THE BERMUDA MONETARY AUTHORITY

BANKS AND DEPOSIT COMPANIES ACT 1999:

The Management of Operational Risk

May 2007

Introduction

1 This paper sets out the policy of the Bermuda Monetary Authority ('the Authority') on the management of operational risk by banks and deposit companies. It has been the subject of detailed consultation with the industry based on a consultation paper published in December 2006.

2 The effectiveness of institutions' operational risk management processes is a key element in determining their soundness. Losses arising from an institution's operational risks may on occasion exceed those stemming from credit losses. It is, therefore, a vital focus for management in ensuring a properly controlled approach to the risks inherent in their business. It is also an important part of the Authority's assessment of institutions' ongoing compliance with the minimum licensing criteria requirements for business to be conducted in a prudent manner, as set out in the Second Schedule to the Banks & Deposit Companies Act ('the Act'). Judgments as to the effectiveness of the arrangements that institutions have in place for this aspect of the prudent conduct of their business also have direct importance for the Authority's determination of the adequacy of their capital under the Basel 2 framework.

3 The Authority seeks to satisfy itself that institutions maintain risk management policies and procedures that are appropriate for their individual business profile, and that they adopt and apply suitable arrangements for identifying, assessing, monitoring and controlling/ mitigating their operational risks. In response to the heightened focus on such risks involving their specific assessment as part of the Basel framework for assessing soundness and capital adequacy, Bermuda's licensed institutions – like those in other jurisdictions internationally – need to keep their operational risk frameworks under regular review with a view to enhancing the effectiveness with which such risks are managed and controlled.

Definition of Operational Risk

4 Operational Risk is defined as the risk of loss resulting from inadequate or failed internal processes, people and systems, or from external events. It must be noted that this definition includes legal risk but excludes strategic and reputation risk. Legal risk includes expenses (e.g. the establishment of a legal reserve) to fund litigation, adverse judgments or settlements – as well as fees and expenses for external legal advice for work related to specific incidents or cases. Such legal risks must, therefore, be included within institutions' monitoring and reporting frameworks for operational risk. However, operational risk would not include the cost of general legal advice on an institution's overall corporate strategy.

Categories of Operational Risk

5 The table in Appendix A summarizes the current international consensus as to the seven major (or "Level 1") categories of operational risk as well as a breakdown of each Level 1 category into a number of sub-categories.

Framework for Operational Risk

6 Institutions must put in place suitable risk management policies and procedures to enable them to identify, assess, monitor and control/ mitigate operational risk. These policies and procedures should be commensurate with the scale and complexity of an institution's operations. In particular, an institution's policies and procedures should cover the following critical elements:

i. Operational Risk Framework
ii. Role of Board and senior management in overseeing the Operational Risk framework
iii. Responsibility for implementation of the framework
iv. Independent control review
v. Collection of operational risk loss event data
vi. Monitoring and reporting

An institution must also ensure that its operational risk framework and arrangements are kept under regular review and amended as necessary, having regard to changes in its risk profile as well as external market developments. Changes in an institution's strategy and general policy for operational risk management must be reviewed and approved by the Board of directors.

Operational Risk Framework

7 Each institution must develop and put in place an operational risk framework, comprising a policy statement and related procedures, that is appropriate and effective, having regard to the scale and nature of its business. For a small, specialized local deposit-taking business which qualifies for use of the Basic Indicator approach in determining the capital charge for operational risk, documentation of the framework may remain relatively high level in character. Even there, however, certain basic matters need to be documented, notably the key elements of operational risk policy including: the definition of operational risk; the primary elements of operational risk identified within the operations of the institution; the role of the board and senior management in overseeing the framework for these risks; the role of the person who has primary responsibility for the day to day management of the framework; the role of internal audit/compliance in respect of such risks; and the collation of basic operational risk loss event data for circulation to Board and senior management.

8 For more complex institutions, a more detailed and extensive framework needs to be in place and documented. This will include, in addition to the above: details of the institution's approach in identifying, assessing, monitoring and controlling/mitigating operational risk throughout the institution's business processes; the 'ownership' and accountabilities for operational risk within the institution's management and control framework (and how they are integrated into the institution's overall risk management processes): details of the quarterly operational risk reporting framework that has been established for the collection and circulation to Board and senior management of key loss event data; details of the approach to policy breaches and non-compliance issues; contingency/ business continuity issues; the approach to the use of insurance in mitigating the risks; and the use of incentives to encourage the improved management of operational risk throughout the organization.

Board and Senior Management Oversight

9 The Board of directors of each institution must be actively involved in setting the strategy and framework for the management of operational risk and must provide effective oversight of the framework to ensure that it is operating satisfactorily. They need to be aware of the major aspects of the institution's operational risks as a distinct risk category that should be managed; to approve and periodically review the institution's operational risk policy; and to ensure that the operational risk framework is subject to effective and comprehensive internal audit by operationally independent, appropriately trained and competent staff. Senior management of each institution must: approve and periodically review the institution's operational risk framework; have responsibility for implementing the operational risk framework consistently throughout the organization; and see that all levels of staff understand their responsibilities with respect to operational risk through training and/ or awareness programs. Overall, the Authority expects both the Board and senior management to ensure that the operational risk framework has sufficient resources – both in the major business lines and in the audit function – to function effectively.

Responsibility for Implementation

10 It is critical for institutions to ensure that there is full clarity among relevant staff as to the processes and procedures for operational risk and the identity of the person or persons who have day-to-day responsibility for the implementation of the framework. Generally, there should be one person designated as Head of Operational Risk (or an equivalent title). This person should be responsible for a clear set of assigned duties including: developing strategies to identity, assess, monitor and control/ mitigate operational risk; codifying overall policies and approving product or business-level procedures; designing and implementing the

institution's operational risk assessment methodology; and designing and implementing the operational risk reporting system.

Independent Control Review

11 An institution's operational risk framework needs to be subject to periodic validation and independent review (e.g., by internal audit) that include: the activities of the business units, the activities of the Head of Operational Risk, and the accuracy and completeness of the operational risk loss data. The effectiveness of internal review is itself subject to regular review by the Authority as part of its on-site testing of institutions' compliance.

Collection of Operational Risk Loss Event Data

12 Institutions must put in place systems enabling them to identify and systematically track all material operational loss events. Generally, a materiality threshold of $10,000 should apply. Tracking must relate to operational risk loss *event* data rather than purely to losses occasioned by operational risk. This is because many operational risks may result in no financial loss or even in a profit – e.g. if a 'sell' instruction is incorrectly transacted as a 'buy', and, when unwound, the price proves to have moved in favour of the transacting institution. In such a case, where the potential risk of loss exceeds the reporting threshold, the case remains a 'loss event' since it could have resulted in a financial loss.

13 The complexity and sophistication of institutions' internal reporting arrangements should reflect the overall level of complexity of their business. However, other than for the smallest institutions, management should develop operational loss databases that track loss events on the basis of the mapping approach to event type categories and business lines set out in Appendix A and Appendix B to this paper, Among other things, the effect is to facilitate comparisons between institutions and lines of business.

Monitoring and Reporting

14 Each institution must prepare a regular (normally, quarterly) operational risk report that is distributed to the Board of directors and senior management. It will also be shared with the Authority upon request. Operational risk reports will reflect the scope and sophistication of institution's operational risk frameworks. For example, such a report might include the following information:

i. Data on the level & trend of historical operational losses including, where relevant, a summary of recent operational losses by loss event type (see Attachment C) and of exposures to potential future operational losses;

ii. A brief description of the most significant operational losses for the prior quarter;

iii. Where relevant, summary of operational risks identified and assessed by each line of business during the prior quarter and the status of any corrective actions.

iv. Summary of any operational risks identified as a result of an independent internal (or external) review (e.g. by internal audit, external accountants and/or the Authority) and the status of any corrective actions.

v. Where relevant, a calculation of the capital requirement for operational risk, by line of business.

Role of the Authority

15 The Authority looks to satisfy itself as to the ongoing appropriateness and effectiveness of the operational risk framework in place within institutions. In addition to the matters referred to above, the Authority also maintains under regular review the overall quality and comprehensiveness of institutions' business resumption and contingency plans in order to satisfy itself that, in the event of a severe business disruption, the institution is able to continue to operate and to minimize losses (including those that may arise from disturbances to payment and settlement systems). Similarly, the Authority seeks to ensure that institutions have appropriate IT policies and procedures in place to address such issues as information security and system development, and that they have invested in IT to the extent that is required by the nature, scale and complexity of their operations. In the same way, the Authority scrutinizes carefully the arrangements that institutions have in place to develop, implement and apply appropriate policies and procedures for the assessment, management and monitoring of outsourced activities. In this latter regard, the Authority's approach is set out in its paper 'Outsourcing of Services or Functions by Institutions Licensed under the Banks and Deposit Companies Act 1999'.

16 As part of its role in maintaining the appropriateness and the effectiveness of institutions' operational risk arrangements under regular review, the Authority determines with each institution, the nature and frequency of routine reporting to the Authority of operational risk issues and developments that is to apply. Typically, this involves the provision to the Authority of the standard operational risk reports prepared by institutions for their internal management reporting purposes, or of extracts from these reports.

17 Institutions that are currently seeking to develop and enhance their own approach to the identification, assessment, monitoring and control of operational risks may also like to take account of the additional guidance included in Appendix D to this paper.

APPENDIX A
OPERATIONAL LOSS EVENT TYPE CATEGORIES

Event Type Category (Level 1)	**Categories (Level 2)**	**Activity Examples (Level 3)**
Internal fraud	Unauthorized activity	Transactions not reported (intentional) Transaction type unauthorized (w/ monetary loss) Mis-marking of position (intentional)
	Theft and fraud	Fraud/ credit fraud/ worthless deposits Theft/ extortion/ embezzlement/ robbery Misappropriation of assets Malicious destruction of assets Forgery Check kiting Smuggling Account takeover/ impersonation/ etc. Tax non-compliance/ evasion (willful) Bribes/ kickbacks Insider trading (not on firm's account)
External fraud	Theft and fraud	Theft/ robbery Forgery Cheque kiting
	Systems security	Hacking damage Theft of information (w/ monetary loss)
Employment practices and workplace safety	Employee relations	Compensation, benefit, termination issues Organized labour activity
	Safe environment	General liability (slip and fall, etc) Employee health & safety rules events Workers' compensation
	Diversity & discrimination	All discrimination types
Clients, products and business practices	Suitability, disclosure and fiduciary	Fiduciary breaches/ guideline violations Suitability/ disclosure issues (KYC, etc) Retail customer disclosure violations Breach of privacy Aggressive sales Account churning Misuse of confidential information Lender liability
	Improper business or market practices	Anti-trust Improper trade/ market practices Market manipulation Insider trading (on firm's account) Unlicensed activity Money laundering
	Product flaws	Product defects (unauthorized, etc)
		Model errors
	Selection, sponsorship and exposure	Failure to investigate client per guidelines Exceeding client exposure limits
	Advisory activities	Disputes over performance of advisory activities

APPENDIX A
OPERATIONAL LOSS EVENT TYPE CATEGORIES
(Continued)

Event Type Category (Level 1)	**Categories (Level 2)**	**Activity Examples (Level 3)**
Damage to physical assets	Disasters and other events	Natural disaster losses Human losses from external sources (terrorism, vandalism)
Business disruption and system failures	Systems	Hardware Software Telecommunications Utility outage/ disruptions
Execution, delivery & process management	Transaction capture, execution & maintenance	Miscommunication Data entry, maintenance or loading error Missed deadline or responsibility Model/ system mis-operation Accounting error/ entry attribution error Other task mis-performance Delivery failure Collateral management failure Reference data maintenance
	Monitoring and reporting	Failed mandatory reporting obligation Inaccurate external report (loss incurred)
	Customer intake & documentation	Client permissions/ disclaimer missing Legal documents missing/ incomplete
	Customer/ Client account Management	Unapproved access given to accounts Incorrect client records (loss incurred) Negligent loss or damage of client assets
	Trade counterparties	Non-client counterparty mis-performance Misc. non-client counterparty disputes
	Vendors & suppliers	Outsourcing Vendor disputes

APPENDIX B
MAPPING OF BUSINESS LINES

Level 1	Level 2	Activity Groups
Corporate finance	Corporate finance	Mergers & acquisitions, underwriting, privatizations, securitization, research, debt (government, high yield), equity, syndications IPO, secondary private placements
	Municipal/ Government Finance	
	Merchant banking	
	Advisory services	
Trading & sales	Sales	Fixed income, equity, foreign exchange, commodities, credit, funding, own position securities, lending & repos, brokerage, debt, prime brokerage
	Market making	
	Proprietary positions	
	Treasury	
Retail banking	Retail banking	Retail lending & deposits, banking services, trust & estates
	Private banking	Private lending & deposits, banking services, trust & estates, investment advice
	Card services	Merchant/ commercial/ corporate cards, private labels and retail
Commercial banking	Commercial banking	Project finance, real estate, export finance, trade finance, factoring, leasing, lending, guarantees, bills of exchange
Payment & settlement	External clients	Payments and collections, funds transfer, clearing & settlement
Agency services	Custody	Escrow, depository receipts, securities lending (customers), corporate actions
	Corporate agency	Issuer & paying agents
	Corporate trust	
Asset management	Discretionary fund Management	Pooled, segregated, retail, institutional, closed, open, private equity
	Non-discretionary fund Management	Pooled, segregated, retail, institutional, closed, open
Retail brokerage	Retail brokerage	Execution and full service

APPENDIX C
SAMPLE OPERATIONAL RISK MANAGEMENT REPORT

		Operational Losses ($000)			
Level 1	**Level 2**	**4Q05**	**1Q06**	**2Q06**	**3Q06**
Internal fraud	Unauthorized activity				
	Theft and fraud				
External fraud	Theft and fraud				
	Systems security				
Employment practices & workplace safety	Employee relations				
	Safe environment				
	Diversity & discrimination				
Clients, products & business practices	Suitability, disclosure & fiduciary				
	Improper business or market practices				
	Product flaws				
	Selection, sponsorship & exposure				
	Advisory activities				
Damage to physical assets	Disasters & other events				
Business disruption & system failures	Systems				
Execution, delivery & process mgmt.	Transaction, capture, Execution & maintenance				
	Monitoring & reporting				
	Customer intake & Documentation				
	Customer/ client account Management				
	Trade counterparties				
	Vendors & suppliers				
GRAND TOTALS:					

Appendix D

Approach to the Identification, Assessment, Monitoring and Control of Operational Risk

Identification of Risks

1. Most banks have taken the approach of charging a small group of managers with the task of analyzing each line of business with a view to determining where the institution may be vulnerable to each potential operational risk by type. The process is often enhanced through the use of an independent facilitator. Alternatively, each business's end-to-end processes may be mapped, with a view to similarly identifying the potential operational risk vulnerabilities. Having identified the vulnerabilities, it is then necessary to seek to assess the degree to which the controls in place within the institution may be felt to limit the vulnerability in practice.

2. For example, a bank will be vulnerable to internal fraud if it does not have effective dual control over all assets. Typically, banks will identify the key control points that they need to monitor or test on a regular basis (testing more often for higher risk vulnerabilities) to be sure that their controls are satisfactory to protect them from potential operational losses. Banks also review their historical operational losses to identify root causes of each loss in order to enable them to put better controls in place to prevent such losses from re-occurring in the future. Once a vulnerability to operational risk has been identified, there should be a corrective action plan in place to remedy it.

3. Banks on occasion fail to identify all of their operational losses, largely because they may not appreciate all the types of circumstance giving rise to an operational loss. Many – internal and external fraud risks, for example, and the risks arising out of improper business or market practices, poor 'know your customer' controls etc – will be well-appreciated. Others, however, may be less immediately evident, and banks should therefore review carefully the full range of operational event type loss categories set out in Appendix A to the paper. For example, a large portion of operational losses are frequently legal or litigation-related; these must always be evaluated and included where appropriate. Other examples of operational losses would include rebates or refunds given to clients (e.g. by sales or marketing personnel) in recompense for earlier operating mistakes. Similarly, the cost of terminating an employee's contract over and above the standard severance package – perhaps due to concern about potential vulnerability to suit by such an employee – ranks as an operational loss. A separate range of loss events will relate to execution, delivery and product management; and, for example, will include risks to which institutions become exposed through the use of arrangements such as outsourcing, without the imposition of an acceptable control environment to protect themselves. In order to ensure that all possible losses have been identified, it is

often helpful if a small group of managers get together to discuss possible operational losses on a regular basis, usually just prior to the deadline for the regular submission of the operational loss event data.

Assessing Operational Risks

4. The process of assessing an *inherent operational risk* (i.e., an operational risk before taking into account any controls to mitigate that risk) usually involves an evaluation of both the probability of that risk occurring and an evaluation of the potential impact if that operational risk were to occur. Once an inherent operational risk has been assessed, the relevant controls also need to be assessed in order to form a judgment as to the residual operational risk (i.e., the net operational risk after taking into account the quality of the controls). Some banks use a high/ medium/ low-type evaluation and others use a numerical scale to evaluate their inherent operational risks and the related controls. Some banks use a matrix to evaluate their inherent operational risks (impact x probability) or one to evaluate their residual operational risks (inherent risk x controls) – often on a scale of eg 1 to 3 or 1 to 5.

Monitoring Operational Risks

5. Banks usually monitor their operational risks through the mechanism of a periodic (typically, quarterly) operational risk report. Some banks have each individual line of business prepare an operational risk report so that they can be collated to produce an overall bank-wide report for the Board and senior management.

Controlling/ Mitigating Operational Risks

6. Banks should seek to control their operational risks through strong controls which are matched against each of their material operational risk vulnerabilities, together with a robust overall control environment. At the same time, insurance may be purchased in order to transfer operational risk exposure to the marketplace. Such purchases of insurance in respect of operational risk should be identified within an institution's operational risk policy, and also feature within the periodic operational risk reporting.