TURKS & CAICOS ISLANDS
FINANCIAL SERVICES COMMISSION

Turks & Caicos Islands Financial Services Commission

Guidelines Pursuant to Section 43 of the Financial Services Ordinance 2007

The Management of Operational Risk

Introduction

1 These guidelines apply to all banks licensed under the Banking Ordinance. They are issued under section 43 of the Financial Services Ordinance 2007 to provide guidance as to the conduct expected by the Commission of licensees in the operation of their licensed business. Failure to follow these guidelines is considered by the Commission, and may also be taken into account by the Court, in determining whether there has been a contravention of any financial services Ordinances or other provisions.

2 The effectiveness of banks' operational risk management processes is a key element in determining their soundness. Losses arising from operational risk 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 Commission's assessment of banks to ensure that business is conducted on a continuing basis with proper prudence and banking skills. The Commission assesses carefully the relevant policies adopted by banks and the effectiveness of their implementation; where deficiencies are identified, banks are expected to take corrective action on a timely basis.

3 The Commission seeks to satisfy itself that banks maintain risk management policies and procedures that are appropriate for their individual business profile and risk appetite, as well as with market and macro-economic conditions, 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, banks in the TCI – 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 reputational risk. Legal risk includes expenses (eg 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 eg the cost of general legal advice on an institution's overall corporate strategy.

Categories of operational risk

5 The table in Appendix 1 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 the institution's operations. In particular, institutions *policies and procedures* should cover the following critical elements:

- Policies & procedures
- Role of Board and senior management in overseeing the Operational Risk framework
- Responsibility for implementation of the framework
- Independent control review
- Collection of operational risk loss event data
- Monitoring and reporting

Banks must also ensure that their operational risks frameworks and arrangements are kept under regular review by the Board and senior management, and amended as necessary, having regard to changes in the risk profile as well as external market developments. Changes in strategies, policies and procedures for operational risk management must be approved by the Board.

Operational Risk Framework

7 A bank 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. In the case of a small or highly specialized bank, 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 bank's operations; the role of the board and senior management in overseeing the framework for these risks; the role of the executive who has primary responsibility for the day to day management of the framework; the role of internal audit/compliance in respect of such risks; the collation of basic operational risk event data for circulation to Board and senior management; and basic plans for disaster recovery and business continuity.

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 bank's approach in identifying, assessing, monitoring and controlling/mitigating operational risk throughout its business processes; the 'ownership' and accountabilities for operational risk within the management and control framework (and how they are integrated into the bank's overall risk management processes); details of a quarterly operational risk reporting framework 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; more extensive planning for disaster recovery and business continuity; 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 A bank's Board 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. Members need to be aware of the major aspects of the bank's operational risks as a distinct risk category that should be managed; to approve and periodically review the bank'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. The bank's senior management must: approve and periodically review the operational risk framework; have responsibility for implementing the 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 Commission expects 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 identify 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 with clear internal responsibility at a senior level. This person should be responsible for a clear set of assigned duties including: developing strategies to identify, 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 banks' 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. An appropriate materiality threshold may be set, although that should not exceed $10,000, and in many cases should be appreciably lower. 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 – eg 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 banks' 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 1 and Appendix 2 to this paper, among other things, this helps to facilitate comparisons between institutions and sectors.

Monitoring and Reporting

14 A bank must prepare a regular (normally quarterly) operational risk report for consideration by its Board and senior management. This will also be shared with the Commission upon request. Operational risk reports will reflect the scope and sophistication of the particular operational risk frameworks. However, they should typically include at least the following information:

- Data on the level & trend of historical operational losses and of exposures to potential future operational losses;
- Significant operational losses for the prior quarter, together with a brief description and, where relevant, a summary of recent operational losses by loss event type (see Appendix 3).
- 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.
- Summary of any operational risks identified as a result of internal (or external) review and the status of any corrective actions.

Role of the Commission

15 The Commission looks to satisfy itself as to the ongoing appropriateness and effectiveness of the operational risk framework in place within banks. As part of this process, the Commission also reviews the adequacy of banks' contingency plans for disaster recovery and business continuity in order to satisfy itself that, in the event of a severe business disruption, the bank is able to continue to operate and to minimize losses (including those that may arise from disturbances to payment and settlement systems). Similarly, the Commission seeks to ensure that banks 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 Commission scrutinizes carefully the arrangements that banks have in place to develop, implement and apply appropriate policies and procedures for the assessment, management and monitoring of any activities or processes that they outsource to third parties.

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

APPENDIX 1
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 Check kiting
	Systems security	Hacking damage Theft of information (w/ monetary loss)
Employment practices and workplace safety	Employee relations	Compensation, benefit, termination issues Organized labor 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	Suitabiltiy, 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

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 2
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 3
SAMPLE OPERATIONAL RISK MANAGEMENT REPORT

		Operational Losses ($000)			
Level 1	**Level 2**	**4Q12**	**1Q13**	**2Q13**	**3Q13**
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:					