BANKIGA DHEXE EE SOOMAALIYA

البنك المركزي الصـومـالي

CENTRAL BANK OF SOMALIA

Licensing and Supervision Department

Qaybta Shati-siinta iyo Kormeerka

OPERATIONAL RISK GUIDELINES FOR COMMERCIAL BANKS

2020

Table of Contents

1. Introduction

Management of operational risk is not a new practice; it has always been important for banks to try to prevent fraud, maintain the integrity of internal controls, and reduce errors in transaction processing, and so on.

However, a growing number of high-profile operational loss events worldwide have led banks and supervisors to increasingly view operational risk management as an integral part of the risk management activity.

This guideline outlines the essential principles governing a bank's operational risk management framework and emphasizes the importance for it to be effectively managed, as a distinct risk category.

2. Authority

This guideline is made by the Central Bank of Somalia (CBS) pursuant to its authority set forth in the Financial Institution Law 2012; Chapter XIV —Section 108.

3. Scope

This guideline applies to all institutions licensed by the CBS to engage in banking business in Somalia.

4. Purpose

The aim of this guideline is to bring awareness to banks on the existence and importance of operational risk, and consequentially requiring them to develop and implement a suitable framework for its effective management.

5. Background to Operational Risk

"Operational risk is 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 risks" - BCBS[i] definition.

5.1 Causal Nature of Operational Risk

At the broadest level, there are four possible causes.

- Processes, for example, cash management failures, vendor disputes, shortcomings in the loan approval process.

Basel Committee on Banking Supervision - https://www.bis.org/bcbs/

- People, for example, incompetency, ignorance of established policies or procedures, staffing shortages.

- Systems, for example, cyber-attacks, financial accounting system errors

- External events, for example, terrorism, natural catastrophes, and power outages.

5.2 Types of Operational Risk

There are many ways in which operational risk can manifest itself. This is illustrated below:

Figure 1: Examples of Operational Risk

System failures, data loss due to insufficient back-ups and cyber-attacks from malicious individuals, are the kinds of operational risk from information technology which may threaten the business continuity of a bank. Sanctions from failure to comply with laws e.g. breaches to anti-money laundering and countering the financing of terrorism legislations, and market misconduct may cause huge financial losses to the bank. Operational risk may also arise as a result of external events, like terrorism attacks, external fraud and from natural disasters e.g. tsunami.

5.3 Characteristics of Operational Risk

Operational risk is different from the other risks a bank faces in several respects.

A. Inherent and Pervasive

Operational risk exists in virtually all a bank's products, activities, businesses lines, processes, systems and locations.

B. Greater in number, Frequency and Size

Because of the operational risk's inherent and pervasive nature, the potential sources of operational risk are arguably greater in number and operational risk events tend to be more frequent. In addition, the potential loss from a single event can seriously harm the bank.

C. The Human Factor

The 'human factor' including employee behavior and human resources, poses a major management challenge for banks. Operational risk losses can result from both unintentional and intentional human acts.

D. Capital Not Always the Solution

Though banks hold capital as one of the measures for addressing many types of risks, not all operational risk can be addressed through capital. A notable example is business continuity risk, where capital offers little benefit since if a bank is unable to resume operations following an event, capital cannot restore its operations.

5.4 Threat of Operational Risk

Failure to effectively recognize and manage operational risk may expose a bank to significant losses, which may threaten the bank's existence, and can affect other banks as well.

6. Operational Risk Management

The Basel Committee's Principles for the sound management of operational risk2 describe eleven (11) principles of sound operational risk management, which are the basic principles referred to in this document.

https://www.bis.org/publ/bcbs195.pdf

6.1 Development of Operational Risk Management Environment

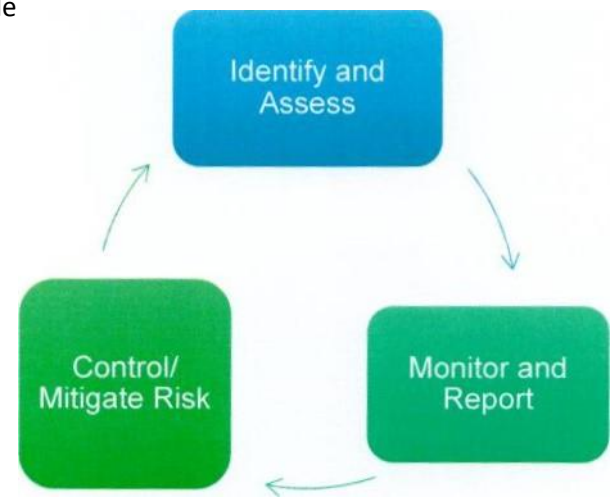
The responsibility to create a culture that supports high ethical standards throughout the organization rests with the banks' Board of Directors and Senior Management. In the operational risk context, an effective risk management framework with adequate policies and procedures should be in place. This should be approved by the Board and implemented by Senior Management consistently throughout the organization. The design, implementation, and maintenance of internal control to manage operational risk falls on Senior management, which should be communicated to all staff such that they understand fully their responsibilities in this aspect.

6.2 Risk Management Cycle

Banks are required to establish an operational risk management framework. This would include, identifying risks to the bank, setting tolerance levels, measuring exposures to those risks, taking steps to control or mitigate the risks, and monitoring and reporting on the bank's risk exposures and capital positions to senior management and the board. This framework should be integrated into the governance structure of the bank.

The risk management cycle is shown diagrammatically, and each component is subsequently explained.

Figure 2: Risk Management Cycle



6.2.1 Identifying and Assessing Operational Risk

Effective risk identification considers both internal factors, such as organizational changes and employee turnover, and external factors, such as changes in the economy and advances in technology. Sound risk assessment allows a bank to better understand its risk profile and most effectively target risk management resources. The following are some of the tools that a bank may employ to identify and assess operational risk:

- Audit findings: while audit findings primarily focus on control weaknesses and vulnerability, they can also provide an insight into inherent risks due to internal or external factors.
- Business Process Mapping: Identifies the key steps in business processes (workflow) and the key risk points.
- Risk self-assessment (RSA): a bank assesses its operations against a library of potential threats and vulnerabilities and considers their potential impact.
- Human Factor: assessment of the staff capacity in order to determine risks associated with their functional roles. Scenario Analysis: a process of obtaining expert opinion of business line and risk managers to identify probable operational risk events and assess their likely outcome.
- New Product Approval Process: before launching a new product, a bank needs to ensure that it will not create undue risk.

6.2.2 Monitoring and Reporting

Banks should implement a process of regular monitoring of their operational risk profile and significant exposure to losses. An appropriate reporting framework should be in place. This includes pertinent information to be regularly reported to Senior Management and the Board for proactive management of operational risk and decision-making purposes.

Operational risk reports need to be comprehensive, accurate, consistent, and actionable across business lines and products. They shall include at a minimum:

- breaches of the bank's risk appetite and tolerance limits
- details of recent significant operational risk events and losses
- relevant external events and any potential impact on the bank

6.2.3 Controlling and Mitigating Risks

Banks should have a strong control environment that utilizes policies, processes, and systems; appropriate internal controls; and appropriate risk mitigation and/or transfer strategies.

Examples of these controls include:

- system for ensuring compliance with policies.
- segregation of duties
- dual control
- clearly established authorities and/or processes for approval
- close monitoring of adherence to assigned risk thresholds or limits.
- safeguards for access to, and use of, bank assets and records
- appropriate staffing level and training to maintain expertise.
- ongoing processes to identify business lines or products where returns appear to be out of line with reasonable expectations.
- regular verification and reconciliation of transactions and accounts and a vacation policy that provides for employees being absent from their duties for at least a minimum number of consecutive days.

Effective use and sound implementation of technology and outsourcing can contribute to the control environment. For example, automated processes are less prone to error than manual processes. However, other risks may be introduced and therefore they need to be appropriately managed.

On risk mitigation, the risk can be:

- Reduced by introducing additional or strengthening internal controls.
- Avoided by reducing the level of activity or exiting it.
- Transferred to another party, for example, through insurance with carefully considered terms and conditions to truly manage the risk.

7. Central Bank's Reporting Requirements

Following are operational risk reports that commercial banks shall send to Central Bank of Somalia in quarterly basis and when deemed necessary the Central bank of Somalia may change the frequency of the reporting.

Table: 1 Operational Risk Required Reports template:

Name of the Bank	
Headquarter Address	
Type of Event	
External Event /internal Event	
Date of occurrence of event	
Date of detection of event	
Financial loss	
Location	
Corrective Actions taken	
Current status	
Reporting Officer Name & Title	

1. Effective Date

This guideline will be effective from May 1st, 2020. In the meantime, Commercial banks shall report progress made regarding the matter.

BANKIGA DHEXE EE SOOMAALIYA

البنك المركزي الصومالي

CBS

CENTRAL BANK OF SOMALIA

Licensing and Supervision Department