Appendix III: PSMOR principles

Principles		Criteria	
1. Operational risk culture		1	Code of conduct or ethics policy
		2	Compensation policies aligned with the bank's statement of risk appetite and tolerance
		3	Compensation policies that balance risk and reward
		4	Operational risk training available throughout the organisation
2. Operational risk management framework		5	Integration of ORMF into overall risk management process
		6	Documented in board of directors-approved policies
		7	Identifies the governance structures used to manage operational risk
		8	Describes each of the operational risk identification and assessment tools
		9	Describes the bank's accepted operational risk appetite and tolerance
		10	Describes the bank's approach to establishing and monitoring thresholds
		11	Establishes risk reporting and MIS
		12	Provides for a common taxonomy of operational risk terms
		13	Provides for appropriate independent review and assessment
		14	Requires the policies to be reviewed whenever a material change occurs
		15	Includes definitions of operational risk and operational event types
		16	Was reviewed and updated to ensure alignment of the enhanced BCBS Principles
		17	Application of ORMF to all the bank's material operating groups and entities
		18	Describes the roles and responsibilities of each of the three lines of defence
		19	Establishes the mandates, membership and representation
		20	Provides for the use of the operational risk taxonomy
3. Board of directors		21	Establishes a management culture, and supporting processes
		22	Develops comprehensive, dynamic oversight and control environments
		23	Approves the policies of the operational risk management framework
		24	Regularly reviews the framework to ensure op risk from external market changes is being managed
		25	Ensures that the bank's framework is subject to effective independent review
		26	Ensures that management applies best practice as it evolves
		27	Establishes clear lines of management responsibility and accountability for implementing a strong control environment
4. Operational risk appetite and tolerance		28	Articulates the nature, types and levels of operational risk
		29	Has been approved and reviewed by the board of directors
		30	The board regularly reviews the appropriateness of limits and the overall operational risk appetite and tolerance statement
		31	The board monitors management's adherence to the risk appetite and tolerance statement
5. Three lines of defence and senior management	Senior mgmt.	32	Develops clear, effective and robust governance structures with well defined, transparent and consistent lines of responsibility
		33	Establishes and maintains robust challenge mechanisms and effective issue resolution processes
		34	Develops specific policies, procedures and systems for management of operational risk consistent with risk appetite/tolerance
		35	Ensures effective coordination and communication with staff responsible for managing risks
		36	Ensures that management of the corporate operational risk function has sufficient stature within the

Principles		Criteria	
			bank
		37	Ensures that the bank's activities are conducted by staff with the necessary experience, technical capabilities and access to resources
		38	Ensures that staff responsible for monitoring and enforcing compliance have independent authority
		39	Ensures establishment of specific and formal operational risk management committees
		40	The operational risk committee(s) receives input from operational risk committees by country, business or functional areas
		41	The operational risk committee(s) meets at appropriate frequencies with adequate time and resources
		42	The operational risk committee(s) maintains records of committee operations that allow for review and evaluation
		43	Appropriate level of operational risk training is available at all levels throughout the organisation
	Three lines of defence	44	Established roles and responsibilities for the three lines of defence
		45	Implemented a more refined approach to assigning specific roles and responsibilities for the three lines of defence
		46	Strong risk culture and good communication between the three lines of defence to ensure good operational risk governance
	First line of defence	47	Responsibility has been assigned for identifying and managing the operational risks inherent in products, activities etc
		48	Provided with adequate resources, tools and training to ensure awareness of all operational risks and effectiveness of assessments
	Second line of defence	49	Second line of defence responsibilities have been assigned
		50	Independent challenge is appropriately evidenced
		51	Second line of defence responsibilities have clearly been assigned to other internal control groups or centres of competence
		52	Second line of defence responsibilities include development and ownership of operational risk management policies
		53	Corporate operational risk function should have a sufficient number of personnel with expertise in the management of operational risk
		54	Corporate operational risk function has implemented a quality assurance programme that ensures an independent challenge
	Third line of defence	55	Third line of defence responsibilities include independent review and challenge
		56	Review and challenge are monitored by persons not involved in the development, implementation and operation of framework
		57	Internal audit or other independent parties have sufficient resources to carry out their responsibilities as third line of defence
		58	Adequate coverage to independently verify that the framework has been implemented as intended
		59	Frequency and scope of review of both first and second lines of defence are sufficient and commensurate with other risk functions
		60	Coverage includes judgement of appropriateness and adequacy of the framework and associated governance processes
		61	Internal audit or other independent parties evaluate if framework meets organisational needs and supervisory expectations
		62	If independent review is outsourced, management considers the effectiveness of these arrangements and the appropriateness of relying on the provider as third line of defence
6. Risk identification and assessment		63	Audit findings are considered as part of the operational risk profile assessment
		64	Bank has a process that takes account of audit findings when challenging business self-assessments
		65	Audit function conducts a detailed end-to-end analysis of the operational risk profile assessment

Principles	Criteria	
		process
	66	Bank captures and aggregates all material risk data across the banking group
	67	Internal loss data are available by business line, legal entity, asset type, industry, region etc
	68	Methodology for capturing loss data is adequately documented and accounts for all material risks in all positions
	69	As a key practice in capturing material risks, the bank makes use of internal loss data as part of a robust operational risk framework
	70	Internal loss events are analysed to provide insight into the causes of large losses and to establish whether control failures are isolated or systemic
	71	Uses a consistent approach to perform root cause analysis and analysis of control effectiveness for material loss
	72	Captures and monitors all operational risk contributions to credit and market risk-related losses
	73	Uses external data elements, consisting of gross operational loss amounts, dates, recoveries and relevant causal information
	74	External loss data are compared with internal loss data, and used to explore possible weaknesses in the control environment
	75	External loss data collection process includes an analysis of material external losses to provide insights into emerging risks
	76	A risk self-assessment is used to assess the processes underlying the bank's operations against a library of potential threats
	77	Uses a risk and control self-assessment (RCSA) to evaluate inherent risk, the effectiveness of the control environment, and residual risk
	78	Risk assessment forms part of a comprehensive enterprise operational risk profile and is integrated into an overall process
	79	Scorecards build on RCSAs by weighting residual risks to provide a means of translating the RCSA output into metrics
	80	RCSAs are used on an enterprise-wide basis, including for control functions such as risk management, compliance, internal audit etc
	81	The frequency of RCSA updates is adequately aligned with the underlying operational risk profile
	82	Use of business process mapping to identify key steps and risks in business processes, activities and organisational functions
	83	Well documented, consistent and widely communicated business process mapping methodology that engages all business/risk areas
	84	Business process maps are used to reveal individual risks, risk interdependencies, and areas of control or risk management weakness
	85	Risk and performance indicators are used to provide insight into risk exposure
	86	Key risk indicators (KRIs) are used to monitor the main drivers of exposure associated with key risks
	87	Key performance indicators (KPIs) are used to provide insight into the status of operational processes
	88	KRIs are selected for each business line, as well as for the overall bank level, for each material operational risk
	89	KRIs and KPIs are paired with escalation triggers to warn when risk levels approach or exceed thresholds or limits, and prompt mitigation plans
	90	KRIs, KPIs and escalation triggers are subject to regular review and enhancement
	91	Use of scenario analysis to identify potential operational risk events, and assess their potential outcomes
	92	Scenario analysis is performed at a level which allows for the understanding of inherent risk in products, activities and processes

Principles	Criteria	
	93	Scenario analysis is used to consider potential sources of significant operational risk and the need for additional controls or mitigation
	94	Scenario analysis is used as a source for assessing risk profile
	95	Robust governance framework exists to ensure the integrity and consistency of the scenario analysis process
	96	Bank uses the output of the risk assessment tools as inputs to a model that quantifies its exposure to operational risk
	97	Adequately documents the rationale for all material assumptions underpinning the bank's chosen analytical frameworks
	98	Quantification of the bank's exposure to operational risk takes into account reasonableness, and includes an independent validation/review
	99	In quantifying exposure, data integrity is covered by strong governance and robust verification/validation procedures
	100	Comparative analysis is used to compare results of various assessment tools
	101	Where capital estimation is a risk assessment tool, outcomes are benchmarked against internal data, external data, scenario analysis etc
	102	Use and effectiveness of risk assessment tools are benchmarked against industry practice
	103	Ensures that the internal pricing and performance measurement mechanism appropriately takes into account operational risk
	104	Risk-taking incentives are appropriately aligned with risk appetite and tolerance
	105	Established procedures for each operational risk management tool
	106	Structured and consistent processes to monitor and track action plans developed from the use of all operational risk management tools
7. Change management	107	Operational risk management framework that addresses operational risk exposure related to new activities, products etc
	108	Policies and procedures that address the process for review and approval of new products, activities, processes and systems
	109	Inherent risks in the new product, service, or activity
	110	Changes to the bank's operational risk profile and appetite and tolerance, including the risk of existing products or activities
	111	Necessary controls, risk management processes, and risk mitigation strategies
	112	Residual risk
	113	Changes to relevant risk thresholds or limits
	114	Procedures and metrics to measure, monitor, and manage the risk of the new product or activity
	115	Defined specific objective criteria and procedures to clearly identify new activities, products, technology systems, or business with geographically distant markets
	116	Clearly allocated roles and responsibilities or both the first and second lines of defence in order to assess the risk exposure relating to such changes
	117	Thorough assessment of all operational risk aspects consistent with the bank's operational risk taxonomy and measurement categories
	118	Reviews and updates the policy and procedures regularly and/or on event-driven basis, to take into account the rate of growth, state-of-the-art developments etc
	119	Ensures that appropriate investment has been made for human resources and technology infrastructure before new products are introduced
	120	Monitors the implementation of new products, activities, processes and systems in order to identify any material differences to the expected operational risk profile
	121	If unexpected risks emerge, the banks has a process to identify these risks and implement appropriate mitigating controls

Principles	Criteria	
	122	Formal post-implementation review process exists to ensure effective implementation of new or material changes to products, activities, processes and systems
8. Monitoring and reporting	123	Ensures that reports are comprehensive, accurate, consistent and actionable across business lines and products
	124	Reports are manageable in scope and volume; effective decision-making is not impeded by either too much or too little data
	125	Reporting is timely and a bank is able to produce reports in both normal and stressed market conditions
	126	Frequency of reporting reflects the risks involved and the pace and nature of changes in the operational environment
	127	Results of monitoring activities are included in regular management and board reports, as are assessments of the framework performed by IA and/or RM functions
	128	Operational risk reports contain internal financial, operational, and compliance indicators, as well as external market or environment information
	129	Reports generated by supervisory authorities are reported internally to senior management and the board, where appropriate
	130	Operational risk reports include breaches of the bank's risk appetite and tolerance statement, as well as thresholds or limits
	131	Operational risk reports include details of recent significant internal operational risk events and losses
	132	Operational risk reports include relevant external events and any potential impact on the bank and operational risk capital
	133	Operational risk reports include an operational risk profile for the bank, including the inherent and residual risk levels for its taxonomy
	134	Operational risk reports include details of key and emerging operational risks
	135	Operational risk reports include an effective balance of qualitative and quantitative information
	136	Operational risk reports include key action plans in place to address material control gaps
	137	Data capture and risk-reporting processes are analysed periodically with a view to enhancing risk management performance and to advancing risk management policies etc
9. Control and mitigation	138	Top-level reviews of progress toward stated objectives
	139	Verifying compliance with management controls
	140	Review of the treatment and resolution of instances of non-compliance
	141	Evaluation of the required approvals and authorisations to ensure accountability at an appropriate level of management
	142	Tracking reports for approved exceptions to thresholds or limits, management overrides and other deviations from policy
	143	Clearly established authorities and/or processes for approval
	144	Close monitoring of adherence to assigned risk thresholds or limits
	145	Safeguards for access to, and use of, bank assets and records
	146	Appropriate staffing level and training to maintain expertise
	147	Ongoing processes to identify business lines or products where returns appear to be out of line with reasonable expectations
	148	Regular verification and reconciliation of transactions and accounts
	149	A vacation policy that requires bank's officers and employees to be absent from their duties for a period of not less than two consecutive weeks every year
	150	Governance and oversight controls that ensure technology, including outsourcing arrangements, is aligned with business objectives

Principles	Criteria	
	151	Policies and procedures that facilitate identification and assessment of risk
	152	Establishment of risk appetite and tolerance statement as well as performance expectations to assist in controlling and managing risk
	153	Implementation of an effective control environment and the use of risk transfer strategies that mitigate risk
	154	Monitoring processes that test for compliance with policy thresholds or limits
	155	Management makes appropriate capital investment or otherwise provides for a robust infrastructure at all times
	156	Procedures for determining whether and how activities can be outsourced
	157	Processes for conducting due diligence in the selection of potential service providers
	158	Sound structuring of outsourcing arrangements, including for ownership and confidentiality of data, as well as termination rights
	159	Programmes for managing and monitoring the risks associated with the outsourcing arrangement, including financial condition
	160	Establishment of an effective control environment at the bank and the service provider
	161	Development of viable contingency plans
	162	Execution of comprehensive contracts and/or service level agreements with a clear allocation of responsibilities
	163	The board determines the maximum loss exposure that the bank is willing and has the financial capacity to assume
	164	The board performs an annual review of the bank's risk and insurance management programme
	165	Bank carefully considers the extent to which risk mitigation tools such insurance truly reduces, transfers or creates risk
10. Resiliency and continuity	166	Established business continuity plans commensurate with the nature, size and complexity of operations
	167	Established business continuity plans cover all business and groups of the bank
	168	Continuity management incorporates business impact analysis, recovery strategies, testing, training and awareness programmes etc
	169	Identifies critical business operations, key internal and external dependencies, and appropriate resilience levels
	170	Plausible disruptive scenarios are assessed for financial, operational and reputational impact
	171	Contingency plans establish contingency strategies, recovers and resumption procedures, and communication plans
	172	Periodically reviews continuity plans to ensure contingency strategies remain consistent with current operations, risks and threats etc
	173	Resilience and continuity training and awareness programmes are implemented to ensure staff effectively execute contingency plans
	174	Plans are tested periodically to ensure that recovery and resumption objectives and timeframes can be met
	175	Participates in disaster recovery and business continuity testing with key service providers
	176	Results of formal testing activity are reported to senior management and the board
11. Role of disclosure	177	The amount and types of disclosure are commensurate with the size, risk profile and complexity of the bank's operations
	178	Discloses operational risk management framework so that stakeholders can determine bank's operational risk effectiveness
	179	Formal disclosure policy that addresses approach for determining operational risk disclosures and internal controls

Principles	Criteria	
	180	Implemented a process for assessing the appropriateness of the disclosures