South African Reserve Bank
From the Office of
the Registrar of Banks

Ref: 15/8/2

G6/2014

2014-07-22

To: All banks, branches of foreign institutions, controlling companies, eligible institutions and auditors of banks or controlling companies

Guidance Note G6/2014 issued in terms of section 6(5) of the Banks Act, 1990

Application process for approval to adopt the standardised approach or alternative standardised approach for measuring banks' operational risk exposure

Executive summary

In terms of regulation 33(8) of the Regulations relating to Banks (the Regulations), banks, branches of foreign institutions and controlling companies (hereinafter collectively referred to as 'banks') are required to obtain prior written approval from the Registrar of Banks to adopt the standardised approach (TSA) or alternative standardised approach (ASA) for measuring their exposure to operational risk.

The purpose of this guidance note is to inform all banks of the process to be followed and the information to be submitted when applying to adopt the TSA or ASA. This guidance note relates to all future applications to obtain the relevant approval from the Registrar and does not require banks that received approval previously to reapply.

1. Guidance on submitting an application to adopt the standardised approach or the alternative standardised approach

1.1 All banks intending to adopt the TSA or ASA are required to submit a duly completed TSA/ASA application pack, attached hereto as Annexure A. This includes the information stipulated in the various sections of the application pack and a duly completed declaration signed by the applicant bank's chief executive officer.

1.2 This guidance note relates to all future applications to obtain the relevant approval from the Registrar and does not require banks that received approval previously to reapply.

1.3 Banks should notify this Office of their intention to apply to adopt the TSA/ASA at least six months prior to submitting a formal written application.

1.4 This Office requires a period of up to 12 months to consider the application. Upon instruction by this Office, applicant banks will also be required to perform a BA return reporting parallel run during the above-mentioned application period.

1.5 In accordance with the requirements specified in regulation 33(4) of the Regulations, banks are hereby reminded that once a bank has adopted one of the more sophisticated approaches for the measurement of the bank's exposure to operational risk, the bank shall not revert to a simpler approach without the prior written approval of the Registrar.

2. Acknowledgement of receipt

Two additional copies of this guidance note are enclosed for use by your institution's independent auditors. The attached acknowledgement of receipt, duly completed and signed by both the chief executive officer of the institution and the said auditors, should be returned to this Office at the earliest convenience of the aforementioned signatories.

René van Wyk
Registrar of Banks

Encl. 3

The previous guidance note issued was Guidance Note G5/2014, dated 8 July 2014.

Annexure A

Application process for approval to adopt the standardised approach or alternative standardised approach for measuring banks' operational risk exposure

1. Introduction

This document sets out the information to be submitted to the Office of the Registrar of Banks (this Office) of the South African Reserve Bank (SARB) by a bank when applying to adopt the standardised approach (TSA) or alternative standardised approach (ASA) for operational risk capital measurement.

A duly completed application should contain the following:

1.1. Responses to requests for information as contained in this paper (further requests for information, including additional documentation, may be required during the process).

1.2. The declarations and signatures form (signed by the chief executive officer of the applicant bank).

> **Note**
> The submission of a signed application by an applicant bank confirms that the applicant bank grants consent for any information provided as part of the application to be shared with other regulators for the purposes of the approval process.

All information is to be submitted both in electronic format (via CD or USB drive), and hard copy.

2. Scope of application

The application process applies to all banks wishing to adopt the TSA/ASA to calculate their operational risk capital requirement.

Where applications are made by banks with international activities, this Office reserves the right to share the information contained in the application pack with other regulators as needed to support the approval process.

3. Application requirements

Banks are required to provide this Office with the following:

a) summary information on its plans for TSA/ASA implementation;

b) explanation of how the TSA/ASA implementation is organised with respect to the division of responsibilities and capacity allocated;

c) list of entities included in the application;

d) the applicant bank's approach to a number of key areas such as governance;

e) how the applicant bank has met the TSA/ASA qualifying criteria as contained in legislation;

f) the organisational design of the group, including business lines and control functions;

g) description of the group and legal entity structures;

h) overview of the management committee structure;

i) processes followed in dividing the applicant bank's activities into the eight business lines as contained in legislation;

j) design and implementation of an internal operational risk system;

k) role of internal audit;

l) role of external audit;

m) key contact person in the applicant bank for the TSA/ASA application.

4. Overview of the applicant bank's own self-assessment against relevant standards

The information requested in this section is designed to provide this Office with an overview of the applicant bank's own self-assessment conducted against the TSA/ASA minimum standards. This Office proposes to take into account the comprehensiveness and quality of the work undertaken as part of the self-assessment when scoping the supervisory review work.

This Office expects that as part of the application requirements above, applicant banks will produce evidence to demonstrate that it has met the required TSA/ASA minimum standards as stipulated in the Regulations.

This Office recommends that applicant banks initially submit the following completed annexures with regard to the work undertaken to meet the TSA/ASA qualifying criteria:

4.1 Confirmation that self-assessments have taken place and been reviewed by signatory.

Annexure B – Operational risk self-assessment template.
Annexure C – Principles for the Sound Management of Operational Risk[1] template.

4.2 A brief description of the self-assessment processes applicant banks have undertaken, including how self-assessments against each relevant qualitative and quantitative standard were carried out, and details of any parallel runs undertaken prior to the application, including the results and remedial actions taken for unsatisfactory performance against the relevant standard. This section should also include a description of the governance processes followed in terms of completion of the self-assessments.

4.3 Exception-based results of self-assessments, including an indication of the applicant bank's view of materiality. Outline the steps being taken to comply with relevant legislation and indicate the expected completion date of such steps.

[1] Available at http://www.bis.org/publ195.htm.

5. Summary of the applicant bank's approach in a number of key areas

This section is designed to give this Office a summary of the applicant bank's approach in a number of key areas including, but not limited to, governance, internal audit involvement and IT components. This Office is of the opinion that an applicant bank's approach in these areas will be important in determining whether the TSA/ASA application is ultimately approved. These are areas that this Office intends to pay particular attention to in its supervisory review work; however, this could be expanded to focus on additional areas if this Office considers it necessary.

5.1 Governance

As contained in the application requirements, this Office requested high-level information on the applicant bank's governance of operational risk. In this section, this Office requires applicant banks to provide more granular information on operational risk governance. Information to be submitted should include:

5.1.1 A summary of the applicant bank's approach to the governance of operational risk.

5.1.2 A brief explanation of the role of the board (it should be made clear where the board delegates authority to a sub-committee or executive management).

5.1.3 A brief explanation of the role of the operational risk management function and how its independence is ensured; the role of the audit/risk committee; the more general role of senior management in operational risk management; and the role of internal and external audit.

5.1.4 A brief explanation of reporting structures (including how and the frequency with which operational risk committees report upwards to risk management, internal audit and board functions).

5.1.5 A brief explanation of the nature and extent of management information produced at each level within the organisation. Applicant banks should be able to provide a description and example of high-level management information that is produced. Applicant banks should also explain how the nature and content of management information are determined and reviewed, and describe how this is assessed as relevant on an ongoing basis.

5.1.6 A brief overview of the operational risk decision-making process and how it works in practice at different levels within the applicant bank.

5.2 Overview of internal audit's involvement

This Office regards internal audit's involvement in the implementation of TSA/ASA as crucial. The application should hence detail internal audit's tasks relating to TSA/ASA. The information on the role of internal audit should at a minimum include:

5.2.1 The tasks, responsibilities and independence of internal audit.

5.2.2 A description of and motivation for both the audit approach and the audit plan.

5.2.3 Details on the available capacity for audit tasks.

5.2.4 An overview of the audit examinations of the progress of the TSA/ASA implementation, roll-out of and compliance with relevant (proposed) legislation, and the allocation of a rating according to the applicant bank's internal measurement system.

5.2.5 An overview of all unresolved high-risk issues (as per the applicant bank's internal definition), including action plans and expected timelines to resolve them.

5.3 Information technology components (systems, platforms, network components)

The applicant bank should clarify its policy in relation to the IT components that will be used in the TSA/ASA. It should submit the following as a minimum requirement:

5.3.1 A diagram of the centralised and decentralised IT architecture.

5.3.2 The classification of the IT components relating to confidentiality, integrity and availability.

5.4 Documentation

A list of all the internal documents the applicant bank holds that it considers relevant to the application, including a brief description of their contents.

6. Section E – Sign-off

This section should be signed by the chief executive officer of the applicant bank.

6.1 Declaration

By signing and submitting this application form:

- I declare that I am duly authorised to do so.

- I confirm that the information contained within this application is correct, complete, accurate and truthful, and represents a true and fair view to the best of my knowledge and belief and that I have taken all reasonable steps to ensure that this is the case.

- I confirm that I am aware that it may be an offence knowingly or recklessly to give the SARB information that is false or misleading in a material particular.

- I acknowledge that some questions do not require the bank to provide supporting evidence in response. However, the records that demonstrate compliance will be available to the SARB on request.

- I acknowledge that I will notify the SARB immediately if there is a significant change to the information given in the form. If I fail to do so, this may result in a delay in the application process.

- I confirm that I consent to any information provided in relation to this application to be shared with relevant regulators at the SARB's discretion.

Date: _____

Name of signatory: _____

Position of signatory: _____

Signature: _____

Operational risk self-assessment template

The applicant bank is required to complete a self-assessment as outlined in this paper, according to the following criteria:	
Criteria Rating	**Description**
Compliant	All "essential" criteria are met without any significant deficiencies in all operations
Largely compliant	Minor shortcomings, but not sufficient enough to raise doubts about the institution's ability to achieve the objective
Materially non-compliant	Shortcoming is sufficient to raise doubts about the institution's ability to achieve compliance
Non-compliant	No substantive progress towards compliance has been achieved
Not applicable	Deemed not to have relevance

The rating rationale column must be completed at all times, even in instances where a rating of 'Not applicable' has been selected. In addition, banks must ensure that evidence is collected and maintained as substantiation to the 'Criteria Rating' and 'Rating Rationale' as this may be requested for inspection by this Office.

*** Rating Rationale -** Provides justification, explanation, meaning and context and plays an important part in understanding the reasons or principles employed in arriving at the 'Criteria Rating' assigned. Detailed explanations are therefore required in terms of what the bank does in practice. Examples can also be included. Moreover, be reminded that evidence should be collected and maintained.

^ Action Plans - It is recommended that SMART (Specific, Measurable, Attainable, Realistic, Timely) principles are applied when setting action plans. Detailed explanations are therefore required in terms of the steps / actions the bank will be taking to attain the 'Compliant' 'Criteria Rating' status. If 'Compliant' has been selected, then the column can be left blank and / or details can be provided in terms of any maintenance or enhancements planned.

A. OPERATIONAL RISK GOVERNANCE

Area of Assessment	Reference	#	Criteria	Information Request	Assessment Rating	Rating Rationale	Action Plans
Board of Directors							
1. Board of Director approvals	**Reg 33** (8)(b)(i)(A)	1.1	The board of directors are actively involved in the oversight of the operational risk management framework.	(a) Frequency of Board review of firm-wide framework to operational risk management.			
2. Operational risk strategy	**Reg 33** (8)(b)(i)(B)	2.1	The bank has an operational risk management system that is conceptually sound and is implemented with integrity.	None			
3. Role of senior management	**Reg 33** (8)(b)(i)(A)	3.1	Senior management is actively involved in the oversight of the operational risk management framework.	None			
Operational Risk Management Function							
4. Operational risk management function	**Reg 33** (8)(b)(ii)(A)	4.1	The bank has an operational risk management system with clear responsibilities assigned to an operational risk management function.	None			
		4.2	The operational risk management function develops strategies to identify, assess, monitor and control/mitigate operational risk.	None			
		4.3	The operational risk management function develops comprehensive policies and procedures concerning operational risk management and controls.	None			
		4.4	The operational risk management function designs and implements a methodology to comprehensively assess the bank's exposure to operational risk.	None			
		4.5	The operational risk management function designs and implements the risk-reporting system for operational risk.	None			
Risk Management - Operational Risk							
5. Operational Risk control and mitigation	**Reg 33** (8)(b)(ii)(D) and (E)	5.1	The bank has an operational risk management system that is well documented.	None			
		5.2	The bank has a routine in place for ensuring compliance with a documented set of internal policies, controls and procedures concerning the operational risk management system, which includes policies for the treatment of non-compliance issues.	(a) Describe how the bank ensures compliance with its internal policies, controls and procedures for operational risk.			
6. Staffing	**Reg 33** (8)(b)(i)(C)	6.1	The bank has sufficient resources in the major business lines to implement the adopted approach to operational risk, including control and audit areas.	None			
Internal Audit Function							
7. Internal audit coverage	**Reg 33** (8)(b)(ii)(F)	7.1	The bank's operational risk management processes and assessment system are subject to validation and regular independent review (these reviews include the activities of both the business units and of the operational risk management function).	(a) Describe the responsibilities of the audit function with respect to operational risk.			

A. OPERATIONAL RISK GOVERNANCE

Area of Assessment	Reference	#	Criteria	Information Request	Assessment Rating	Rating Rationale	Action Plans
Operational Risk Reporting							
8. Regular and effective monitoring of operational risk profile	**Reg 33** (8)(b)(ii)(C) and (E)(i)	8.1	The bank has regular reporting of operational risk exposures, including material operational losses, to business unit management, senior management, and to the board of directors.	(a) Identify operational risk reporting activities directed at senior management and the board of directors and indicate the frequency.			
		8.2	The bank has procedures for taking appropriate action according to the information within the management reports.	(a) Describe how the bank uses the information within operational risk management reports.			

B. GROSS INCOME MAPPING

Area of Assessment	Reference	#	Criteria	Information Request	Assessment Rating	Rating Rationale	Action Plans
1. Gross income mapping policies and documentation	Reg 33 (8)(b)(i)(D)	1.1	Specific policies and documentation of criteria have been developed for mapping gross income for current business lines and activities into the standardised framework.	(a) Provide all policies and documentation of criteria developed for mapping gross income.			
		1.2	Criteria must be reviewed and adjusted for new or changing business activities as appropriate.	None			
2. Principles of business line mapping	Reg 33 (8)(d)(ii)	2.1	All activities are mapped into one of the eight business lines in a mutually exclusive and jointly exhaustive manner.	(a) Identify if all activities have been mapped into the eight level 1 business lines in a mutually exclusive and jointly exhaustive manner.			
				(b) Identify any existing gaps and the action plans to close them.			
	Reg 33 (8)(d)(ii)(B)	2.2	Any banking/non-banking activity that cannot be readily mapped into the business line framework, but which represents an ancillary function to an activity included in the framework, are allocated to the business line it supports.	None			
		2.3	If more than one business line is supported through the ancillary activity, an objective mapping criteria is used.	(a) If appropriate, describe the objective mapping criteria being used.			
	Reg 33 (8)(d)(ii)(C)	2.4	If an activity cannot be mapped into a particular business line then the business line yielding the highest charge is used. The same business line equally applies to any associated ancillary activity.	(a) Identify any activities that could not be mapped into a particular business line and provide the charge used.			
	Reg 33 (8)(d)(iii)	2.5	Internal pricing methods are used to allocate gross income between business lines provided that total gross income for the bank still equals the sum of gross income for the eight business lines.	(a) Discuss the pricing methods used to allocate gross income.			
	Reg 33 (8)(d)(ii)(A)	2.6	Mapping activities into business lines for operational risk capital purposes are consistent with the definitions of business lines used for regulatory capital calculations in other risk categories. Any deviations must be clearly motivated and documented.	(a) Identify any activities that are inconsistent with Basel business line definitions.			
				(b) Identify motivations for any existing deviations.			
	Reg 33 (8)(d)(iv)	2.7	The mapping process is clearly documented. More specifically, business line definitions are sufficiently documented to allow for business line mapping replication.	(a) Identify documentation for mapping process and assess its allowance for business line mapping replication.			
		2.8	Documentation clearly motivate any exceptions or overrides and be kept on record.	(a) Identify how documentation addresses exceptions and overrides.			
	Reg 33 (8)(d)(v)	2.9	Processes are in place to define the mapping of any new activities or products.	(a) Identify processes in place to define the mapping of any new activities or products.			
	Reg 33 (8)(d)(i)	2.10	Senior management is responsible for the mapping policy.	(a) Identify who is responsible for the mapping policy.			
				(b) Identify the format in which the mapping policy has been presented and approved by the Board			
	Reg 33 (8)(d)(vi)	2.11	The mapping process to business lines is subject to independent review.	(a) Identify if the mapping process has been subject to independent review (and by whom). If independent review has not taken place, identify future plans to do so.			

C. LOSS DATA COLLECTION

Area of Assessment	Reference	#	Criteria	Information Request	Assessment Rating	Rating Rationale	Action Plans
1. Bank's internal operational risk assessment system using operational loss data	**Reg 33** (8)(b)(ii)(B)	1.1	The bank has a systematic tracking of relevant operational risk data including material losses by business line.	(a) Provide details on the operational loss data collection process (centralized vs. decentralized).			
				(b) List the source systems used and provide detail on how they are used in the loss collection process.			
				(c) Identify the function responsible for the data collection.			
				(d) List the criteria for collection of operational losses.			
				(e) Identify the status of data collection on an enterprise wide level.			
				(f) Provide the historical length of operational loss data.			
				(g) Identify how the bank ensures that data is collected in a complete and consistent manner.			
				(h) Identify whether operational losses are mapped to Basel II lines of business and event types.			
				(i) List the data fields populated in the collection of loss data.			
				(j) Describe how the bank distinguishes credit and market risk losses that are a result of operational events.			
				(k) Provide details on how the bank collects multiple operational losses resulting from one event.			
				(l) List all policies & procedure documents relating to loss data collection.			
		1.2	There is close integration of the operational risk assessment system into the risk management process of the bank.	(a) Explain how the bank uses the operational risk assessment system in its risk management process.			
		1.3	Output is an integral part of the process of monitoring controlling the banks operational risk profile.	(a) Describe how the bank uses operational risk data (including loss data) to monitor the banks operational risk profile.			
		1.4	Operational risk data (including loss data) has a role in risk reporting, management reporting, and risk analysis.	(a) List all reports using operational risk data (including loss data), identifying how the reports are distributed.			
	Reg 33 (8)(b)(ii)(A)(v)	1.5	There are techniques for creating incentives to improve the management of operational risk throughout the firm.	(a) Identify any techniques the bank uses for creating incentives to improve the management of operational risk throughout the firm.			
2. Regular reporting of operational risk exposures	**Reg 33** (8)(b)(ii)(C) and (E)	2.1	There is regular reporting of operational risk exposures, including material operational losses, to business unit management, senior management, and to the board of directors.	(a) List all reports that include operational risk exposures (including material losses), identifying frequency, owners of report and audience of the report.			
		2.2	There are procedures for taking appropriate action according to the information within the management reports.	(a) Describe how the operational risk exposure reports are used to respond to operational risk and the management of the risk.			

D. RISK AND CONTROL SELF-ASSESSMENT / KEY RISK INDICATORS

Area of Assessment	Reference	#	Criteria	Information Request	Assessment Rating	Rating Rationale	Action Plans
1. Reporting	n/a	1.1	Operational risk results from risk assessment tools are reported and used in the management of operational risk.	(a) List all reports of risk assessment tools and indicate how they are used.			
		1.2	There is appropriate reporting of results from risk assessments tools to the Board, senior management and business units.	None			

Basel Committee on Banking Supervision (BCBS) Paper
Principles for the Sound Management of Operational Risk

This Office continually monitors developments with regard to operational risk. In this regard the BCBS issued two consultative documents on operational risk in December 2010, namely "Sound practices for the management and supervision of operational risk" and "Operational risk: Supervisory guidelines for the advanced measurement approaches". South African banks were invited to respond to these two documents and to highlight any practical difficulties foreseen or potential effects on both themselves and the general banking sector that would require some consideration from the BCBS. This Office received feedback on both papers from banks during the first quarter of 2011 and consolidated and presented the comments to the Standards Implementation Group Operational Risk (SIGOR) for its consideration. The two final papers were published by the BCBS during June 2011.

The first paper, "Principles for the Sound Management of Operational Risk" (Available at http://www.bis.org/publ/bcbs195.htm) updates and replaces the Basel Committee's 2003 paper entitled "Sound practices for the management and supervision of operational risk". The updated version highlights the evolution of operational risk management since 2003, and is based on best industry practice and supervisory experience. The Basel Committee anticipated that industry sound practice would continue to evolve, and banks and supervisors have expanded their knowledge and experience in implementing operational risk management frameworks. A range of practice reviews covering governance, data and modelling issues, loss data collection exercises, and quantitative impact studies (QISs) have also contributed to industry and supervisory knowledge and the emergence of sound industry practice. The principles outlined in the report are discussed within the context of four overarching themes: (i) fundamental principles of operational risk management, (ii) governance, (iii) risk management environment and (iv) role of disclosure.

Banks are required to complete a self-assessment against the principles outlined in the paper, according to the following criteria:

Criteria Rating	Description
Compliant	All "essential" criteria are met without any significant deficiencies in all operations
Largely compliant	Minor shortcomings, but not sufficient enough to raise doubts about the institution's ability to achieve the objective of a given principle
Materially non-compliant	Shortcoming is sufficient to raise doubts about the institution's ability to achieve compliance
Non-compliant	No substantive progress towards compliance has been achieved
Not applicable	A principle deemed not to have relevance

The rating rationale column must be completed at all times, even in instances where a rating of 'Not applicable' has been selected. In addition, banks must ensure that evidence is collected and maintained as substantiation to the 'Criteria Rating' and 'Rating Rationale' as this may be requested for inspection by this Office. Furthermore, the BCBS paper and documents referred to in the body and footnotes thereof, should be read in full to be able to consider as sound practices where applicable as well as for understanding and information purposes.

* **Rating Rationale** - Provides justification, explanation, meaning and context and plays an important part in understanding the reasons or principles employed in arriving at the 'Criteria Rating' assigned. Detailed explanations are therefore required in terms of what the bank does in practice. Examples can also be included. Moreover, be reminded that evidence should be collected and maintained.

^ **Action Plans** - It is recommended that SMART (Specific, Measurable, Attainable, Realistic, Timely) principles are applied when setting action plans. Detailed explanations are therefore required in terms of the steps / actions the bank will be taking to attain the 'Compliant' 'Criteria Rating' status. If 'Compliant' has been selected, then the column can be left blank and / or details can be provided in terms of any maintenance or enhancements planned.

Principle	Description / Criteria	Paragraph #	Paragraph Description	Sub - Paragraph	Criteria Rating	Rating Rationale*	Action Plans^
Fundamental principles of operational risk management							
1	**The board of directors should take the lead in establishing a strong risk management culture. The board of directors and senior management should establish a corporate culture that is guided by strong risk management and that supports and provides appropriate standards and incentives for professional and responsible behaviour. In this regard, it is the responsibility of the board of directors to ensure that a strong operational risk management culture exists throughout the whole organisation.**	21	Banks with a strong culture of risk management and ethical business practices are less likely to experience potentially damaging operational risk events and are better placed to deal effectively with those events that do occur. The actions of the board and senior management, and policies, processes and systems provide the foundation for a sound risk management culture.	None			
		22	The board should establish a code of conduct or an ethics policy that sets clear expectations for integrity and ethical values of the highest standard and identify acceptable business practices and prohibited conflicts. Clear expectations and accountabilities ensure that bank staff understand their roles and responsibilities for risk, as well as their authority to act. Strong and consistent senior management support for risk management and ethical behaviour convincingly reinforces codes of conduct and ethics, compensation strategies, and training programmes. Compensation policies should be aligned to the bank's statement of risk appetite and tolerance, long-term strategic direction, financial goals and overall safety and soundness. They should also appropriately balance risk and reward.	None			
		23	Senior management should ensure that an appropriate level of operational risk training is available at al levels throughout the organisation. Training that is provided should reflect the seniority, role and responsibilities of the individuals for whom it is intended.	None			
2	**Banks should develop, implement and maintain a Framework that is fully integrated into the bank's overall risk management processes. The Framework for operational risk management chosen by an individual bank will depend on a range of factors, including its nature, size, complexity and risk profile.**	24	The fundamental premise of sound risk management is that the board of directors and bank management understand the nature and complexity of the risks inherent in the portfolio of bank products, services and activities. This is particularly important for operational risk, given that operational risk is inherent in all business products, activities, processes and systems.	None			
		25	A vital means of understanding the nature and complexity of operational risk is to have the components of the Framework fully integrated into the overall risk management processes of the bank. The Framework should be appropriately integrated into the risk management processes across all levels of the organisation including those at the group and business line levels, as well as into new business initiatives' products, activities, processes and systems. In addition, results of the bank's operational risk assessment should be incorporated into the overall bank business strategy development processes	None			

Principle	Description / Criteria	Paragraph #	Paragraph Description	Sub - Paragraph	Criteria Rating	Rating Rationale*	Action Plans^
		26	The Framework should be comprehensively and appropriately documented in board of directors approved policies and should include definitions of operational risk and operational loss. Banks that do not adequately describe and classify operational risk and loss exposure may significantly reduce the effectiveness of their Framework.	None			
		27	Framework documentation should clearly:	(a) identify the governance structures used to manage operational risk, including reporting lines and accountabilities;			
				(b) describe the risk assessment tools and how they are			
				(c) describe the bank's accepted operational risk appetite and tolerance, as well as thresholds or limits for inherent and residual risk, and approved risk mitigation strategies and instruments;			
				(d) describe the bank's approach to establishing and monitoring thresholds or limits for inherent and residual risk exposure;			
				(e) establish risk reporting and Management Information Systems (MIS);			
				(f) provide for a common taxonomy of operational risk terms to ensure consistency of risk identification, exposure rating and risk management objectives;			
				(g) provide for appropriate independent review and assessment of operational risk; and			
				(h) require the policies to be reviewed whenever a material change in the operational risk profile of the bank occurs, and revised as appropriate;			
Governance							
The Board of Directors							
3	**The board of directors should establish, approve and periodically review the Framework. The board of directors should oversee senior management to ensure that the policies, processes and systems are implemented effectively at all decision levels.**	28	The board of directors should:	(a) establish a management culture, and supporting processes, to understand the nature and scope of the operational risk inherent in the bank's strategies and activities, and develop comprehensive, dynamic oversight and control environments that are fully integrated into or coordinated with the overall framework for managing all risks across the enterprise;			
				(b) provide senior management with clear guidance and direction regarding the principles underlying the Framework and approve the corresponding policies developed by senior management;			
				(c) regularly review the Framework to ensure that the bank has identified and is managing the operational risk arising from external market changes and other environmental factors, as well as those operational risks associated with new products, activities, processes or systems, including changes in risk profiles and priorities (e.g. changing			
				(d) ensure that the bank's Framework is subject to effective independent review by audit or other appropriately trained parties;and			
				(e) ensure that as best practice evolves management is availing themselves of these advances.			
		29	Strong internal controls are a critical aspect of operational risk management, and the board of directors should establish clear lines of management responsibility and accountability for implementing a strong control environment. The control environment should provide appropriate independence/separation of duties between operational risk management functions, business lines and	None			
4	**The board of directors should approve and review a risk appetite and tolerance statement for operational risk that articulates the nature, types and levels of operational risk that the bank is willing to assume.**	30	When approving and reviewing the risk appetite and tolerance statement, the board of directors should consider all relevant risks, the bank's level of risk aversion, its current financial condition and the bank's strategic direction. The risk appetite and tolerance statement should encapsulate the various operational risk appetites within a bank and ensure that they are consistent. The board of directors should approve appropriate thresholds or limits for specific operational risks, and an overall operational risk appetite	None			
		31	The board of directors should regularly review the appropriateness of limits and the overall operational risk appetite and tolerance statement. This review should consider changes in the external environment, material increases in business or activity volumes, the quality of the control environment, the effectiveness of risk management or mitigation strategies, loss experience, and the frequency, volume or nature of limit breaches. The board should monitor management adherence to the risk appetite and tolerance statement and provide for timely detection and remediation of breaches.	None			

Principle	Description / Criteria	Paragraph #	Paragraph Description	Sub - Paragraph	Criteria Rating	Rating Rationale*	Action Plans^
Senior Management							
5	**Senior management should develop for approval by the board of directors a clear, effective and robust governance structure with well defined, transparent and consistent lines of responsibility. Senior management is responsible for consistently implementing and maintaining throughout the organisation policies, processes and systems for managing operational risk in all of the bank's material products, activities, processes and systems consistent with the risk appetite and tolerance.**	32	Senior management is responsible for establishing and maintaining robust challenge mechanisms and effective issue-resolution processes. These should include systems to report, track and, when necessary, escalate issues to ensure resolution. Banks should be able to demonstrate that the three lines of defence approach is operating satisfactorily and to explain how the board and senior management ensure that this approach is implemented and operating in an appropriate and acceptable manner.	None			
		33	Senior management should translate the operational risk management Framework established by the board of directors into specific policies and procedures that can be implemented and verified within the different business units. Senior management should clearly assign authority, responsibility and reporting relationships to encourage and maintain accountability, and to ensure that the necessary resources are available to manage operational risk in line within the bank's risk appetite and tolerance statement. Moreover, senior management should ensure that the management oversight process is appropriate for the risks inherent in a business unit's activity.	None			
		34	Senior management should ensure that staff responsible for managing operational risk coordinate and 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 risk transfer and outsourcing arrangements. Failure to do so could result in significant gaps or overlaps in a bank's overall risk management programme.	None			
		35	The managers of the CORF should be of sufficient stature within the bank to perform their duties effectively, ideally evidenced by title commensurate with other risk management functions such as credit, market and liquidity	None			
		36	Senior management should ensure that bank activities are conducted by staff with the necessary experience, technical capabilities and access to resources. Staff responsible for monitoring and enforcing compliance with the institution's risk policy should have authority independent from the units they oversee.	None			
		37	A bank's governance structure should be commensurate with the nature, size, complexity and risk profile of its activities. When designing the operational risk governance structure, a bank should take the following into consideration:	(a) Committee structure – Sound industry practice for larger and more complex organisations with a central group function and separate business units is to utilise a board-created enterprise level risk committee for overseeing all risks, to which a management level operational risk committee reports. Depending on the nature, size and complexity of the bank, the enterprise level risk committee may receive input from operational risk committees by country, business or functional area. Smaller and less complex organisations may utilise a flatter organisational structure that oversees operational risk directly within the board's risk management committee;			
				(b) Committee composition – Sound industry practice is for operational risk committees (or the risk committee in smaller banks) to include a combination of members with expertise in business activities and financial, as well as independent risk management. Committee membership can also include independent non-executive board members, which is a requirement in some jurisdictions; and			
				(c) Committee operation – Committee meetings should be held at appropriate frequencies with adequate time and resources to permit productive discussion and decision-making. Records of committee operations should be adequate to permit review and evaluation of committee			

Principle	Description / Criteria	Paragraph #	Paragraph Description	Sub - Paragraph	Criteria Rating	Rating Rationale*	Action Plans^
Risk Management Environment							
Identification and Assessment							
6	**Senior management should ensure the identification and assessment of the operational risk inherent in all material products, activities, processes and systems to make sure the inherent risks and incentives are well understood.**	38	Risk identification and assessment are fundamental characteristics of an effective operational risk management system. Effective risk identification considers both internal factors and external factors. Sound risk assessment allows the bank to better understand its risk profile and allocate risk management resources and strategies most effectively.	None			
		39	Examples of tools that may be used for identifying and assessing operational risk include:	(a) Audit Findings: While audit findings primarily focus on control weaknesses and vulnerabilities, they can also provide insight into inherent risk due to internal or external			
				(b) Internal Loss Data Collection and Analysis: Internal operational loss data provides meaningful information for assessing a bank's exposure to operational risk and the effectiveness of internal controls. Analysis of loss events can provide insight into the causes of large losses and information on whether control failures are isolated or systematic. Banks may also find it useful to capture and monitor operational risk contributions to credit and market risk related losses in order to obtain a more complete view of their operational risk exposure;			
				(c) External Data Collection and Analysis: External data elements consist of gross operational loss amounts, dates, recoveries, and relevant causal information for operational loss events occurring at organisations other than the bank. External loss data can be compared with internal loss data, or used to explore possible weaknesses in the control environment or consider previously unidentified risk			
				(d) Risk Assessments: In a risk assessment, often referred to as a Risk Self Assessment (RSA), a bank assesses the processes underlying its operations against a library of potential threats and vulnerabilities and considers their potential impact. A similar approach, Risk Control Self Assessments (RCSA), typically evaluates inherent risk (the risk before controls are considered), the effectiveness of the control environment, and residual risk (the risk exposure after controls are considered). Scorecards build on RCSAs by weighting residual risks to provide a means of translating the RCSA output into metrics that give a relative ranking of the control environment;			
				(e) Business Process Mapping: Business process mappings identify the key steps in business processes, activities and organisational functions. They also identify the key risk points in the overall business process. Process maps can reveal individual risks, risk interdependencies, and areas of control or risk management weakness. They also can help prioritise subsequent management action;			
				(f) Risk and Performance Indicators: Risk and performance indicators are risk metrics and/or statistics that provide insight into a bank's risk exposure. Risk indicators, often referred to as Key Risk Indicators (KRIs), are used to monitor the main drivers of exposure associated with key risks. Performance indicators, often referred to as Key Performance Indicators (KPIs), provide insight into the status of operational processes, which may in turn provide insight into operational weaknesses, failures, and potential loss. Risk and performance indicators are often paired with escalation triggers to warn when risk levels approach or exceed thresholds or limits and prompt mitigation plans;			
				(g) Scenario Analysis: Scenario analysis is a process of obtaining expert opinion of business line and risk managers to identify potential operational risk events and assess their potential outcome. Scenario analysis is an effective tool to consider potential sources of significant operational risk and the need for additional risk management controls or mitigation solutions. Given the subjectivity of the scenario process, a robust governance framework is essential to ensure the integrity and consistency of the process;			
				(h) Measurement: Larger banks may find it useful to quantify their exposure to operational risk by using the output of the risk assessment tools as inputs into a model that estimates operational risk exposure. The results of the model can be used in an economic capital process and can be allocated to business lines to link risk and return; and			

Principle	Description / Criteria	Paragraph #	Paragraph Description	Sub - Paragraph	Criteria Rating	Rating Rationale*	Action Plans^
				(i) Comparative Analysis: Comparative analysis consists of comparing the results of the various assessment tools to provide a more comprehensive view of the bank's operational risk profile. For example, comparison of the frequency and severity of internal data with RCSAs can help the bank determine whether self assessment processes are functioning effectively. Scenario data can be compared to internal and external data to gain a better understanding of the severity of the bank's exposure to potential risk events.			
		40	The bank should ensure that the internal pricing and performance measurement mechanisms appropriately take into account operational risk. Where operational risk is not considered, risk-taking incentives might not be appropriately aligned with the risk appetite and tolerance.	None			
7	**Senior management should ensure that there is an approval process for all new products, activities, processes and systems that fully assesses operational risk.**	41	In general, a bank's operational risk exposure is increased when a bank engages in new activities or develops new products; enters unfamiliar markets; implements new business processes or technology systems; and/or engages in businesses that are geographically distant from the head office. Moreover, the level of risk may escalate when new products activities, processes, or systems transition from an introductory level to a level that represents material sources of revenue or business-critical operations. A bank should ensure that its risk management control infrastructure is appropriate at inception and that it keeps pace with the rate of growth of, or changes to, products activities, processes	None			
		42	A bank should have policies and procedures that address the process for review and approval of new products, activities, processes and systems. The review and approval process should consider:	(a) inherent risks in the new product, service, or activity;			
				(b) changes to the bank's operational risk profile and appetite and tolerance, including the risk of existing products or activities;			
				(c) the necessary controls, risk management processes, and risk mitigation strategies;			
				(d) the residual risk;			
				(e) changes to relevant risk thresholds or limits; and			
				(f) the procedures and metrics to measure, monitor, and manage the risk of the new product or activity.			
				The approval process should also include ensuring that appropriate investment has been made for human resources and technology infrastructure before new products are introduced. The implementation of new products, activities, processes and systems should be monitored in order to identify any material differences to the expected operational risk profile, and to manage any unexpected risks.			
Monitoring and Reporting							
8	**Senior management should implement a process to regularly monitor operational risk profiles and material exposures to losses. Appropriate reporting mechanisms should be in place at the board, senior management, and business line levels that support proactive management of operational risk.**	43	Banks are encouraged to continuously improve the quality of operational risk reporting. A bank should ensure that its reports are comprehensive, accurate, consistent and actionable across business lines and products. Reports should be manageable in scope and volume; effective decision-making is impeded by both excessive amounts and paucity of data.	None			
		44	Reporting should be timely and a bank should be able to produce reports in both normal and stressed market conditions. The frequency of reporting should reflect the risks involved and the pace and nature of changes in the operating environment. The results of monitoring activities should be included in regular management and board reports, as should assessments of the Framework performed by the internal audit and/or risk management functions. Reports generated by (and/or for) supervisory authorities should also be reported internally to senior management and the board, where appropriate.	None			
		45	Operational risk reports may contain internal financial, operational, and compliance indicators, as well as external market or environmental information about events and conditions that are relevant to decision making. Operational risk reports should include:	(a) breaches of the bank's risk appetite and tolerance statement, as well as thresholds or limits;			
				(b) details of recent significant internal operational risk events and losses;and			
				(c) relevant external events and any potential impact on the bank and operational risk capital.			
		46	Data capture and risk reporting processes should be analysed periodically with a view to continuously enhancing risk management performance as well as advancing risk management policies, procedures and practices.	None			

Principle	Description / Criteria	Paragraph #	Paragraph Description	Sub - Paragraph	Criteria Rating	Rating Rationale*	Action Plans^
Control and Mitigation							
9	**Banks should have a strong control environment that utilises policies, processes and systems; appropriate internal controls; and appropriate risk mitigation and/or transfer strategies.**	47	Internal controls should be designed to provide reasonable assurance that a bank will have efficient and effective operations; safeguard its assets; produce reliable financial reports; and comply with applicable laws and regulations. A sound internal control programme consists of five components that are integral to the risk management process: control environment, risk assessment, control activities, information and communication, and monitoring	None			
		48	Control processes and procedures should include a system for ensuring compliance with policies. Examples of principle elements of a policy compliance assessment include:	(a) top-level reviews of progress towards stated objectives;			
				(b) verifying compliance with management controls;			
				(c) review of the treatment and resolution of instances of non-compliance;			
				(d) evaluation of the required approvals and authorisations to ensure accountability to an appropriate level of management;and			
				(e) tracking reports for approved exceptions to thresholds or limits, management overrides and other deviations from			
		49	An effective control environment also requires appropriate segregation of duties. Assignments that establish conflicting duties for individuals or a team without dual controls or other countermeasures may enable concealment of losses, errors or other inappropriate actions. Therefore, areas of potential conflicts of interest should be identified, minimised, and be subject to careful independent monitoring and review.	None			
		50	In addition to segregation of duties and dual control, banks should ensure that other traditional internal controls are in place as appropriate to address operational risk. Examples of these controls include:	(a) clearly established authorities and/or processes for approval;			
				(b) close monitoring of adherence to assigned risk thresholds or limits;			
				(c) safeguards for access to, and use of, bank assets and records;			
				(d) appropriate staffing level and training to maintain			
				(e) ongoing processes to identify business lines or products where returns appear to be out of line with reasonable expectations;			
				(f) regular verification and reconciliation of transactions and accounts; and			
				(g) a vacation policy that provides for officers and employees being absent from their duties for a period of not less than two consecutive weeks.			
		51	Effective use and sound implementation of technology can contribute to the control environment. For example, automated processes are less prone to error than manual processes. However, automated processes introduce risks that must be addressed through sound technology governance and infrastructure risk management	None			
		52	The use of technology related products, activities, processes and delivery channels exposes a bank to strategic, operational, and reputational risks and the possibility of material financial loss. Consequently, a bank should have an integrated approach to identifying, measuring, monitoring and managing technology risks. Sound technology risk management uses the same precepts as operational risk management and includes:	(a) governance and oversight controls that ensure technology, including outsourcing arrangements, is aligned with and supportive of the bank's business objectives;			
				(b) policies and procedures that facilitate identification and assessment of risk;			
				(c) establishment of a risk appetite and tolerance statement as well as performance expectations to assist in controlling and managing risk;			
				(d) implementation of an effective control environment and the use of risk transfer strategies that mitigate risk; and			
				(e) monitoring processes that test for compliance with policy thresholds or limits.			
		53	Management should ensure the bank has a sound technology infrastructure that meets current and long-term business requirements by providing sufficient capacity for normal activity levels as well as peaks during periods of market stress; ensuring data and system integrity, security, and availability; and supporting integrated and comprehensive risk management. Mergers and acquisitions resulting in fragmented and disconnected infrastructure, cost-cutting measures or inadequate investment can undermine a bank's ability to aggregate and analyse information across risk dimensions or the consolidated enterprise, manage and report risk on a business line or legal entity basis, or oversee and manage risk in periods of high growth. Management should make appropriate capital investment or otherwise provide for a robust infrastructure at all times, particularly before mergers are consummated, high growth strategies are initiated, or new products are introduced.	None			

Principle	Description / Criteria	Paragraph #	Paragraph Description	Sub - Paragraph	Criteria Rating	Rating Rationale*	Action Plans^
		54	Outsourcing is the use of a third party – either an affiliate within a corporate group or an unaffiliated external entity – to perform activities on behalf of the bank. Outsourcing can involve transaction processing or business processes. While outsourcing can help manage costs, provide expertise, expand product offerings, and improve services, it also introduces risks that management should address. The board and senior management are responsible for understanding the operational risks associated with outsourcing arrangements and ensuring that effective risk management policies and practices are in place to manage the risk in outsourcing activities. Outsourcing policies and risk management activities should encompass:	(a) procedures for determining whether and how activities can be outsourced;			
				(b) processes for conducting due diligence in the selection of potential service providers;			
				(c) sound structuring of the outsourcing arrangement, including ownership and confidentiality of data, as well as termination rights;			
				(d) programmes for managing and monitoring the risks associated with the outsourcing arrangement, including the financial condition of the service provider;			
				(e) establishment of an effective control environment at the bank and the service provider;			
				(f) development of viable contingency plans; and			
				(g) execution of comprehensive contracts and/or service level agreements with a clear allocation of responsibilities between the outsourcing provider and the bank.			
		55	In those circumstances where internal controls do not adequately address risk and exiting the risk is not a reasonable option, management can complement controls by seeking to transfer the risk to another party such as through insurance. The board of directors should determine the maximum loss exposure the bank is willing and has the financial capacity to assume, and should perform an annual review of the bank's risk and insurance management programme. While the specific insurance or risk transfer needs of a bank should be determined on an individual basis, many jurisdictions have regulatory requirements that must be considered.	None			
		56	Because risk transfer is an imperfect substitute for sound controls and risk management programmes, banks should view risk transfer tools as complementary to, rather than a replacement for, thorough internal operational risk control. Having mechanisms in place to quickly identify, recognise and rectify distinct 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, transfer the risk to another business sector or area, or create a new risk (e.g. counterparty risk).	None			

Principle	Description / Criteria	Paragraph #	Paragraph Description	Sub - Paragraph	Criteria Rating	Rating Rationale*	Action Plans^
Business Resiliency and Continuity							
10	**Banks should have business resiliency and continuity plans in place to ensure an ability to operate on an ongoing basis and limit losses in the event of severe business disruption.**	57	Banks are exposed to disruptive events, some of which may be severe and result in an inability to fulfil some or all of their business obligations. Incidents that damage or render inaccessible the bank's facilities, telecommunication or information technology infrastructures, or a pandemic event that affects human resources, can result in significant financial losses to the bank, as well as broader disruptions to the financial system. To provide resiliency against this risk, a bank should establish business continuity plans commensurate with the nature, size and complexity of their operations. Such plans should take into account different types of likely or plausible scenarios to which the bank may	None			
		58	Continuity management should incorporate business impact analysis, recovery strategies, testing, training and awareness programmes, and communication and crisis management programmes. A bank should identify critical business operations, key internal and external dependencies, and appropriate resilience levels. Plausible disruptive scenarios should be assessed for their financial, operational and reputational impact, and the resulting risk assessment should be the foundation for recovery priorities and objectives. Continuity plans should establish contingency strategies, recovery and resumption procedures, and communication plans for informing management, employees, regulatory authorities, customer, suppliers, and – where appropriate – civil authorities.	None			
		59	A bank should periodically review its continuity plans to ensure contingency strategies remain consistent with current operations, risks and threats, resiliency requirements, and recovery priorities. Training and awareness programmes should be implemented to ensure that staff can effectively execute contingency plans. Plans should be tested periodically to ensure that recovery and resumption objectives and timeframes can be met. Where possible, a bank should participate in disaster recovery and business continuity testing with key service providers. Results of formal testing activity should be reported to management and the board.	None			
Role of Disclosure							
11	**A bank's public disclosures should allow stakeholders to assess its approach to operational risk management.**	60	A bank's public disclosure of relevant operational risk management information can lead to transparency and the development of better industry practice through market discipline. The amount and type of disclosure should be commensurate with the size, risk profile and complexity of a bank's operations, and evolving industry practice.	None			
		61	A bank should disclose its operational risk management framework in a manner that will allow stakeholders to determine whether the bank identifies, assesses, monitors and controls/mitigates operational risk effectively.	None			
		62	A bank's disclosures should be consistent with how senior management and the board of directors assess and manage the operational risk of the bank.	None			
		63	A bank should have a formal disclosure policy approved by the board of directors that addresses the bank's approach for determining what operational risk disclosures it will make and the internal controls over the disclosure process. In addition, banks should implement a process for assessing the appropriateness of their disclosures, including the verification and frequency of them.	None			