Appendix IV: Emerging and noteworthy practices

Principles	Emerging and noteworthy practices	
1. Operational risk culture	1	The code of conduct or ethics policy applies to all the bank's staff and appointees, including members of the board of directors.
	2	The code of conduct or ethics policy is regularly reviewed and attested to by employees, is regularly approved by the board of directors, and is publicly available on the bank's website.
	3	A separate code of conduct is established specifically designed for certain roles (eg treasury dealers, senior management etc).
	4	Establishment and implementation of a whistle-blower programme.
	5	A senior ethics committee that oversees the code of conduct or ethics policy and its implementation within the bank.
	6	Linking the compensation programme and remuneration to risk-adjusted indicators.
	7	Establishing operational risk awareness for all employees; more advanced training on the operational risk identification and assessment tools, and processes and policies for individuals with operational risk responsibilities.
	8	Customised and mandatory operational risk training for many roles including business unit operations, supervisory levels, senior management, and the board of directors.
	9	Strong internal monitoring of training practices relative to requirements.
2. Operational risk management framework	10	The ORMF was reviewed and updated to ensure alignment following the publication of the enhanced *BCBS Principles for the Sound Management of Operational Risk* in June 2011.
	11	Referencing the relevant operational risk management policies and procedures.
	12	Applying the ORMF to all the bank's material operating groups and entities, including subsidiaries, joint ventures and geographic regions.
	13	The ORMF requires consistent implementation of the bank's operational risk taxonomy across all business lines and operational risk tools.
	14	Describing the roles and responsibilities of each of the three lines of defence as they relate to the use of the operational risk identification and assessment tools.
	15	Establishing the mandates, membership, and representation of various operational risk governance committees.
	16	Establishing a quality assurance programme to ensure that independent challenge and review, as applied by the second line of defence, results in consistent risk and control assessments.
	17	Creation of an operational risk dictionary that includes definitions and examples of the various operational risks in the bank's taxonomy. In addition, the dictionary includes guidance related to the classification of each of the operational risks within the taxonomy, to ensure consistent identification and classification across the bank.
	18	Establishing a control library to inventory all the controls within the bank and each of its business lines.
	19	Defining operational risk events beyond direct financial losses, so that such events include indirect losses such as forgone revenue and lost business, and reputational damage.
	20	Using a central operational risk system and data repository that allows for the central capture, aggregation, and reporting of key operational risk data including operational losses, operational risk assessments, control deficiencies, and key risk indicators.
	21	Regularly reconciling operational risk event data to the relevant source (ie general ledger).
3. Board of directors	22	Establishing a code of conduct or an ethics policy that sets clear expectations for integrity and ethical values of the highest standard and identifies acceptable business practices and prohibited conflicts.

Principles	Emerging and noteworthy practices	
	23	The board regularly challenges senior management on the design and effectiveness of the bank's operational risk management framework.
	24	The board reviews and approves an operational risk strategy that sets forth the long-term vision for the programme and the initiatives planned to support implementation.
	25	The board supports the establishment of a formal culture communications strategy, whereby senior management communicates the importance of strong risk management practices through a variety of forums such as employee communications and formal training sessions.
	26	The board ensures that internal audit includes the ORMF as a focus within business unit audits, to complement the overall audit of the ORMF.
	27	The board ensures that the scope of internal audit's work on the bank's ORMF is not limited to risk measurement (ie model) activities and includes a sufficient focus on risk management activities.
	28	The board commissions an external third-party review of the design and effectiveness of the bank's ORMF.
4. Operational risk appetite and tolerance	29	Defining operational risk appetite and tolerance at both a divisional and taxonomy level.
	30	Utilising both quantitative and qualitative components within the bank's operational risk appetite and tolerance statement.
	31	Setting limits based on established key risk indicators such as loss metrics, deficiencies, events and residual risk assessments using operational risk identification and assessment tools that have been implemented.
5. Senior mgmt.	32	Ensuring that an appropriate level of operational risk training is available at all levels throughout the organisation and that the training reflects the seniority, role and responsibility of the individuals for whom it is intended.
	33	Membership of the operational risk committee consists of the first line of defence, the CORF, and other second line of defence control functions.
	34	ORC meetings are convened regularly, minutes are prepared, and action items are tracked to completion.
	35	Succession plans for key operational risk individuals have been established to ensure continuation of critical operations and maintenance of expertise.
Three lines of defence	36	A well documented and clearly articulated set of responsibilities for each of the three lines of defence: First line of defence responsibilities include using operational risk management tools to identify and manage risks, assess and enhance controls, monitor and report the operational risk profile, ensure that the operational risk profile is consistent with the established risk appetite and tolerance, adhere to policies, standards and guidelines, and promote a strong risk culture. Second line of defence responsibilities include designing operational risk management tools used by the business to identify and manage risks, apply "independent challenge" to the first line of defence's use of and output from the operational risk management tools, develop and maintain policies, standards and guidelines, review and contribute to the monitoring and reporting of operational risk profile, design and provide operational risk training and awareness, and promote a strong risk culture. Third line of defence responsibilities include independently verifying that the ORMF has been adequately designed and implemented by both the first and second lines of defence, reviewing the "independent challenge" applied by the second line of defence to the first line of defence's use of and output from the operational risk management tools, review the monitoring, reporting and governance processes, and promote a strong risk culture.
	37	Independent challenge is defined as the process of developing an independent view regarding the business unit's operational risk management activities including the identification of operational risks, assessment of operational risks, identification of controls, assessment of controls, assumptions and acceptance of risk.
	38	Independent challenge is applied through the various operational risk management tools, applied through reporting and other governance processes, shared with the business in a constructive

Principles	Emerging and noteworthy practices	
		manner, performed on a timely basis and adequately evidenced/documented.
	39	Corporate control groups with relevant subject matter (eg compliance, legal, business continuity, technology risk management etc) are engaged to support the second line of defence for various operational risk management tools.
First line of defence	40	The business line management is responsible for "operational risk management", as they are responsible for planning, directing, and controlling day-to-day operations.
	41	Identifying and assessing the inherent operational risk within the respective business units, through the use of the operational risk management tools and assessing the materiality of the inherent risks to the respective business units.
	42	Establishing appropriate mitigating controls relative to the inherent operational risks, and assessing the design and effectiveness of these controls through the use of the operational risk management tools.
	43	Monitoring and reporting the organisation's operational risk profile, and ensuring adherence to established operational risk appetite and tolerance.
	44	Reporting on any residual operational risk that is not mitigated by controls, including operational risk events, control deficiencies, process inadequacies, and non-compliance with operational risk tolerances.
	45	Promoting a strong operational risk management culture throughout the first line of defence.
	46	Responsible for adherence to various risk policies and frameworks.
	47	Business line management is provided with adequate resources, tools and training to ensure awareness of all operational risks and effectiveness of assessments.
	48	In general, the CORF is staffed with tenured individuals who have the appropriate seniority and experience; the titles, stature and compensation of operational risk staff are commensurate with those of other risk functions.
	49	Developing an independent view regarding the business unit's identification of operational risks, assessment of operational risks, identification of controls, assessment of controls, assumptions, and acceptance of risk.
	50	The independent challenge applied to operational risk management tools, measurement activities and reporting systems is appropriately evidenced.
	51	Second line of defence responsibilities have clearly been assigned to other internal control groups or centres of competence (eg business continuity management, compliance, legal etc).
	52	The corporate operational risk function has implemented a quality assurance programme that ensures that the independent challenge applied to the operational risk management tools, measurement and reporting systems is consistent and appropriately evidenced.
	53	Conducts periodic independent review and testing of the design and effectiveness of the ORMF and associated governance processes through the first and second lines of defence.
	54	Proactively manages the closure of issues and ensures that the management promptly, accurately and adequately responds to the issues raised.
	55	Internal audit or other independent parties have sufficient resources to carry out their responsibilities as the third line of defence.
	56	The frequency and scope of review by independent parties of both the first and second line of defence are sufficient and commensurate with other risk management functions.
6. Risk identification and assessment	Audit findings	
	57	The consideration of internal audit findings as an input to the various operational risk management tools (eg RCSAs, scenarios, key risk/performance indicators etc).
	58	The bank employs a process that considers audit findings in the challenging of business self-assessments.
	59	The bank's audit function conducts a detailed end-to-end analysis of the operational risk profile assessment process, including assessments of process governance, the detail and quality of reporting, the process by which deficiencies are identified, tracked, and remediated, and generally

Principles	Emerging and noteworthy practices	
		whether the programme is functioning in a manner consistent with established policies.
	60	The use of internal audit findings to compare management's risk and control assessments with the various operational risk management tools.
	61	The use of internal audit findings as an input to the regular updating of the bank's operational risk profile.
	62	Monitoring the number of open and overdue internal audit issues as a key indicator.
	Internal loss data collection and analysis	
	63	The bank captures and aggregates all material risk data across the banking group.
	64	Collecting and analysing information relating to all internal operational risk events, including losses, near-misses and profitable events.
	65	Establishing an internal threshold (eg $100,000 or €100,000) above which any operational risk event (ie losses, near-misses and profitable events) is subject to a thorough and standardised root cause analysis by the first line of defence, which in turn is subject to independent review and challenge by the second line of defence.
	66	Supporting guidance and a standardised template is provided to the first line of defence by the second line of defence to ensure consistency in approach.
	67	Embedding the bank's operational risk taxonomy into the template, so as to enable the use of this information when considering the other operational risk management tools and the bank's operational risk profile.
	68	Close monitoring of the action plans resulting from the root cause analysis.
	69	Escalating the details of the root cause analysis and resulting action plan for items above a defined internal threshold to senior management or an operational risk committee for review.
	70	Internal loss data are available by business line, legal entity, asset type, industry, region etc to support the identification and reporting of risk exposures, concentrations and emerging risks.
	71	The bank adequately documents the methodology by which loss data are captured and considered for all material risks in all of its positions, portfolios and business lines.
	72	Sharing operational risk event details across business lines and geographies and encouraging remediation along similar lines wherever applicable.
	73	As a key practice in capturing material risks, the bank makes use of internal loss data as part of a robust operational risk framework.
	74	Using operational loss data to assess the quality of other operational risk tools such as the RCSA, and to review whether the associated risk or control assessment may have been improperly evaluated.
	75	Establishing a regular meeting between the operational risk management function and other risk management functions to review and discuss issues and events, including boundary losses.
	External data collection and analysis	
	76	External loss data received from industry consortia or other external parties are used to benchmark and assess internal loss data.
	77	The external loss data collection process includes an analysis of material external losses that may provide insight into emerging operational risks.
	78	External loss data received from industry consortiums or other external parties are used as key inputs for both the scenario analysis and RCSA tools.
	79	Establishing a formal process to review and assess for applicability the details of operational risk events made available through the media and other sources.
	80	The operational risk management function distributes to business lines and operational risk officers a monthly newsletter listing all the significant industry events.
	81	Examples of external losses are reviewed monthly on a thematic basis both for applicability and to establish whether similar gaps exist within the bank's own business lines.

Principles	Emerging and noteworthy practices	
	Risk and control self-assessment (RCSA)	
	82	Implementing a multi-tiered approach for the RCSA tool (ie conducting RCSAs at the bank-wide, divisional and business-line levels).
	83	Risk assessment forms part of a comprehensive enterprise operational risk profile and is integrated into an overall process.
	84	RCSAs are used on an enterprise-wide basis, including for control functions such as risk management, compliance, internal audit etc
	85	Maintaining sufficient evidence of the review and independent challenge of the RCSAs by the second line of defence.
	86	The aggregation of bank-wide themes and issues identified through the RCSAs.
	87	Embedding the bank's operational risk taxonomy within the RCSA to ensure alignment with other tools and to allow for aggregation of a risk profile.
	88	Completing RCSAs for key shared business functions or processes.
	89	The frequency of RCSA updates is adequately aligned with the underlying operational risk profile.
	90	Categorising residual risk into one of four categories summarising the status: treat, tolerate, terminate or transfer.
	91	The use and effectiveness of risk assessment tools are benchmarked against industry practice.
	92	Where capital estimation is a risk assessment tool, outcomes are benchmarked against internal data, external data, scenario analysis and any other result of the various assessment tools to assess the bank's operational risk profile.
	Business process mapping	
	93	Implementing a business process framework that provides guidelines for the creation of business process maps.
	94	Undertaking a risk-based approach to business mapping, implying a focus on high-risk processes rather than all business processes within the bank.
	95	Establishing a central repository for all business process maps.
	96	Embedding the bank's operational risk taxonomy into the business process mapping methodology for aggregation and comparison with the operational risk profile.
	Key risk and performance measures	
	97	Establishing key risk and performance indicators at multiple levels throughout the bank, including at the group-wide level, the divisional level, and the individual business-line level.
	98	KRIs, KPIs and escalation triggers are subject to regular review and enhancement.
	99	The first line of defence creates action plans for metrics that breach their respective thresholds.
	100	The second line of defence independently challenges the selection of indicators and thresholds, as well as the proposed action plans.
	Scenario analysis	
	101	Scenario analysis is performed at a level that provides for a full understanding of the inherent risk in products, activities and processes.
	102	Scenario analysis is used as an input for assessing the risk profile.
	103	Implementing scenarios at the bank-wide, divisional and business unit levels.
	104	Using scenarios to assess existing controls, to identify additional controls necessary to mitigate the associated risks, and develop and monitor appropriate action plans as needed.
	105	Using scenarios to supplement the RCSA and other operational risk management tools, by focusing on low-probability, high-impact events that the other tools may not necessarily identify.
	106	Using scenarios to compare the control environment, and help assess the completeness and adequacy of assessments in other tools (ie RCSA).
	107	Using operational risk scenarios for enterprise-wide risk management assessment purposes (ie

Principles	Emerging and noteworthy practices	
		earthquakes etc).
	108	Reviewing the universe of scenarios annually; creating a plan to develop, update, retire, reclassify or maintain the scenarios over the course of the year.
	109	Establishing a scenario governance committee that oversees the overall scenario programme.
	Comparative analysis	
	110	Using the assessments and outputs of each of the operational risk management tools to assess the effectiveness of other tools.
	111	Comparing the operational risk management tool assessments and outputs across similar business lines and geographies (ie RCSAs, operational risk events, scenarios etc).
	112	Establishing a formal process to conduct this comparative analysis by both the first and second lines of defence.
	Other risk identification and assessment activities	
	113	Conducting formal benchmarking of operational risk management practices.
	114	Establishing policies and procedures for each of the bank's operational risk management tools describing the expected use of such tools as well as the various roles and responsibilities of the three lines of defence as they relate to the use of the tools.
	115	Creating, monitoring and remediating action plans resulting from the use of each of the bank's operational risk management tools.
	116	The bank adequately documents the rationale for all material assumptions underpinning its chosen analytical frameworks, including the choice of inputs, distributional assumptions, and weighting of quantitative and qualitative elements.
	117	The quantification of the bank's exposure to operational risk takes into account reasonableness, and includes an independent validation/review.
	118	In quantifying exposure to operational risk by using the output of the risk assessment tools, data integrity is covered by strong governance and robust verification/validation procedures.
7. Change management	119	Alignment of risk and control assessments, within the change management process, with the bank's operational risk taxonomy to allow for integration and aggregation of results within the bank's overall risk profile.
	120	A formal project governance programme that involves several approvals or "gates" through the life of a new product or initiative.
	121	The bank has defined objective criteria and procedures to identify new activities, products, technology systems, or business with geographically distant markets.
	122	The bank has clearly allocated roles and responsibilities for both the first and second lines of defence in order to assess the risk exposure relating to change initiatives in line with the accepted risk appetite of the bank.
	123	The identification of controls or actions required, either pre- or post-implementation, which are closely monitored by the second line of defence to ensure remediation.
	124	Establishing oversight committees to monitor the implementation of new product and new initiative frameworks as well as to review and approve specific business cases.
	125	Implementing a risk-based approach to the application of requirements for risk and control assessments, as well as approvals, such that products and initiatives subject to higher levels of risk and impact are subject to greater intensity of governance and oversight.
	126	A product risk framework that sets forth requirements at the various stages of the product life cycle (eg development, change, grandfathering and closure).
	127	Maintaining a central list of all the bank's products.
	128	Operational risk and control assessments related to new products and initiatives are performed by the first line of defence, and are subject to independent challenge by the second lines of defence.
	129	Appropriately formalised and documented involvement of several control groups within the second line of defence's review of risk and control assessments, such as finance, compliance, legal, business

Principles	Emerging and noteworthy practices	
		continuity, technology, and other risk management groups.
	130	Establishing a formal post-implementation review to assess the realisation of anticipated benefits such as cost reduction, revenue generation, and risk reduction prior to the formal closure of the project.
	131	A formal post-implementation review process exists to ensure effective implementation of new or material changes to products, activities, processes and systems.
	132	The bank reviews and updates the policy and procedures regularly, and/or on an event-driven basis, to take into account growth rates, technological developments, legal framework changes etc
8. Monitoring and reporting	133	Production of operational risk reports on a regular (ie quarterly or monthly) basis that are distributed to senior management and/or the board.
	134	Operational risk reports include an operational risk profile for the bank, including the inherent and residual risk levels for its taxonomy.
	135	Operational risk reports include details of key and emerging operational risks.
	136	Operational risk reports include an effective balance of qualitative and quantitative information.
	137	Operational risk reporting includes an appropriate balance of information related to changes in both the business environment and operational risk data (loss data, KRIs), and includes an update of key operational risk action items.
	138	Reporting of adherence to the operational risk appetite and tolerance.
	139	Inclusion of the operational risk profile in operational risk reporting, as well as key themes and issues identified through the use of operational risk management tools.
	140	Operational risk reports include key action plans to address material control gaps.
9. Control and mitigation	141	The use of metrics for comparison of returns (by business unit, by product) with the budget (projected outcome), fluctuation of daily P&L (specifically in trading/financing business unit) and specific transactions with an irregular return ratio.
	142	Clear assignment of both first and second line of defence responsibilities as they relate to the assessment and control of outsourcing risk.
	143	The use of operational risk management tools (ie RCSAs, KRIs etc) to help manage outsourcing risks.
	144	The development of contingency plans and alternative/backup arrangements for material outsourcing arrangements.
10. Resiliency and continuity	145	Well established process to identify and categorise the criticality of business functions, vulnerabilities and disruptive impact, and the establishment of thresholds for activation of business continuity plans (eg maximum tolerable outage etc).
	146	The integration of disruptive scenario analysis into other risk management tools and processes (eg KRIs, Pillar II etc).
	147	The provision of customised business continuity training to staff, according to their specific roles, as well as regular review of the training to ensure its applicability.
11. Role of disclosure	148	Developing a disclosure policy that is regularly approved by senior management and the board.
	149	Implementing, as part of the audit process, a review to assess the effectiveness of the policy.