of Bahrain conventional bank licensees, these requirements apply to the licensee as a whole, including any overseas branches. In the case of overseas conventional bank licensees, all the requirements of Chapter OM-7 are limited to the business booked in their branch in Bahrain and the records of that branch (see Rule OM-7.1.1). They are thus not required to hold copies of shareholders' and Directors' meetings, except where relevant to the branch's operations.

Customer Records

OM-7.3.3 Record-keeping requirements with respect to customer records, including customer identification and due diligence records, are contained in Module FC (Financial Crime). These requirements address specific requirements under the Amiri Decree Law No. 4 of 2001, the standards promulgated by the Financial Action Task Force, as well as to the best practice requirements of the Basel Committee Core Principles methodology, and its paper on "Customer due diligence for banks".

Promotional Schemes

OM-7.3.4 **Conventional bank licensees must maintain all materials related to promotional schemes as outlined in Section BC-1.1 for a minimum period of 5 years.**

OM-8.1 Introduction

OM-8.1.1 Section CA-7.1 of the Capital Adequacy Module allows banks to use either the basic indicator approach or standardised approach to compute capital charge for operational risk. This chapter sets out the qualitative aspect of these two approaches.

OM-8.1.2 Operational risk is defined as the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. This definition includes legal risk[1], but excludes strategic and reputational risk.

1 Legal risk includes, but is not limited to, exposure to fines, penalties, or punitive damages resulting from supervisory actions, as well as private settlements.

OM-8.2 Basic Indicator Approach

OM-8.2.1 Banks applying the basic indicator approach for capital adequacy purposes as detailed in section CA-7.1 of Capital Adequacy Module are encouraged to comply with the principles set forth in this section.

Developing an Appropriate Risk Management Environment

OM-8.2.2 Failure to understand and manage operational risk, which is present in virtually all bank transactions and activities, may greatly increase the likelihood that some risks will go unrecognised and uncontrolled. Both the board and senior management are responsible for creating an organisational culture that places high priority on effective operational risk management and adherence to sound operating controls. Operational risk management is most effective where a bank's culture emphasises high standards of ethical behaviour at all levels of the bank. The board and senior management should promote an organisational culture which establishes through both actions and words the expectations of integrity for all employees in conducting the business of the bank.

OM-8.2.3 Principle 1: The board of directors must be aware of the major aspects of the bank's operational risks as a distinct risk category that must be managed, and it must approve and periodically review the bank's operational risk management framework. The framework must provide a bank-wide definition of operational risk and lay down the principles of how operational risk is to be identified, assessed, monitored, and controlled/mitigated.

OM-8.2.4 The board of directors should approve the implementation of a bank-wide framework to explicitly manage operational risk as a distinct risk to the bank's safety and soundness. The board should provide senior management with clear guidance and direction regarding the principles underlying the framework and approve the corresponding policies developed by senior management.

OM-8.2.5 An operational risk framework should be based on an appropriate definition of operational risk which clearly articulates what constitutes operational risk in that bank. The framework should cover the bank's appetite and tolerance for operational risk, as specified through the policies for managing this risk and the bank's prioritisation of operational risk management activities, including the extent of, and manner in which, operational risk is transferred outside the bank. It should also include policies outlining the bank's approach to identifying, assessing, monitoring and controlling/mitigating the risk. The degree of formality and sophistication of the bank's operational risk management framework should be commensurate with the bank's risk profile.

OM-8.2 Basic Indicator Approach (continued)

OM-8.2.6 The board is responsible for establishing a management structure capable of implementing the bank's operational risk management framework. Since a significant aspect of managing operational risk relates to the establishment of strong internal controls, it is particularly important that the board establishes clear lines of management responsibility, accountability and reporting. In addition, there should be separation of responsibilities and reporting lines between operational risk control functions, business lines and support functions in order to avoid conflicts of interest. The framework should also articulate the key processes the bank needs to have in place to manage operational risk.

OM-8.2.7 The board should review the framework regularly to ensure that the bank is managing the operational risks arising from external market changes and other environmental factors, as well as those operational risks associated with new products, activities or systems. This review process should also aim to assess industry best practice in operational risk management appropriate for the bank's activities, systems and processes. If necessary, the board should ensure that the operational risk management framework is revised in light of this analysis, so that material operational risks are captured within the framework.

OM-8.2.8 **Principle 2: The board of directors must ensure that the bank's operational risk management framework is subject to effective and comprehensive internal audit by operationally independent, appropriately trained and competent staff. The internal audit function must not be directly responsible for operational risk management.**

OM-8.2.9 Banks should have in place adequate internal audit coverage to verify that operating policies and procedures have been implemented effectively. The board (either directly or indirectly through its audit committee) should ensure that the scope and frequency of the audit programme is appropriate to the risk exposures. Audit should periodically validate that the bank's operational risk management framework is being implemented effectively across the bank.

OM-8.2.10 To the extent that the audit function is involved in oversight of the operational risk management framework, the board should ensure that the independence of the audit function is maintained. This independence may be compromised if the audit function is directly involved in the operational risk management process. The audit function may provide valuable input to those responsible for operational risk management, but should not itself have direct operational risk management responsibilities. In practice, the CBB recognises that the audit function at some banks (particularly smaller banks) may have initial responsibility for developing an operational risk management programme. Where this is the case, banks should see that responsibility for day-to-day operational risk management is transferred elsewhere in a timely manner.

OM-8.2 Basic Indicator Approach (continued)

OM-8.2.11 **Principle 3: Senior management must have responsibility for implementing the operational risk management framework approved by the board of directors. The framework must be consistently implemented throughout the whole banking organisation, and all levels of staff must understand their responsibilities with respect to operational risk management. Senior management must also have responsibility for developing policies, processes and procedures for managing operational risk in all of the bank's material products, activities, processes and systems.**

OM-8.2.12 Management should translate the operational risk management framework established by the board of directors into specific policies, processes and procedures that can be implemented and verified within the different business units. While each level of management is responsible for the appropriateness and effectiveness of policies, processes, procedures and controls within its purview, senior management should clearly assign authority, responsibility and reporting relationships to encourage and maintain this accountability, and ensure that the necessary resources are available to manage operational risk effectively. Moreover, senior management should assess the appropriateness of the management oversight process in light of the risks inherent in a business unit's policy.

OM-8.2.13 Senior management should ensure that bank activities are conducted by qualified staff with the necessary experience, technical capabilities and access to resources, and that staff responsible for monitoring and enforcing compliance with the institution's risk policy have authority independent from the units they oversee. Management should ensure that the bank's operational risk management policy has been clearly communicated to staff at all levels in units that incur material operational risks.

OM-8.2.14 Senior management should ensure that staff responsible for managing operational risk communicate effectively with staff responsible for managing credit, market, and other risks, as well as with those in the bank who are responsible for the procurement of external services such as insurance purchasing and outsourcing agreements. Failure to do so could result in significant gaps or overlaps in a bank's overall risk management programme.

OM-8.2.15 Senior management should also ensure that the bank's remuneration policies are consistent with its appetite for risk. Remuneration policies which reward staff that deviate from policies (e.g. by exceeding established limits) weaken the bank's risk management processes.

OM-8.2.16 Particular attention should be given to the quality of documentation controls and to transaction-handling practices. Policies, processes and procedures related to advanced technologies supporting high transactions volumes, in particular, should be well documented and disseminated to all relevant personnel.

OM-8.2 Basic Indicator Approach (continued)

Risk Management: Identification, Assessment, Monitoring and Mitigation/Control

OM-8.2.17 **Principle 4: Banks must identify and assess the operational risk inherent in all material products, activities, processes and systems. Banks must also ensure that before new products, activities, processes and systems are introduced or undertaken, the operational risk inherent in them is subject to adequate assessment procedures.**

OM-8.2.18 Risk identification is paramount for the subsequent development of a viable operational risk monitoring and control system. Effective risk identification considers both internal factors (such as the bank's structure, the nature of the bank's activities, the quality of the bank's human resources, organisational changes and employee turnover) and external factors (such as changes in the industry and technological advances) that could adversely affect the achievement of the bank's objectives.

OM-8.2.19 In addition to identifying the most potentially adverse risks, banks should assess their vulnerability to these risks. Effective risk assessment allows the bank to better understand its risk profile and most effectively target risk management resources.

OM-8.2.20 Amongst the possible tools used by banks for identifying and assessing operational risk are:

(a) Self- or Risk Assessment: a bank assesses its operations and activities against a menu of potential operational risk vulnerabilities. This process is internally driven and often incorporates checklists and/or workshops to identify the strengths and weaknesses of the operational risk environment. Scorecards, for example, provide a means of translating qualitative assessments into quantitative metrics that give a relative ranking of different types of operational risk exposures. Some scores may relate to risks unique to a specific business line while others may rank risks that cut across business lines. Scores may address inherent risks, as well as the controls to mitigate them. In addition, scorecards may be used by banks to allocate economic capital to business lines in relation to performance in managing and controlling various aspects of operational risk.

(b) Risk Mapping: in this process, various business units, organisational functions or process flows are mapped by risk type. This exercise can reveal areas of weakness and help prioritise subsequent management action.

(c) Risk Indicators: risk indicators are statistics and/or metrics, often financial, which can provide insight into a bank's risk position. These indicators tend to be reviewed on a periodic basis (such as monthly or quarterly) to alert banks to changes that may be indicative of risk concerns. Such indicators may include the number of failed trades, staff turnover rates and the frequency and/or severity of errors and omissions.

OM-8.2 Basic Indicator Approach (continued)

(d) Measurement: some banks have begun to quantify their exposure to operational risk using a variety of approaches. For example, data on a bank's historical loss experience could provide meaningful information for assessing the bank's exposure to operational risk and developing a policy to mitigate/control the risk. An effective way of making good use of this information is to establish a framework for systematically tracking and recording the frequency, severity and other relevant information on individual loss events. Some banks have also combined internal loss data with external loss data, scenario analyses, and risk assessment factors.

OM-8.2.21 **Principle 5: Banks must implement a process to regularly monitor operational risk profiles and material exposures to losses. There must be regular reporting of pertinent information to senior management and the board of directors that supports the proactive management of operational risk.**

OM-8.2.22 An effective monitoring process is essential for adequately managing operational risk. Regular monitoring activities can offer the advantage of quickly detecting and correcting deficiencies in the policies, processes and procedures for managing operational risk. Promptly detecting and addressing these deficiencies can substantially reduce the potential frequency and/or severity of a loss event.

OM-8.2.23 In addition to monitoring operational loss events, banks should identify appropriate indicators that provide early warning of an increased risk of future losses. Such indicators (often referred to as key risk indicators or early warning indicators) should be forward-looking and could reflect potential sources of operational risk such as rapid growth, the introduction of new products, employee turnover, transaction breaks, system downtime, and so on. When thresholds are directly linked to these indicators an effective monitoring process can help identify key material risks in a transparent manner and enable the bank to act upon these risks appropriately.

OM-8.2.24 The frequency of monitoring should reflect the risks involved and the frequency and nature of changes in the operating environment. Monitoring should be an integrated part of a bank's activities. The results of these monitoring activities should be included in regular management and board reports, as should compliance reviews performed by the internal audit and/or risk management functions. Reports generated by (and/or for) supervisory authorities may also inform this monitoring and should likewise be reported internally to senior management and the board, where appropriate.

OM-8.2 Basic Indicator Approach (continued)

OM-8.2.25 Senior management should receive regular reports from appropriate areas such as business units, group functions, the operational risk management office and internal audit. The operational risk reports should contain internal financial, operational, and compliance data, as well as external market information about events and conditions that are relevant to decision making. Reports should be distributed to appropriate levels of management and to areas of the bank on which areas of concern may have an impact. Reports should fully reflect any identified problem areas and should motivate timely corrective action on outstanding issues. To ensure the usefulness and reliability of these risk and audit reports, management should regularly verify the timeliness, accuracy, and relevance of reporting systems and internal controls in general. Management may also use reports prepared by external sources (auditors, supervisors) to assess the usefulness and reliability of internal reports. Reports should be analysed with a view to improving existing risk management performance as well as developing new risk management policies, procedures and practices.

OM-8.2.26 In general, the board of directors should receive sufficient higher-level information to enable them to understand the bank's overall operational risk profile and focus on the material and strategic implications for the business.

OM-8.2.27 **Principle 6: Banks must have policies, processes and procedures to control and/or mitigate material operational risks. Banks must periodically review their risk limitation and control strategies and must adjust their operational risk profile accordingly using appropriate strategies, in light of their overall risk appetite and profile.**

OM-8.2.28 Control activities are designed to address the operational risks that a bank has identified. For all material operational risks that have been identified, the bank should decide whether to use appropriate procedures to control and/or mitigate the risks, or bear the risks. For those risks that cannot be controlled, the bank should decide whether to accept these risks, reduce the level of business activity involved, or withdraw from this activity completely. Control processes and procedures should be established and banks should have a system in place for ensuring compliance with a documented set of internal policies concerning the risk management system. Principle elements of this could include, for example:

(a) Top-level reviews of the bank's progress towards the stated objectives;
(b) Checking for compliance with management controls;
(c) Policies, processes and procedures concerning the review, treatment and resolution of non-compliance issues; and
(d) A system of documented approvals and authorisations to ensure accountability to an appropriate level of management.

OM-8.2 Basic Indicator Approach (continued)

OM-8.2.29 Although a framework of formal, written policies and procedures is critical, it needs to be reinforced through a strong control culture that promotes sound risk management practices. Both the board of directors and senior management are responsible for establishing a strong internal control culture in which control activities are an integral part of the regular activities of a bank. Controls that are an integral part of the regular activities enable quick responses to changing conditions and avoid unnecessary costs.

OM-8.2.30 An effective internal control system also requires that there be appropriate segregation of duties and that personnel are not assigned responsibilities which may create a conflict of interest. Assigning such conflicting duties to individuals, or a team, may enable them to conceal losses, errors or inappropriate actions. Therefore, areas of potential conflicts of interest should be identified, minimised, and subject to careful independent monitoring and review.

OM-8.2.31 In addition to segregation of duties, banks should ensure that other internal practices are in place as appropriate to control operational risk. Examples of these include:

(a) Close monitoring of adherence to assigned risk limits or thresholds;
(b) Maintaining safeguards for access to, and use of, bank assets and records;
(c) Ensuring that staff have appropriate expertise and training;
(d) Identifying business lines or products where returns appear to be out of line with reasonable expectations (e.g., where a supposedly low risk, low margin trading activity generates high returns that could call into question whether such returns have been achieved as a result of an internal control breach); and
(e) Regular verification and reconciliation of transactions and accounts.

Failure to implement such practices has resulted in significant operational losses for some banks in recent years.

OM-8.2.32 Operational risk can be more pronounced where banks engage in new activities or develop new products (particularly where these activities or products are not consistent with the bank's core business strategies), enter unfamiliar markets, and/or engage in businesses that are geographically distant from the head office. Moreover, in many such instances, banks do not ensure that the risk management control infrastructure keeps pace with the growth in the business activity. A number of the most sizeable and highest-profile losses in recent years have taken place where one or more of these conditions existed. Therefore, it is incumbent upon banks to ensure that special attention is paid to internal control activities where such conditions exist.

OM-8.2 Basic Indicator Approach (continued)

OM-8.2.33 Some significant operational risks have low probabilities but potentially very large financial impact. Moreover, not all risk events can be controlled (e.g., natural disasters). Risk mitigation tools or programmes can be used to reduce the exposure to, or frequency and/or severity of, such events. For example, insurance policies, particularly those with prompt and certain pay-out features, can be used to externalise the risk of "low frequency, high severity" losses which may occur as a result of events such as third-party claims resulting from errors and omissions, physical loss of securities, employee or third-party fraud, and natural disasters.

OM-8.2.34 However, banks should view risk mitigation tools as complementary to, rather than a replacement for, thorough internal operational risk control. Having mechanisms in place to quickly recognise and rectify legitimate operational risk errors can greatly reduce exposures. Careful consideration also needs to be given to the extent to which risk mitigation tools such as insurance truly reduce risk, or transfer the risk to another business sector or area, or even create a new risk (e.g. legal or counterparty risk).

OM-8.2.35 Investments in appropriate processing technology and information technology security are also important for risk mitigation. However, banks should be aware that increased automation could transform high-frequency, low-severity losses into low frequency, high-severity losses. The latter may be associated with loss or extended disruption of services caused by internal factors or by factors beyond the bank's immediate control (e.g., external events). Such problems may cause serious difficulties for banks and could jeopardise an institution's ability to conduct key business activities. As discussed below in Principle 7, banks should establish disaster recovery and business continuity plans that address this risk.

OM-8.2.36 Banks should also establish policies for managing the risks associated with outsourcing activities. Outsourcing of activities can reduce the institution's risk profile by transferring activities to others with greater expertise and scale to manage the risks associated with specialised business activities. However, a bank's use of third parties does not diminish the responsibility of the board of directors and management to ensure that the third-party activity is conducted in a safe and sound manner and in compliance with applicable laws. Outsourcing arrangements should be based on robust contracts and/or service level agreements that ensure a clear allocation of responsibilities between external service providers and the outsourcing bank. Furthermore, banks need to manage residual risks associated with outsourcing arrangements, including disruption of services.

OM-8.2 Basic Indicator Approach (continued)

OM-8.2.37 Depending on the scale and nature of the activity, banks should understand the potential impact on their operations and their customers of any potential deficiencies in services provided by vendors and other third-party or intra-group service providers, including both operational breakdowns and the potential business failure or default of the external parties. The board and management should ensure that the expectations and obligations of each party are clearly defined, understood and enforceable. The extent of the external party's liability and financial ability to compensate the bank for errors, negligence, and other operational failures should be explicitly considered as part of the risk assessment. Banks should carry out an initial due diligence test and monitor the activities of third party providers, especially those lacking experience of the banking industry's regulated environment, and review this process (including re-evaluations of due diligence) on a regular basis. For critical activities, the bank may need to consider contingency plans, including the availability of alternative external parties and the costs and resources required to switch external parties, potentially on very short notice.

OM-8.2.38 In some instances, banks may decide to either retain a certain level of operational risk or self-insure against that risk. Where this is the case and the risk is material, the decision to retain or self-insure the risk should be transparent within the organisation and should be consistent with the bank's overall business strategy and appetite for risk.

OM-8.2.39 **Principle 7: Banks must have in place contingency and business continuity plans to ensure their ability to operate on an ongoing basis and limit losses in the event of severe business disruption.**

OM-8.2.40 For reasons that may be beyond a bank's control, a severe event may result in the inability of the bank to fulfil some or all of its business obligations, particularly where the bank's physical, telecommunication, or information technology infrastructures have been damaged or made inaccessible. This can, in turn, result in significant financial losses to the bank, as well as broader disruptions to the financial system through channels such as the payments system. This potential requires that banks establish disaster recovery and business continuity plans that take into account different types of plausible scenarios to which the bank may be vulnerable, commensurate with the size and complexity of the bank's operations.

OM-8.2.41 Banks should identify critical business processes, including those where there is dependence on external vendors or other third parties, for which rapid resumption of service would be most essential. For these processes, banks should identify alternative mechanisms for resuming service in the event of an outage. Particular attention should be paid to the ability to restore electronic or physical records that are necessary for business resumption. Where such records are backed-up at an off-site facility, or where a bank's operations must be relocated to a new site, care should be taken that these sites are at an adequate distance from the impacted operations to minimise the risk that both primary and back-up records and facilities will be unavailable simultaneously.

OM-8.2 Basic Indicator Approach (continued)

OM-8.2.42 Banks should periodically review their disaster recovery and business continuity plans so that they are consistent with the bank's current operations and business strategies. Moreover, these plans should be tested periodically to ensure that the bank would be able to execute the plans in the unlikely event of a severe business disruption.

OM-8.3 Standardised Approach

OM-8.3.1 **Banks applying standardised approach for capital adequacy purposes as detailed in section CA-7.1 of Capital Adequacy Module, must comply with the requirements principles set in this section. In order to qualify for use of the Standardised Approach, a bank must satisfy the CBB that, at a minimum:**

- **Its board of directors and senior management, as appropriate, are actively involved in the oversight of the operational risk management framework;**
- **It has an operational risk management system that is conceptually sound and is implemented with integrity; and**
- **It has sufficient resources in the use of the approach in the major business lines as well as the control and audit areas.**

OM-8.3.2 The CBB will have the right to insist on a period of initial monitoring of a bank's Standardised Approach before it is used for regulatory capital purposes.

OM-8.3.3 **A bank must develop specific policies and have documented criteria for mapping gross income for current business lines and activities into the standardised framework. The criteria must be reviewed and adjusted for new or changing business activities as appropriate. Further guidance on business line mapping is set out in paragraph CA-7.1.8 of the Capital Adequacy Module.**

OM-8.3.4 **A bank using the standardised approach must meet the following additional criteria:**

(a) The bank must have an operational risk management system with clear responsibilities assigned to an operational risk management function. The operational risk management function is responsible for developing strategies to identify, assess, monitor and control/mitigate operational risk; for codifying bank-level policies and procedures concerning operational risk management and controls; for the design and implementation of the bank's operational risk assessment methodology; and for the design and implementation of a risk-reporting system for operational risk.

OM-8.3 Standardised Approach (continued)

(b) As part of the bank's internal operational risk assessment system, the bank must systematically track relevant operational risk data including material losses by business line. Its operational risk assessment system must be closely integrated into the risk management processes of the bank. Its output must be an integral part of the process of monitoring and controlling the banks operational risk profile. For instance, this information must play a prominent role in risk reporting, management reporting, and risk analysis. The bank must have techniques for creating incentives to improve the management of operational risk throughout the bank.

(c) There must be regular reporting of operational risk exposures, including material operational losses, to business unit management, senior management, and to the board of directors. The bank must have procedures for taking appropriate action according to the information within the management reports.

(d) The bank's operational risk management system must be well documented. The bank must have a routine in place for ensuring compliance with a documented set of internal policies, controls and procedures concerning the operational risk management system, which must include policies for the treatment of noncompliance issues.

(e) The bank's operational risk management processes and assessment system must be subject to validation and regular independent review. These reviews must include both the activities of the business units and of the operational risk management function.

(f) The bank's operational risk assessment system (including the internal validation processes) must be subject to regular review by external auditors and /or the CBB.