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

As you are aware, 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 used;			
				(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 business volumes);			
				(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 support functions.	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 and tolerance.	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			
Senior Management							

Principle	Description / Criteria	Paragraph #	Paragraph Description	Sub - Paragraph	Criteria Rating	Rating Rationale*	Action Plans^
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 risk.	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			
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 factors;			
				(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;			

Principle	Description / Criteria	Paragraph #	Paragraph Description	Sub - Paragraph	Criteria Rating	Rating Rationale*	Action Plans^
				(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			
				(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 and systems.	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;			

Principle	Description / Criteria	Paragraph #	Paragraph Description	Sub - Paragraph	Criteria Rating	Rating Rationale*	Action Plans^
				(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			
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 activities.	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.			

Principle	Description / Criteria	Paragraph #	Paragraph Description	Sub - Paragraph	Criteria Rating	Rating Rationale*	Action Plans^
		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 programmes.	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			
		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			

Principle	Description / Criteria	Paragraph #	Paragraph Description	Sub - Paragraph	Criteria Rating	Rating Rationale*	Action Plans^
		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			
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 be vulnerable.	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			